

3.6. Tétel. Bármely két $f, g \in T[x]$ polinomnak létezik legnagyobb közös osztója és legkisebb közös többszöröse. A legnagyobb közös osztó kiszámítható az **euklideszi algoritmussal**, és kifejezhető f és g „lineáris kombinációjaként”:

$$\exists u, v \in T[x]: fu + gv = \text{Inko}(f, g).$$

3.7. Tétel. Tetszőleges nemzéró $f, g, h \in T[x]$ polinomok esetén az $fu + gv = h$ egyenlet akkor és csak akkor oldható meg az ismeretlen $u, v \in T[x]$ polinomokra nézve, ha $\text{Inko}(f, g) \mid h$:

$$\exists u, v \in T[x]: fu + gv = h \iff \text{Inko}(f, g) \mid h.$$

Handwritten note: $ax + by = c$ van megoldása $\iff \text{HKO}(a, b) \mid c$

3.8. Definíció. Tetszőleges $f, g, m \in T[x]$ esetén azt mondjuk, hogy f **kongruens** g -vel modulo m , ha $m \mid f - g$

$$f \equiv g \pmod{m} \iff m \mid f - g.$$

3.9. Tétel. A modulo m kongruencia ekvivalenciareláció $T[x]$ -en, és két polinom akkor és csak akkor kongruens modulo m , ha ugyanazt a maradékot adják m -mel osztva.

3.10. Tétel. Tetszőleges $f, g, h \in T[x]$ esetén az $fu \equiv h \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg (az u ismeretlen polinomra nézve), ha $\text{Inko}(f, m) \mid h$:

$$\exists u \in T[x]: fu \equiv h \pmod{m} \iff \text{Inko}(f, m) \mid h.$$

Handwritten note: $ax \equiv b \pmod{m}$ van megoldása $\iff \text{HKO}(a, m) \mid b$

3.11. Definíció. Legyen $m \in T[x]$ legalább elsőfokú polinom.

- modulo m **maradékosztály**: $\bar{f} = \{ g \in T[x] : f \equiv g \pmod{m} \}$
- a maradékosztályok halmaza: $T[x]/\langle m \rangle = \{ \bar{f} : f \in T[x] \}$ *$\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$*
- műveletek: $\bar{f} + \bar{g} = \overline{f + g}$, $-\bar{g} = \overline{-g}$, $\bar{f} \cdot \bar{g} = \overline{f \cdot g}$

3.12. Tétel. A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (additív inverze, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik elemet választjuk reprezentánsnak, és ezekkel a műveletekkel $T[x]/\langle m \rangle$ kommutatív egységelemes gyűrűt alkot (modulo m **maradékosztály-gyűrű**).

3.13. Tétel. Az $\bar{f} \in T[x]/\langle m \rangle$ maradékosztálynak akkor és csak akkor létezik multiplikatív inverze, ha $\text{Inko}(f, m) \sim 1$. Ilyenkor a multiplikatív inverz egyértelműen meghatározott.

3.14. Feladat. Határozzuk meg az f és g valós polinomok legnagyobb közös osztóját, és adjuk meg az $fu + gv = \text{lko}(f, g)$ egyenlet egy megoldását.

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

mp.

$$\overbrace{(x^4 + 2x^3 - x^2 - 4x - 2)}^f : \overbrace{(x^4 + x^3 - x^2 - 2x - 2)}^g = 1$$

$$\begin{array}{r} x^4 + x^3 - x^2 - 2x - 2 \\ \hline x^3 \quad -2x \end{array}$$

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

$$\overbrace{(x^4 + x^3 - x^2 - 2x - 2)}^g : \overbrace{(x^3 - 2x)}^{f-g} = x + 1$$

$$\begin{array}{r} x^4 \quad -2x^2 \\ \hline x^3 + x^2 - 2x - 2 \\ x^3 \quad -2x \\ \hline x^2 \quad -2 \end{array}$$

$$\textcircled{2} g = (x+1) \cdot (x^3 - 2x) + x^2 - 2$$

$$x^2 - 2 \sim \text{lko}(f, g)$$

$$(x^3 - 2x) : (x^2 - 2) = x$$

$$\begin{array}{r} x^3 - 2x \\ \hline 0 \end{array}$$

$$\text{lko}(f, g) \sim x^2 - 2 \stackrel{\textcircled{2}}{=} g - (x+1) \cdot \underbrace{(x^3 - 2x)}_{f-g} \stackrel{\textcircled{1}}{=} g - (x+1)(f-g)$$

$$= \underbrace{(-x-1)}_u \cdot f + \underbrace{(x+2)}_v \cdot g$$



$$f = (x^2 - 2) \cdot (x^2 + x + 1) \quad f \text{ gyökei: } \pm\sqrt{2}, -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$$

$$g = (x^2 - 2) \cdot (x^2 + 2x + 1) \quad g \text{ gyökei: } \pm\sqrt{2}, -1, -1$$

3.15. Feladat. Határozzuk meg az f és g valós polinomok legnagyobb közös osztóját, és adjuk meg az $fu + gv = \text{lko}(f, g)$ egyenlet egy megoldását.

$$f = x^3 - 2, \quad g = x^2 - 2x + 1$$

$$\begin{array}{r} \overbrace{(x^3 - 2)}^f : \overbrace{(x^2 - 2x + 1)}^g = x + 2 \\ \underline{x^3 - 2x^2 + x} \\ 2x^2 - x - 2 \\ \underline{2x^2 - 4x + 2} \\ 3x - 4 \end{array}$$

$$\textcircled{1} f = (x+2)g + (3x-4)$$

$$\begin{array}{r} \overbrace{(x^2 - 2x + 1)}^g : \overbrace{(3x - 4)}^f = \frac{1}{3}x - \frac{2}{9} \\ \underline{x^2 - \frac{4}{3}x} \\ -\frac{2}{3}x + 1 \\ \underline{-\frac{2}{3}x + \frac{8}{9}} \\ \frac{1}{9} \sim 1 \sim \text{lko}(f, g) \end{array}$$

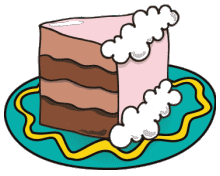
$$\textcircled{2} g = \left(\frac{1}{3}x - \frac{2}{9}\right) \cdot (3x - 4) + \frac{1}{9}$$

$$\text{lko}(f, g) \sim 1 \stackrel{\textcircled{2}}{=} gg - (3x-2) \cdot \underbrace{(3x-4)}_{f-(x+2)g} \stackrel{\textcircled{1}}{=} gg - (3x-2)(f-(x+2)g)$$

$$= gg - (3x-2) \cdot f + (3x-2) \cdot (x+2)g$$

$$= (-3x+2) \cdot f + (g + 3x^2 + 4x - 4)g$$

$$= \underbrace{(-3x+2)}_u \cdot f + \underbrace{(3x^2 + 4x + 5)}_v \cdot g$$



$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = \frac{1}{g(\sqrt[3]{2})}$$

$$f(\sqrt[3]{2}) = 0$$

$$(-3x + 2) \cdot f(x) + (3x^2 + 4x + 5) \cdot g(x) = 1$$

$$\underbrace{(-3\sqrt[3]{2} + 2) \cdot \underbrace{f(\sqrt[3]{2})}_0}_{0} + \underbrace{(3 \cdot \sqrt[3]{4} + 4\sqrt[3]{2} + 5) \cdot g(\sqrt[3]{2})}_{\frac{1}{g(\sqrt[3]{2})}} = 1 \quad x = \sqrt[3]{2}$$

$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = 3 \cdot \sqrt[3]{4} + 4 \cdot \sqrt[3]{2} + 5$$

3.16. Feladat. Készítsük el meg a $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ maradékosztály-gyűrűben az összeadás és a szorzás művelettáblázatát.

$$\begin{aligned} \mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle &= \{ \bar{f} \mid f \in \mathbb{Z}_2[x] \} \\ &= \{ \bar{f} \mid f \in \mathbb{Z}_2[x], \deg f \leq 1 \} = \\ &= \{ \overline{ax+b} \mid a, b \in \mathbb{Z}_2 \} = \\ &= \{ \bar{0}, \bar{1}, \bar{x}, \overline{x+1} \} \end{aligned} \quad \left| \quad \begin{aligned} \mathbb{Z}_4 &= \{ \bar{a} \mid a \in \mathbb{Z} \} = \\ &= \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \} \end{aligned} \right.$$

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

||S
V

.	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

GALOIS FIELD



$$\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle = \text{GF}(4)$$

lent e? IGEN

$$\bar{1}^{-1} = \bar{1}$$

$$\bar{x}^{-1} = \overline{x+1}$$

$$\overline{x+1}^{-1} = \bar{x}$$

$x^2 + x + 1$ irreducibilis $\mathbb{Z}_2$ felett

$$x^2 \equiv 1 \pmod{x^2 + x + 1}$$

$$x^2 : (x^2 + x + 1) = 1$$

$$\begin{array}{r} x^2 + x + 1 \\ -x - 1 \\ \hline x + 1 \end{array}$$

$$(x^2 + x) : (x^2 + x + 1) = 1$$

$$\begin{array}{r} x^2 + x + 1 \\ -x - 1 \\ \hline -1 = 1 \end{array}$$

3.17. Feladat. Határozzuk meg az $\bar{f}$ maradékosztály multiplikatív inverzét a $\mathbb{Z}_5[x]/\langle m \rangle$ maradékosztály-gyűrűben. Hány eleme van ennek a gyűrűnek?

$$f = 2x^2 - 3x + 2, \quad m = x^3 + 1$$

pr. $\mathbb{Z}_5[x]/\langle x^3+1 \rangle = \{ \bar{f} \mid f \in \mathbb{Z}_5[x], \deg f \leq 2 \} =$
 $= \{ \overline{ax^2 + bx + c} \mid a, b, c \in \mathbb{Z}_5 \}$
 $5 \cdot 5 \cdot 5 = 125$ elemű gyűrű.

$$\bar{f}^{-1} = \bar{u} \Leftrightarrow \bar{f} \cdot \bar{u} = \bar{1} \Leftrightarrow f \cdot u \equiv 1 \pmod{m} \Leftrightarrow m \mid f \cdot u - 1 \Leftrightarrow$$

$$\Leftrightarrow f \cdot u - 1 = m \cdot v \quad (\exists v \in \mathbb{Z}_5[x])$$

$$f \cdot u - m \cdot v = 1 \stackrel{?}{\sim} \text{hb}(f, m)$$

$$\overbrace{(x^3+1)}^m : \overbrace{(2x^2-3x+2)}^f = 3x+2$$

$$\begin{array}{r} x^3 + x^2 + x \\ \underline{4x^2 + 4x + 1} \\ 4x^2 + 4x + 4 \\ \underline{} \\ 2 \end{array}$$

$$\textcircled{1} \quad m = (3x+2) \cdot f + 2$$

$$2 \sim 1 \sim \text{hb}(f, m)$$

$$2 \stackrel{\textcircled{2}}{=} m - (3x+2) \cdot f \quad / : 3$$

$$1 = 3m - (9x+6) \cdot f$$

$$1 = \underbrace{3m}_{-v} + \underbrace{(x+4) \cdot f}_u$$

$$\bar{f}^{-1} = \overline{2x^2 - 3x + 2}^{-1} = \overline{x + 4}$$

4. Polinomfüggvények, gyökök

4.1. Definíció. Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinom.

- Az f polinom $c \in T$ helyen vett **helyettesítési értéke**:

$$f(c) = a_n c^n + \dots + a_1 c + a_0 \in T.$$

- Az f polinomhoz tartozó **polinomfüggvény**:

$$f: T \rightarrow T, c \mapsto f(c).$$

- A $c \in T$ elem **gyöke** az $f \in T[x]$ polinomnak, ha $f(c) = 0$.

4.2. Példa. Az $f = x^2 \in \mathbb{Z}_2[x]$ és $g = x^3 \in \mathbb{Z}_2[x]$ polinomokhoz ugyanaz a polinomfüggvény tartozik:

$$\mathbb{Z}_2 \rightarrow \mathbb{Z}_2, \quad \bar{0} \mapsto \bar{0}, \bar{1} \mapsto \bar{1}.$$

gyözteljesítés

4.3. Tétel (Bézout tétele). Bármely $f \in T[x]$ és $\alpha \in T$ esetén

$$f(\alpha) = 0 \iff x - \alpha \mid f. \iff f = (x - \alpha) \cdot (\dots)$$

Bizonyítás. Osszuk el f -et maradékosan $(x - \alpha)$ -val.

$$f = (x - \alpha) \cdot q + r$$

$\deg r < 1$, azaz r konstans

$$x = \alpha: f(\alpha) = \underbrace{(\alpha - \alpha)}_0 \cdot q(\alpha) + r$$

$$f(\alpha) = r$$

$$f(\alpha) = 0 \iff r = 0 \iff x - \alpha \mid f$$

□

4.4. Következmény. Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\text{Inko}(f, g)$ gyökei.

Bizonyítás.

$$f(\alpha) = 0 \text{ és } g(\alpha) = 0 \xrightarrow{B} x - \alpha \mid f \text{ és } x - \alpha \mid g$$

$$\iff x - \alpha \mid d$$

$$\iff d(\alpha) = 0$$

□

4.5. Következmény. Ha $f \in T[x]$ és $\alpha_1, \dots, \alpha_k \in T$ páronként különböző elemek, akkor

$$f(\alpha_1) = \dots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás. $\boxed{\Leftarrow}$ $f = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \cdot (\dots)$

$$f(\alpha_1) = \underbrace{(\alpha_1 - \alpha_1)}_0 \cdot \dots \cdot (\alpha_1 - \alpha_k) \cdot (\dots) = 0$$

$$\boxed{\Rightarrow} f(\alpha_1) = 0 \stackrel{B}{\Rightarrow} f = (x - \alpha_1) \cdot f_1$$

$$f(\alpha_2) = 0 \Rightarrow 0 = \underbrace{(\alpha_2 - \alpha_1)}_{\neq 0} \cdot \underbrace{f_1(\alpha_2)}_0 \stackrel{B}{\Rightarrow} f_1 = (x - \alpha_2) \cdot f_2$$

$$\Rightarrow f = (x - \alpha_1) \cdot (x - \alpha_2) \cdot f_2$$

$$f(\alpha_3) = 0 \Rightarrow 0 = \underbrace{(\alpha_3 - \alpha_1)}_{\neq 0} \cdot \underbrace{(\alpha_3 - \alpha_2)}_{\neq 0} \cdot \underbrace{f_2(\alpha_3)}_0 \stackrel{B}{\Rightarrow} f_2 = (x - \alpha_3) \cdot f_3 \quad \square$$

4.6. Következmény. Ha a **nemnulla** $f \in T[x]$ polinom fokszáma n , akkor legfeljebb n különböző gyöke van a T testben.

Bizonyítás. Legyen $\alpha_1, \alpha_2, \dots, \alpha_k$ az összes gyök f -vel.

$$(x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \mid f$$

$$\deg((x - \alpha_1) \cdot \dots \cdot (x - \alpha_k)) \leq \deg f$$

$$\begin{aligned} &\mathbb{Z}_8 \text{ nem test} \\ &f = x^2 - 1 \in \mathbb{Z}_8[x] \\ &\text{gyökei: } 1, 3, 5, 7 \end{aligned} \quad \square$$

4.7. Definíció. Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem **k -szoros gyöke**, ha

$$(x - \alpha)^k \mid f \text{ de } (x - \alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitásának** nevezzük.

4.8. Megjegyzés. Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

4.9. Feladat. Hányszoros gyöke $c = 2$ az $f = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8 \in \mathbb{R}[x]$ polinomnak?

$$(x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8) : (x - 2) = x^4 - 3x^3 + x^2 + 4$$

$$\begin{array}{r} x^5 - 2x^4 \\ \hline -3x^4 + 7x^3 - 2x^2 + 4x - 8 \end{array}$$

$$\begin{array}{r} -3x^4 + 6x^3 \\ \hline x^3 - 2x^2 + 4x - 8 \end{array}$$

$$\begin{array}{r} x^3 - 2x^2 + 4x - 8 \\ x^3 - 2x^2 \\ \hline 4x - 8 \end{array}$$

$$\begin{array}{r} 4x - 8 \\ 4x - 8 \\ \hline 0 \end{array}$$

$$4x - 8$$

$$4x - 8$$

$$0$$

$$f = (x - 2) \cdot \underbrace{(x^4 - 3x^3 + x^2 + 4)}_q + \underbrace{0}_{r = f(2)}$$

$$(x^4 - 3x^3 + x^2 + 4) = (x - 2) \cdot (\dots)$$

$$(1 \cdot x^5 - 5 \cdot x^4 + 7 \cdot x^3 - 2 \cdot x^2 + 4 \cdot x - 8) : (x - 2) = 1 \cdot x^4 - 3 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 4$$

$$\begin{array}{r} 1 \cdot x^5 - 2 \cdot 1 \cdot x^4 \\ \hline -3 \cdot x^4 + 7 \cdot x^3 - 2 \cdot x^2 + 4 \cdot x - 8 \\ -3 \cdot x^4 - 2 \cdot (-3) \cdot x^3 \\ \hline 1 \cdot x^3 - 2 \cdot x^2 + 4 \cdot x - 8 \\ 1 \cdot x^3 - 2 \cdot 1 \cdot x^2 \\ \hline 0 \cdot x^2 + 4 \cdot x - 8 \\ 0 \cdot x^2 - 2 \cdot 0 \cdot x \\ \hline 4 \cdot x - 8 \\ 4 \cdot x - 2 \cdot 4 \\ \hline 0 \end{array}$$

$-5 + 2 \cdot 1$ $7 + 2 \cdot (-3)$ $-2 + 2 \cdot 1$ $4 + 2 \cdot 0$

$$f = (x - 2) \cdot \underbrace{(1 \cdot x^4 - 3 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 4)}_q + \underbrace{0}_{r = f(2)}$$

	1	-5	7	-2	4	-8
2	1	-3	1	0	4	0

	...			...
C	...			...

HORNER - Schema

$$C \cdot \text{flower} + \text{tulip}$$

	1	-5	7	-2	4	-8
2	1	-3	1	0	4	0
2	1	-1	-1	-2		0
2	1	1	1			0
2	1	3	7			

$$f = (x-2) \cdot (1x^4 - 3x^3 + 1x^2 + 0x + 4)$$

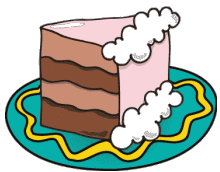
$$(x-2) \cdot (1x^3 - 1x^2 - 1x - 2)$$

$$f = (x-2)^2 \cdot (x^3 - x^2 - x - 2)$$

$$(x-2) \cdot (1x^2 + 1x + 1)$$

$$f = (x-2)^3 \cdot (x^2 + x + 1)$$

$c=2$ f-vel legnagyobb mérete



f mérete: $2, 2, 2, -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$

4.10. Feladat. Hányszoros gyöke $c = \bar{2}$ az $f = x^4 + 2x + \bar{3} \in \mathbb{Z}_5[x]$ polinomnak?

	1	0	0	2	3
2	1	2	4	0	3

 $f(\bar{2}) = \bar{3}$

$c = \bar{2}$ nem is gyöke f -nek!
(nullas+oszo gyök)

4.11. Feladat. Hányszoros gyöke $c = \bar{3}$ az $f = x^4 + 2x + \bar{3} \in \mathbb{Z}_5[x]$ polinomnak?

pp.

	1	0	0	2	3
3	1	3	4	4	0
3	1	1	2	0	
3	1	4	4		
3	1				
3	1				

$$f = (x-3) \cdot (x^3 + 3x^2 + 4x + 4)$$

$$= (x-3)^2 \cdot \underbrace{(x^2 + x + 2)}_g$$

$$g(3) = 4$$

$c = \bar{3}$ f -nek kétszeres gyöke