LÁNG CSABÁNÉ

POLINOMOK ALAPJAI

Példák és megoldások

Lektorálta Ócsai Katalin

ELTE IK Budapest
2008-11-08
2. javított kiadás

Tartalomjegyzék

1. Előszó

Elsősorban az ELTE Informatikai Kar programtervező informatikus, programtervező matematikus, programozó és informatika tanár szakos hallgatói számára készült ez a példatár, amely részletesen kidolgozott példákat tartalmaz.

A példák részben más könyvekből, példatárakból, mások által összeállított feladatsorokból származnak. Azok a források, amelyekről tudomásom van, szerepelnek az *Ajánlott irodalom* fejezetben. A feladatok más része pedig ebben a példatárban jelenik meg először.

A könyvben található hibákra, hiányosságokra vonatkozó észrevételeket köszönettel fogadom.

Budapest, 2008. november

Láng Csabáné

zslang@compalg.inf.elte.hu

ELTE Informatikai Kar Komputeralgebra Tanszék

1117 Budapest, Pázmány Péter sétány 1/C.

2. Példák

2.1. Gyűrűk-testek

2.1-1. Állapítsuk meg, hogy az alábbi halmazok gyűrűt, illetve testet alkotnak-e a szokásos műveletekre.

a. Az egész számok;

b. a racionális számok;

c. azok a valós számok, amelyeknek van valós 100-dik gyöke;

d. azok a komplex számok, amelyeknek van valós 100-dik gyöke;

e. azok a komplex számok, amelyeknek van komplex 100-dik gyöke;

f. a 2×2-es, valós elemű mátrixok;

g. a valós együtthatós polinomok.

Megoldás.

a. Gyürü;

b. Test;

c. Nem alkotnak sem gyűrűt, sem testet. Ezek ugyanis a nem negatív valós számok, nincs a halmazban az ellentettjük (kivéve a nullát).

d. Nem alkotnak sem gyűrűt, sem testet. Ugyanaz, mint a c.

e. Test. Mivel a komplex számok mindegyikéből vonható 100-adik gyök, az összes komplex számról van szó.

f. Gyűrű.

g. Gyűrű (euklideszi). ∎

2.1-2. A modulo m maradékosztályok mikor alkotnak testet a szokásos műveletekre?
Megoldás. Akkor és csak akkor, ha m prím. ∎

2.1-3. Melyek igazak az alábbi állítások közül?

a. Bármely testben $ab = ac,\ a \neq 0 \Rightarrow b = c$.

b. Bármely gyűrűben $ab = ac,\ a \neq 0 \Rightarrow b = c$.

c. Ha egy kommutatív, legalább két elemű gyűrűben $ab = ac,\ a \neq 0 \Rightarrow b = c$, akkor az test.

d. Véges, legalább két elemű kommutatív gyűrűben ha $ab = ac,\ a \neq 0 \Rightarrow b = c$, akkor az test.

Megoldás.

a. Igaz, mert testben nincs nullosztó.

b. Nem igaz, mert van olyan gyűrű, amelyikben van nullosztó. pl. $\mathbb{Z}_6$

c. Nem igaz, ellenpélda a $\mathbb{Z}$ a szokásos műveletekkel.

d. Igaz, mert véges integritási tartomány testet alkot. ∎

2.1-4. Melyek igazak az alábbi állítások közül?

a. Ha egy testben $d \neq 0$ és $c \cdot d = d$, akkor c egységelem.

b. Ha egy kommutatív gyűrűben $d \neq 0$ és $cd = d$, akkor c egységelem.

Megoldás.

a. Igaz.

b. Nem igaz, pl. $10 \cdot 4 \equiv 1 \cdot 4 \pmod{36}$, így $\mathbb{Z}_{36}$-ban $c = \overline{10}$, teljesíti a feltételeket, de nem egységelem. Másik ellenpélda: $7 \cdot 4 \equiv 1 \cdot 4 \pmod{8}$, így $\mathbb{Z}_8$-ban $c = \overline{7}$, teljesíti a feltételeket, de nem egységelem. ∎

2.2. Polinomok maradékos osztása $\mathbb{Q}$ és $\mathbb{Z}_p$ fölött

Polinomok maradékos osztása

Legyen R gyűrű, és tegyük fel, hogy $R[x]$-ben elvégezhető a maradékos osztás. Ez azt jelenti, hogy ha $a, b \in R[x], b \neq 0$, akkor létezik olyan $q, r \in R[x]$, melyre $a = bq + r$, ahol $\deg(r) < \deg(b)$.

Euklideszi gyűrűben elvégezhető a maradékos osztás. Test fölötti polinomok euklideszi gyűrűt alkotnak a fokszámfüggvénnyel, igy közöttük is mindig elvégezhető a maradékos osztás.

$\mathbb{Q}$ és $\mathbb{Z}_p$ testet alkotnak, így az alábbi példákban elvégezhető a maradékos osztás.

Megjegyzés. Polinomok esetén az osztást addig kell végezni, amíg a maradékpolinom nulla lesz, vagy pedig a fokszáma kisebb lesz, mint az osztó polinom fokszáma.

2.2-5. Legyen $f = x^5 + x^4 - 15x^3 + 25x^2 + 2x - 3$ és $g = x^2 + 4x - 5$. Végezzünk maradékos osztást az f és g polinomokkal

a. $\mathbb{Q}$ fölött,

b. $\mathbb{Z}_3$ fölött

Megoldás. a.

$$
\begin{array}{l}
(x^5 + x^4 - 15x^3 + 25x^2 + 2x - 3) : (x^2 + 4x - 5) = x^3 - 3x^2 + 2x + 2 \\
\underline{-(x^5 + 4x^4 - 5x^3)} \\
\qquad -3x^4 - 10x^3 \\
\qquad \underline{-(-3x^4 - 12x^3 + 15x^2)} \\
\qquad\qquad\qquad 2x^3 + 10x^2 \\
\qquad\qquad\qquad \underline{-(2x^3 + 8x^2 - 10x)} \\
\qquad\qquad\qquad\qquad 2x^2 + 12x - 3 \\
\qquad\qquad\qquad\qquad \underline{-(2x^2 + 8x - 10)} \\
\qquad\qquad\qquad\qquad\qquad 4x + 7
\end{array}
$$

A maradékos osztás eredménye:

$(x^5+x^4-15x^3+25x^2+2x-3) = (x^3-3x^2+2x+2)(x^2+4x-5)+(4x+7)$

b. Most $\mathbb{Z}_3$ fölött számolunk. Az alábbiakban a pl. $\overline{2}$ a 2 által reprezentált $\mathbb{Z}_3$-beli maradékosztályt jelenti. A műveleteket modulo 3 végezzük.

$$\begin{array}{l}
(x^5 + x^4 \qquad + x^2 + 2x) : (x^2 + x + 1) = x^3 + 2x + \overline{2} \\
\underline{-(x^5 + x^4 + x^3)} \\
\qquad\qquad 2x^3 + x^2 + 2x \\
\qquad\quad \underline{-(2x^3 + 2x^2 + 2x)} \\
\qquad\qquad\qquad 2x^2 \\
\qquad\qquad\qquad \underline{2x^2 + 2x + \overline{2}} \\
\qquad\qquad\qquad\qquad x + \overline{1}
\end{array}$$

Megjegyzés.

$\mathbb{Q}$ fölött a maradék $4x+7$, $\mathbb{Z}_3$ fölött pedig $x+\overline{1}$, de ha a $4x+7$-et is $\mathbb{Z}_3$ fölötti polinomnak tekintjük, szintén $x+\overline{1}$-et kapunk. Hasonló esetben eljárhatunk úgy is, hogy elvégezzük a maradékos osztást $\mathbb{Q}$ fölött, majd a hányados polinomot és a maradékpolinomot átírjuk $\mathbb{Z}_m$-be. Ha ellenben a feladatunk csupán $\mathbb{Z}_m$ felett végzendő maradékos osztás, általában kevesebbet kell számolnunk, ha azonnal $\mathbb{Z}_m$-ben számolunk, s így az együtthatókat modulo m vesszük. ∎

2.2-6. Hogy kell megválasztani a p, q, m értékeket, hogy az x^3+px+q polinom $\mathbb{C}$ fölött osztható legyen az x^2+mx-1 polinommal.

Megoldás. Az alábbiakban nem részletezzük a maradékos osztás lépéseit, csupán a hányados és a maradék polinomokat adjuk meg. Ha elvégezzük a maradékos osztást, a következőre jutunk.

$$\begin{array}{l}
(x^3 + \qquad\qquad\qquad px + q) : (x^2 + mx - 1) = (x - m) \\
\qquad (m^2 + p + 1)x + (q - m)
\end{array}$$

Így a maradékos osztás eredménye az alábbi.

$$(x^3 + px + q) = (x^2 + mx - 1) \cdot (x - m) + (m^2 + p + 1)x + (q - m)$$

A feltétel szerint a maradék a zérus polinom, tehát a maradékpolinom mindegyik együtthatója nulla, amiből a következő összefüggéseket kapjuk:

$$m^2 + p + 1 = 0 \qquad \text{és} \qquad q = m$$

Minden olyan p, q, m hármas megfelel, amelyik az előző két egyenletet kielégíti. ∎

2.2-7. Határozzuk meg az először megadott polinomnak a másodszorra megadott polinommal való osztásakor kapott maradékát $\mathbb{Q}$ fölött.

a. $2x^4 - 3x^3 + 4x^2 - 5x + 6, \quad x^2 - 3x + 1$

b. $x^3 - 3x^2 - x - 1, \quad 3x^2 - 2x + 1$

Megoldás. Az alábbiakban nem részletezzük a maradékos osztás lépéseit, csupán a hányados és a maradék polinomokat adjuk meg.

a.

$$\begin{aligned}&(2x^4 - 3x^3 + 4x^2 - 5x + 6) : (x^2 - 3x + 1) = 2x^2 + 3x + 11\\ &\qquad\qquad 25x - 5\end{aligned}$$

b.

$$\begin{aligned}&(x^3 - 3x^2 - x - 1) : (3x^2 - 2x + 1) = \frac{1}{3}x - \frac{7}{9}\\ &\qquad -\frac{26}{9}x - \frac{2}{9}\end{aligned}$$

∎

2.2-8. Hogyan kell megválasztani p, q, m értékét, hogy az $x^4 + px + q$ polinom osztható legyen az $x^2 + mx + 1$ polinommal $\mathbb{Q}$ fölött.

Megoldás.

$$\begin{array}{l}
(x^4+px+q):(x^2+mx+1)=x^2-mx+m^2-1\\
\underline{x^4+mx^3+x^2}\\
\quad -mx^3-x^2+px+q\\
\underline{-(-mx^3-m^2x^2-mx)}\\
\qquad (m^2-1)x^2+(p+m)x+q\\
\qquad \underline{-((m^2-1)x^2+m(m^2-1)x+m^2-1)}\\
\qquad\qquad (p+2m-m^3)x+q-m^2+1
\end{array}$$

A feltétel szerint a maradék a zérus polinom, tehát a maradékpolinom mindegyik együtthatója nulla, amiből a következő összefüggéseket kapjuk:

$$p+2m-m^3=0 \quad \text{és} \quad q-m^2+1=0$$

Minden olyan p, q, m hármas megfelel, amelyik az előző két egyenletet kielégíti. ∎

2.3. Legnagyobb közös osztó euklideszi algoritmussal és lineáris kombináció; közös gyök

Euklideszi algoritmus

Tegyük fel, hogy R gyűrű és $R[x]$-ben elvégezhető a maradékos osztás. Legyen $a, b \in R[x], b \neq 0$. A maradékos osztást végezzük el a két rögzített polinomra. Ha a maradék nem nulla, akkor az osztót a maradékkal osszuk el maradékosan. Ezt mindaddig ismételjük, amíg nulla maradékot nem kapunk. Így az euklideszi algoritmushoz jutunk. (Euklidész Kr. e. 300 körül élt görög matematikus.)

$$\begin{array}{rll}
a=bq_0+r_0, & \text{ha } r_0\neq 0, \text{ akkor} & \deg r_0<\deg b;\\
b=r_0q_1+r_1, & \text{ha } r_1\neq 0, \text{ akkor} & \deg r_1<\deg r_0;\\
r_0=r_1q_2+r_2, & \text{ha } r_2\neq 0, \text{ akkor} & \deg r_2<\deg r_1;\\
\vdots & \vdots & \vdots\\
r_{n-2}=r_{n-1}q_n+r_n, & \text{ha } r_n\neq 0, \text{ akkor} & \deg r_n<\deg r_{n-1};\\
r_{n-1}=r_nq_{n+1} & &
\end{array} \tag{I}$$

Ez az eljárás minden esetben véges lesz, mert deg r_0, deg r_1, ..., deg r_n nem negatív egészek szigorúan csökkenő sorozata.

Tétel. Ha $b|a$, akkor $(a,b)=b$. Ha $b\nmid a$, akkor az a,b polinomokkal végzett euklideszi algoritmus utolsó nem nulla maradéka az a és b legnagyobb közös osztója. Ha $(a,b)=d$, akkor léteznek olyan x és y $R[x]$-beli polinomok, melyekkel $ax+by=d$. (Más szóval d-t elő lehet állítani a és b lineáris kombinációjaként, ahol az együtthatók $R[x]$-beli polinomok.)

Megjegyzés. Ha valamely d polinom legnagyobb közös osztó, akkor minden asszociáltja is az. Asszociáltat kapunk, ha $R[x]$-beli egységgel szorozzuk a polinomot. (Integritási tartományban az egységek az egységelem osztói.)

A tételben szereplő lineáris kombinációt a következő módon készíthetünk. Sorban előállítjuk r_0, r_1, ..., r_n-et a és b lineáris kombinációjaként, felhasználva az euklideszi algoritmus számításait. Először r_0-at kifejezzük (I) első egyenletéből,

$$r_0 = a - bq_0.$$

Azután a másodikból kifejezzük r_1-et, és r_0 előállítását beírjuk. Rendezés után r_1 előállítását kapjuk meg a és b lineáris kombinációjaként.

$$r_1 = b - r_0q_1 = b - (a - bq_0)q_1 = b(1 + q_0q_1) - aq_1$$

Az i-edik lépésben az i-edik egyenletből kifejezzük r_i-t, majd a benne szereplő r_{i-1} és r_{i-2} helyére írjuk be a korábban kapott lineáris kombinációt, stb. (Lásd a 11. példát.)

Megjegyzés. Végtelen sok x, y $R[x]$-beli polinompár van, amelyekkel elő lehet állítani a legnagyobb közös osztót.

2.3-9.

a. Keressük meg az 5. feladatban szereplő polinomok legnagyobb közös osztóját $\mathbb{Q}$ fölött. Van-e közös racionális gyökük?

b. Keressük meg a polinomok legnagyobb közös osztóját $\mathbb{Z}_3$ fölött.

Megoldás. Euklideszi algoritmust végzünk.

a. Az 5. feladatban az $f = x^5+x^4-15x^3+25x^2+2x-3$ és $g = x^2+4x-5$ polinomok szerepeltek, a maradékos osztás eredménye $\mathbb{Q}$ fölött az alábbi volt:

$$(x^5+x^4-15x^3+25x^2+2x-3) = (x^3-3x^2+2x+2)(x^2+4x-5)+(4x+7)$$

Most az előbbi osztóval és a maradékkal végezzük a maradékos osztást.

$$\begin{array}{l} \quad (x^2+4x-5):(4x+7) = \dfrac{1}{4}x + \dfrac{9}{16} \\ \underline{-(x^2+\frac{7}{4}x)} \\ \qquad\quad \frac{9}{4}x-5 \\ \qquad \underline{-(\frac{9}{4}x+\frac{63}{16})} \\ \qquad\qquad -\frac{143}{16} \end{array}$$

Most a $(4x+7)$ polinomot kell $-\dfrac{143}{16}$-tal maradékosan osztani. Az osztó konstans polinom, a vele való osztáskor a maradék nulla.

Az f és a g polinomok legnagyobb közös osztója az utolsó nem nulla maradék.

$$(f,g) = -\tfrac{143}{16}$$

Ha van a polinomoknak közös gyökük, akkor ez a gyök gyöke a legnagyobb közös osztónak is. Mivel azonban a legnagyobb közös osztó nem nulla konstans polinom, nincs gyöke, így az f és g polinomoknak nincs közös gyökük.

1. megjegyzés. Akkor és csak akkor van két polinomnak közös gyöke, ha a legnagyobb közös osztó legalább elsőfokú polinom.

2. megjegyzés. Ebben a példában a legnagyobb közös osztó $-\dfrac{143}{16}$, és ennek minden asszociáltja is az. Test esetén a nulla kivételével bármelyik konstans egység, bármelyik két nem nulla konstans egymás asszociáltja, például esetünkben az 1 is legnagyobb közös osztó.

$$-\frac{143}{16} \approx 1$$

b. $\mathbb{Z}_3$ fölött a maradékos osztás eredménye az 5. példában az alábbi volt:

$$x^5+x^4+x^2+2x = (x^3+2x+\overline{2})(x^2+x+\overline{1}) + (x+\overline{1})$$

Az euklideszi algoritmus következő lépéseként az előbbi osztóval és a maradékkal végzünk maradékos osztást.

$$\begin{array}{l} \quad (x^2+x+\overline{1}):(x+\overline{1}) = x \\ \underline{-(x^2+x)\qquad} \\ \qquad\qquad \overline{1} \end{array}$$

Most az $(x + \overline{1})$ polinomot kell $\overline{1}$-gyel maradékosan osztani. Az osztáskor a maradék nulla.

Az f és a g polinomok legnagyobb közös osztója az utolsó nem nulla maradék.

$$(f, g) = \overline{1}$$

A legnagyobb közös osztó nem nulla konstans polinom, nincs gyöke, így az f és g polinomoknak sincs közös gyökük $\mathbb{Z}_3$ fölött. ∎

2.3-10. Van-e az alábbi polinomoknak közös gyökük $\mathbb{C}$ fölött? (Határozzuk meg a következő polinomok legnagyobb közös osztóját euklideszi algoritmussal.)

$$f = x^4 + x^3 - 3x^2 - 4x - 1, \quad g = x^3 + x^2 - x - 1$$

Megoldás. Az alábbiakban csak az osztót és a maradékot jelöljük, a közbülső számításokat nem.

$$(x^4 + x^3 + 3x^2 - 4x - 1) : (x^3 + x^2 - x - 1) = x$$
$$-2x^2 - 3x - 1$$

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

$$(-2x^2 - 3x - 1) : (-\frac{3}{4}x - \frac{3}{4}) = \frac{8}{3}x + \frac{4}{3}$$
$$0$$

A legnagyobb közös osztó az utolsó nem nulla maradék.

$$(f, g) = -\frac{3}{4}x - \frac{3}{4} \approx x + 1$$

Az $x + 1$ polinom gyöke $x = -1$ a közös gyök. ∎

2.3-11. Bizonyítsuk be, hogy az alábbi f és g $\mathbb{Q}$ fölötti polinomok legnagyobb közös osztója 1. Határozzunk meg olyan u és v polinomokat, amelyekre $1 = fu + gv$. (Lineáris kombinációs előállítás.)

a. $f(x) = 3x^3 - 2x^2 + x + 2,\qquad g(x) = x^2 - x + 1;$

b. $f(x) = x^4 - x^3 - 4x^2 + 4x + 1,\quad g(x) = x^2 - x + 1$

Megoldás.

a.

$$
\begin{array}{l}
\ (3x^3 - 2x^2 + x + 2) : (x^2 - x + 1) = 3x + 1 \\
\underline{-(3x^3 - 3x^2 + 3x)} \\
\qquad\qquad\quad x^2 - 2x + 2 \\
\qquad\quad \underline{-(x^2 - x + 1)} \\
\qquad\qquad\qquad -x + 1
\end{array}
$$

$$
\begin{array}{l}
\ (x^2 - x + 1) : (-x + 1) = -x \\
\underline{-(x^2 - x)\qquad} \\
\qquad\qquad\quad 1
\end{array}
$$

A következő maradékos osztásnál a maradék nulla, az utolsó nem nulla maradék az 1, így a legnagyobb közös osztó valóban az 1.

$$(f, g) = 1$$

Most sorban kiszámítjuk a lineáris kombinációs együtthatókat.

Az euklideszi algoritmus eredménye	a maradék lineáris kombinációs előállítása
$f = g(3x + 1) + (-x + 1)$	$(-x + 1) = f - g(3x + 1)$
$g = (-x + 1)(-x) + 1$	$1 = g - (-x + 1)(-x) =$ $= g - (f - g(3x + 1))(-x) =$ $= g(1 + (3x + 1)(-x)) + f \cdot (x) =$ $= g(-3x^2 - x + 1) + f \cdot (x)$

A lineáris kombinációhoz az együttható polinomok:

$$u = x \qquad v = -3x^2 - x + 1$$

b.

$$
\begin{array}{l}
(x^4 - x^3 - 4x^2 + 4x + 1) : (x^2 - x + 1) = x^2 - 5 \\
\underline{-(x^4 - x^3 + x^2)} \\
\qquad -5x^2 + 4x + 1 \\
\qquad \underline{-(-5x^2 + 5x - 5)} \\
\qquad\qquad -x + 6
\end{array}
$$

$$
\begin{array}{l}
(x^2 - x + 1) : (-x + 6) = -x - 5 \\
\underline{-(x^2 - 6x)} \\
\qquad 5x + 1 \\
\qquad \underline{-(5x - 30)} \\
\qquad\qquad 31
\end{array}
$$

A következő maradékos osztásnál a maradék nulla, az utolsó nem nulla maradék az 1, így a legnagyobb közös osztó 31, ami az 1 asszociáltja $\mathbb{Q}$ fölött.

$$(f, g) = 31 \approx 1$$

Most sorban kiszámítjuk a lineáris kombinációs együtthatókat.

Az euklideszi algoritmus eredménye	a maradék lineáris kombinációs előállítása
$f = g(x^2 - 5) + (-x + 6)$	$(-x + 6) = f - g(x^2 - 5)$
$g = (-x + 6)(-x - 5) + 31$	$31 = g + (-x + 6)(x + 5) =$ $= g + (f - g(x^2 - 5))(x + 5) =$ $= g(1 - (x^2 - 5)(x + 5)) + f \cdot (x + 5) =$ $= g(-x^3 - 5x^2 + 5x + 26) + f \cdot (x + 5)$

Az 1=fu+gv lineáris kombinációhoz az együttható polinomok:

$$u = \frac{1}{31}(x + 5) \qquad v = \frac{1}{31}(-x^3 - 5x^2 + 5x + 26)$$

■

2.4. Horner-elrendezés

Legyen f valamilyen R gyűrű fölötti polinom:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0$$

Legyen $\alpha \in R$, és tegyük fel, hogy az f α helyen vett helyettesítési értékét akarjuk kiszámítani. Nézzük az alábbi átalakítást.

$$\begin{aligned} f(\alpha) &= a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_{n-2}\alpha^{n-2} + \ldots + a_1\alpha + a_0 = \\ &= (\ldots(((a_n\alpha + a_{n-1})\alpha + a_{n-2})\alpha + a_{n-3})\alpha + a_{n-4}\ldots)\alpha + a_0 \end{aligned}$$

Ha a legbelső zárójelben lévő számítást végezzük el, majd kifelé haladunk, könnyen előállítható rekurzív számításokat végzünk, s végeredményként általában sokkal kevesebb számítással megkapjuk f értékét az α helyen, mintha egyszerűen csak behelyettesítenénk.

Az alábbi táblázatban való elrendezés (a Horner-elrendezés), könnyen követhetővé teszi a számítást.

	a_n	a_{n-1}	a_{n-2}	a_{n-3}	$\ldots$	a_1	a_0	$f(\alpha)$
α		$b_{n-1} =$ $= a_n$	$b_{n-2} =$ $= a_n\alpha + a_{n-1}$ $= b_{n-1}\alpha + a_{n-1}$	$b_{n-3} =$ $= b_{n-2}\alpha + a_{n-2}$	$\ldots$	b_1	$b_0 =$ $= b_1\alpha + a_1$	$b_0\alpha + a_0$

A második sorban a_{n-1} oszlopába a_n-et írunk, a többi oszlopba, a_{n-i-1} oszlopába pedig a $b_{n-i}\alpha + a_{n-i}$ érték kerül.

2.4-12. Keressük meg az $f(x) = x^4 - 3x^3 + x + 6$ polinom helyettesítési értékét a $3,\ -1,\ 2,\ -2$ helyeken.

Megoldás.

α	1	-3	0	1	6	$f(\alpha)$
3		1	0	0	1	$9 = f(3)$
-1		1	-4	4	-3	$9 = f(-1)$
2		1	-1	-2	-3	$0 = f(2)$
-2		1	-5	10	-19	$44 = f(-2)$

■

2.4-13. Határozzuk meg a következő polinomok osztási maradékát. Oldjuk meg a feladatot maradékos osztással és Horner-elrendezéssel is.

a. $x^4 - 2x^3 + 4x^2 - 6x + 8$ osztva $x - 1$-gyel,

b. $2x^5 - 5x^3 - 8$ osztva $x + 3$-mal,

c. $4x^3 + x^2$ osztva $x + 1 + i$-vel,

d. $x^3 - x^2 - x$ osztva $x - 1 + 2i$-vel.

Megoldás.

Az alábbiakban csak Horner-elrendezéssel végezzük el a számításokat. Aki kiszámítja maradékos osztással is, meggyőződhet arról, hogy a Horner-elrendezéses megoldás kevésbé számításigényes.

Tegyük fel, hogy valamilyen f polinomot maradékosan osztunk egy $x - \alpha$ polinommal:

$$f = g(x - \alpha) + r, \text{ ahol } \deg r < \deg(x - \alpha) = 1$$

Ebből látható, hogy r nulla, vagy nulladfokú polinom. Vegyük az előbbi egyenletet az α helyen.

$$f(\alpha) = r(\alpha)$$

Mivel r konstans, minden helyen ugyanaz az értéke. Ha tehát kiszámítjuk $f(\alpha)$-t, megkapjuk a maradékot. Ezt pedig Horner elrendezéssel könnyen kiszámíthatjuk.

a. Kiszámítjuk f értékét az 1 helyen.

α	1	-2	4	-6	8	$f(\alpha)$
1		1	-1	3	-3	$5 = f(1)$

A maradék $r = 5$.

b. Kiszámítjuk f értékét a -3 helyen.

α	2	0	-5	0	0	-8	$f(\alpha)$
-3		2	-6	13	-39	117	$-359 = f(-3)$

A maradék $r = -359$.

c. Kiszámítjuk f értékét a $-1 - i$ helyen.

α	4	1	0	0	$f(\alpha)$
$-1 - i$		4	$-3 - 4i$	$-1 + 7i$	$8 - 6i$

A maradék $r = 8 - 6i$.

d. Kiszámítjuk f értékét az $1-2i$ helyen.

α	1	-1	-1	0	$f(\alpha)$
$1-2i$		1	$-2i$	$-5-2i$	$-9+8i$

A maradék $r=-9+8i$. ■

2.4-14. Határozzuk meg p értékét úgy, hogy az $f(x)=x^5+3x^4+5x+p$ polinom osztható legyen $x-2$-vel. Oldjuk meg a feladatot maradékos osztással és Horner-elrendezéssel is.

Megoldás.

A megoldás Horner-elrendezéssel:

	1	3	0	0	5	p	$f(2)$
2		1	5	10	20	45	$90+p$

A maradék nulla kell legyen, $90+p=0$, amiből $p=-90$. ■

A hányados polinom együtthatói a Horner elrendezés során keletkező számok

$$(a_nx^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x+a_0):(x-\alpha)=$$

$$=a_nx^{n-1}+(a_n\alpha+a_{n-1})x^{n-2}+((a_n\alpha+a_{n-1})\alpha+a_{n-2})x^{n-3}+\ldots$$

$$\underline{a_nx^n-a_nx^{n-1}\alpha}$$

$$(a_n\alpha+a_{n-1})x^{n-1}+\ldots$$

$$\underline{(a_n\alpha+a_{n-1})x^{n-1}-(a_n\alpha+a_{n-1})\alpha x^{n-2}}$$

$$((a_n\alpha+a_{n-1})\alpha+a_{n-2})x^{n-2}$$

$$\vdots$$

2.5. Többszörös gyök keresése f és f' legnagyobb közös osztójával

2.5-15. Határozzuk meg az a paramétert úgy, hogy az $x^5 - ax^2 - ax + 1$ polinomnak -1 legalább kétszeres gyöke legyen. Oldjuk meg a feladatot

a. maradékos osztással,

b. Horner-elrendezéssel,

c. a derivált polinom felhasználásával.

Megoldás.

a. Az $(x+1)^2 = x^2 + 2x + 1$ polinommal kell maradékosan osztani. A maradék a zérus polinom, tehát mindegyik együttható nulla. Ebből kapjuk az a paraméter lehetséges értékét.

b. Horner elrendezéssel kiszámítjuk f-et a -1 helyen, és a kapott hányadospolinomot (f_1-et) szintén a -1 helyen. Mindkét érték nulla kell legyen.

	1	0	0	$-a$	$-a$	1	$f(\alpha) \mid f_1(\alpha)$
-1		1	-1	1	$-1-a$	1	0
-1			1	-2	3	$-4-a$	$5+a$

Látjuk, hogy az első maradék mindenképpen nulla. A második maradék esetén $5 + a = 0$, amiből $a = -5$.

c. Bebizonyítható, hogy ha egy R integritási tartomány fölötti polinomnak $c \in R$ n-szeres gyöke, akkor a deriváltjának c legalább $n-1$-szeres gyöke. Ha char(R)=0, akkor a deriváltnak c pontosan $n-1$-szeres gyöke.

Megjegyzés. $c \in R$ n-szeres gyöke az f polinomnak, ha $(x-c)^n | f$, de $(x-c)^{n+1} \nmid f$.

Erre támaszkodva Horner elrendezéssel kiszámítjuk f-et a -1 helyen, és a deriváltat szintén a -1 helyen. Mindkét érték nulla kell legyen.

	1	0	0	$-a$	$-a$	1	$f(\alpha)$
-1		1	-1	1	$-1-a$	1	0

$f' = 5x^4 - 2ax - a$

	5	0	0	$-2a$	$-a$	$f'(\alpha)$
-1		5	-5	5	$-5-2a$	$5+a$

Megint nulla az első maradék, $5+a$ a második. $5+a=0$, s így $a=-5$.

Megjegyzés. Ebben a példában a értékétől függetlenül a -1 gyöke a polinomnak. Általában nem ez a helyzet, s így nem elég azt biztosítanunk, hogy a kívánt elem gyöke legyen a polinom deriváltjának, hanem azt is biztosítanunk kell, hogy a kívánt elem gyöke legyen magának a polinomnak is. ∎

2.5-16. Határozzuk meg az a, b paraméterek értékét úgy, hogy $ax^4 + bx^3 + 1$ osztható legyen $(x-1)^2$-nel.

Megoldás.

1. megoldás. Horner elrendezéssel kiszámítjuk f-et az 1 helyen, és a kapott hányadospolinomot (f_1-et) szintén az 1 helyen. Mindkét érték nulla kell legyen.

	a	b	0	0	1	$f(\alpha)\vert f_1(\alpha)$
1		a	$a+b$	$a+b$	$a+b$	$a+b+1$
1			a	$2a+b$	$3a+2b$	$4a+3b$

Az $a+b+1=0$ és $4a+3b=0$ egyenletekből álló egyenletrendszert kell megoldanunk.

A megoldás: $a=3$ és $b=-4$.

2. megoldás. Horner elrendezéssel kiszámítjuk f-et az 1 helyen, és a deriváltat szintén az 1 helyen. Mindkét érték nulla kell legyen.

$f(1) = a+b+1$ (Lásd az előző megoldásban.)

$f' = 4ax^3 + 3bx^2$

	$4a$	$3b$	0	0	$f'(\alpha)$
1		$4a$	$4a+3b$	$4a+3b$	$4a+3b$

Megint az $a+b+1=0$ és $4a+3b=0$ egyenletekből álló egyenletrendszert kaptuk, aminek a megoldása $a=3$ és $b=-4$. ■

2.5-17. Határozzuk meg a következő polinomok és deriváltjaik legnagyobb közös osztóját:

a. $f(x)=(x-1)^3(x+1)^2(x-3) \qquad f\in\mathbb{Z}[x]$

b. $f(x)=(x-1)(x^2-1)(x^3-1)(x^4-1) \qquad f\in\mathbb{Z}[x]$

Megoldás.

a. A polinomnak háromszoros gyöke az 1, a deriváltnak tehát kétszeres gyöke. A polinomnak kétszeres gyöke a -1, így a deriváltnak egyszeres gyöke. Más közös gyöke a polinomnak és a deriváltjának nincs, így
$\text{lnko}(f,f')=(x-1)^2(x+1)$

b.

$$f(x)=(x-1)(x-1)(x+1)(x-1)(x^2+x+1)(x-1)(x+1)(x^2+1)=$$
$$=(x-1)^4(x+1)^2(x^2+x+1)(x^2+1)$$

A polinomnak négyszeres gyöke az 1, a deriváltnak tehát háromszoros gyöke. A polinomnak kétszeres gyöke a -1, így a deriváltnak egyszeres gyöke. Más közös gyöke a polinomnak és a deriváltjának nincs, így

$\text{lnko}(f,f')=(x-1)^3(x+1)$ ■

2.5-18. Van-e többszörös gyöke az $f(x)=x^5-5x^3+5x+2$ polinomnak $\mathbb{C}$ fölött?

Megoldás. Ha a polinom és deriváltjának közös osztója legalább elsőfokú, akkor van közös gyökük, s így a polinomnak van többszörös gyöke. Számítsuk ki euklideszi algoritmussal $\text{lnko}(f,f')$-t.

$$f(x)=x^5-5x^3+5x+2 \qquad f'(x)=5x^4-15x^2+5$$

$$\begin{array}{l}
\quad(x^5-5x^3+5x+2):(5x^4-15x^2+5)=\frac{1}{5}x\\
\underline{-(x^5-3x^3+x)\qquad\quad}\\
\qquad\quad -2x^3+4x+2
\end{array}$$

$$\begin{array}{l} \quad (5x^4 - 15x^2 + 5) : (-2x^3 + 4x + 2) = -\frac{5}{2}x \\ \underline{-(5x^4 - 10x^2 - 5x)} \\ \qquad\qquad -5x^2 + 5x + 5 \end{array}$$

$$\begin{array}{l} \quad (-2x^3 + 4x + 2) : (-5x^2 + 5x + 5) = \frac{2}{5}x + \frac{2}{5} \\ \underline{-(-2x^3 + 2x^2 + 2x)} \\ \quad (-2x^2 + 2x + 2) \\ \underline{-(-2x^2 + 2x + 2)} \\ \qquad\qquad\qquad 0 \end{array}$$

$\mathrm{lnko}(f, f') = -5x^2 + 5x + 5$ A polinom és deriváltjának legnagyobb közös osztója másodfokú, így van f-nek többszörös gyöke. Keressük meg a legnagyobb közös osztó gyökeit.

$$-5x^2 + 5x + 5 = 0$$

$$x^2 - x - 1 = 0$$

$$x_{1,2} = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

A polinomnak kétszeres gyöke az $\frac{1+\sqrt{5}}{2}$, valamint az $\frac{1-\sqrt{5}}{2}$. ■

2.5-19. Bizonyítsuk be, hogy egy, a racionális test felett irreducibilis polinomnak a komplex számok körében sem lehet többszörös gyöke.

Megoldás. Legyen $d = \mathrm{lnko}(f, f')$. $d|f$ és $\deg d < \deg f$, így az irreducibilitás miatt d csak konstans lehet. ■

2.6. Racionális és egész együtthatós polinomok racionális és egész gyökei; polinomok felbontása

2.6-20. Legyen $f(x)$ egész együtthatós polinom. Bizonyítsuk be, hogy ha $f(0)$

és $f(1)$ páratlan, akkor az $f(x)$ polinomnak nincs zérushelye az egész számok körében.

Megoldás. Legyen $f(x) = a_0 + a_1x + ... + a_nx^n$.

1. *megoldás.*

Tudjuk, hogy $f(0)$ páratlan, ami miatt a_0 is páratlan. Másrészt $f(1)$ páratlan, emiatt $\sum_{i=0}^{n} a_i$ is páratlan. Ezekből következik, hogy $\sum_{i=1}^{n} a_i$ páros.

a. Legyen α páros egész, és vegyük az $f(\alpha)$ értékét. $\sum_{i=1}^{n} a_i\alpha^i$ páros, amihez hozzáadva a_0 értékét, páratlan számot kapunk. α nem lehet a polinom gyöke, mert ehhez $f(\alpha) = 0$ kellene legyen, és a 0 páros szám.

b. Legyen most α páratlan egész, és vegyük az $f(\alpha)$ értékét.

Határozzuk meg $\sum_{i=1}^{n} a_i\alpha^i$ paritását.

$$\sum_{i=1}^{n} a_i\alpha^i = (a_1\alpha) + (a_2\alpha^2) + \ldots + (a_n\alpha^n) =$$

$$= (\alpha + \alpha + \ldots + \alpha) + (\alpha^2 + \alpha^2 + \ldots + \alpha^2) + \ldots + (\alpha^n + \alpha^n + \ldots + \alpha^n)$$

Ebben a felírásban az i. zárójelben a_i darab páratlan szám áll, összesen tehát a kifejezésben $\sum_{i=1}^{n} a_i$ darab páratlan szám szerepel. Mivel páros sok páratlan szám összege páros, így $\sum_{i=1}^{n} a_i\alpha^i$ páros. Ehhez pedig hozzáadva a_0 értékét, páratlan számot kapunk. Ez az α sem lehet a polinom gyöke.

Tehát a polinomnak nincs gyöke az egész számok körében.

2. *megoldás.*

Ha $\alpha \in \mathbb{Z}$ gyöke lenne a polinomnak, akkor $f(x) = (x-\alpha)g(x)$ lenne valamilyen egész együtthatós g polinommal. Helyettesítsünk ebbe az egyenletbe 0-t, majd 1-et.

$$f(0) = (0 - \alpha)g(0) \qquad f(1) = (1 - \alpha)g(1)$$

α párosságától függően $(0 - \alpha)$ vagy $(1 - \alpha)$ páros kell legyen, de akkor vagy $f(0)$ vagy $f(1)$ lenne páros a feltétellel ellentétben. ∎

2.6-21. Irreducibilisek-e (felbonthatatlanok-e) az alábbi polinomok?

a. $x^2 - 2$ $\quad \mathbb{Q}$ fölött, $\mathbb{R}$ fölött,

b. $x^2 - 1$ tetszőleges test fölött,

c. $x^2 + 1$ $\mathbb{Q}$, $\mathbb{R}$ fölött, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_2$ fölött,

d. x^2 és $x^2 + x$ $\mathbb{F}_2$ fölött.

Megjegyzés. Másod, vagy harmadfokú f polinom irreducibilitását vizsgálva, elegendő megnéznünk, hogy van-e gyöke a polinomnak az adott R gyűrű, vagy test fölött.

i. Ha ugyanis van f-nek valamilyen c gyöke, akkor $x - c$ leválasztható a polinomról.

$$f = (x - c)g,$$

ahol g is R fölötti polinom.

ii. Fordítva, ha f felbontható, akkor az elsőfokú faktora meghatároz egy gyököt. Ha azonban f negyed- vagy magasabb fokú, lehet, hogy nincs gyöke, mégis felbontható legalább másodfokú irreducibilis polinomok szorzatára.

Megoldás.

a. $x^2 - 2$ $\mathbb{Q}$ fölött irreducibilis, $\mathbb{R}$ fölött nem,
b. $x^2 - 1$ minden test fölött felbontható két elsőfokú polinom szorzatára,
c. $x^2 + 1$ semelyik valós testben nem bontható fel,
$\mathbb{F}_3$ fölött nem bontható fel,
$\mathbb{F}_5$ fölött $x^2 + \overline{1} = x^2 - \overline{4} = (x + \overline{2})(x - \overline{2})$, tehát felbontható,
$\mathbb{F}_2$ fölött $x^2 + \overline{1} = (x + \overline{1})^2$, tehát felbontható,
d. x^2 és $x^2 + x$ $\mathbb{F}_2$ fölött felbontható, hiszen az x mindkettőből kiemelhető.

■

2.6-22. Lássuk be, hogy ha az egész együtthatós f polinomnak gyöke a $\dfrac{p}{q}$ racionális szám, $p, q \in \mathbb{Z}$, $(p, q) = 1$, akkor p osztója a konstans tagnak, q osztója a főegyütthatónak.

Megoldás. Legyen

$$f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n, \quad f\left(\frac{p}{q}\right) = 0, \quad p, q \in \mathbb{Z}, \quad (p, q) = 1.$$

Ha belyettesítjük f-be $\dfrac{p}{q}$-t, nullát kapunk.

$$f\left(\frac{p}{q}\right) = a_0 + a_1\frac{p}{q} + ... + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + a_n\left(\frac{p}{q}\right)^n = 0$$

Szorozzuk végig az egyenletet q^n-nel.

$$a_0q^n + a_1pq^{n-1} + ... + a_{n-1}p^{n-1}q + a_np^n = 0 \qquad (*)$$

Ebből

$$a_0q^n + a_1pq^{n-1} + ... + a_{n-1}p^{n-1}q = -a_np^n$$

A bal oldalnak osztója q – hiszen minden tagban szerepel – így osztója a jobb oldalnak is.

$$q| - a_np^n$$

$(p,q) = 1$ miatt $q|a_n$, amivel beláttuk az állítás egyik részét.

Most rendezzük (*)-ot másként.

$$a_1pq^{n-1} + ... + a_{n-1}p^{n-1}q + a_np^n = -a_0q^n$$

A bal oldalnak osztója p, így osztója a jobb oldalnak is.

$$p| - a_0q^n$$

$(p,q) = 1$ miatt $p|a_0$ is fennáll. ■

2.6-23. Lássuk be, hogy ha $c \in \mathbb{Z}$ gyöke az $f(x) \in \mathbb{Z}[x]$ polinomnak, akkor

$$1 - c\left|\sum_{i=0}^{n} a_i \qquad \text{és} \qquad 1 + c\right|\sum_{i=0}^{n}(-1)^i a_i$$

Megoldás. Mivel c gyöke f-nek, $f(x) = (x-c)q(x)$ valamilyen egész együtthatós q polinommal. Helyettesítsünk az egyenletbe 1-et:

$$f(1) = (1-c)q(1)$$

Ebből $(1-c)|f(1)$, másrészt $f(1)=\sum_{i=0}^{n} a_i$, tehát

$$1-c \left| \sum_{i=0}^{n} a_i \right. .$$

Helyettesítsünk most az egyenletbe -1-et:

$$f(-1)=-(1+c)q(-1)$$

Ebből $(1+c)|f(-1)$, azonban $f(-1)=\sum_{i=0}^{n}(-1)^i a_i$, s így valóban

$$1+c \left| \sum_{i=0}^{n} (-1)^i a_i \right. .$$

■

2.6-24. Keressük meg az $f(x)=x^3-6x^2+15x-14$ polinom racionális gyökeit.

Megoldás. A 22. példa szerint, ha $\frac{p}{q}$ $(p,\ q\in\mathbb{Z},\ (p,\ q)=1)$ gyöke az egész együtthatós polinomnak, akkor $p|14$ és $q|1$. A polinom lehetséges gyökei $\pm1, \pm2, \pm7, \pm14$. Horner-elrendezéssel megvizsgálhatjuk, hogy ezek közül melyik gyök valóban.

Mivel a lehetséges gyökök mind egészek, alkalmazhatjuk a 23. példát is. Az alábbi táblázatban megvizsgáljuk, hogy a 23. példa feltételei melyik c egész számra teljesülnek. Egyedül a 2 marad meg, mint lehetséges gyök. Horner-elrendezéssel kiszámítjuk $f(2)$-t, és 0-t kapunk. A polinom egyetlen racionális gyöke a 2.

? $1+c\| - 36$	? $1-c\| - 4$	c	1	-6	15	-14	$f(c)$
2	0	1		1	-5	10	-4
0	2	-1		1	-7	22	-36
3	-1	2		1	-4	7	0
-1	3	-2		1	-8	31	-76
8	-6	7		1	1	22	140
-6	8	-7		1	-13	106	-756
15	-13	14		1	8	127	1764
-13	15	-14		1	-20	295	-4144

■

2.6-25. Keressük meg az $f(x) = x^5 - 4x^4 - 6x^3 + 16x^2 + 29x + 12$ polinom racionális gyökeit.

Megoldás. A 22. példa szerint, ha $\frac{p}{q}$ $(p,\ q \in \mathbb{Z},\ (p,\ q) = 1)$ gyöke az egész együtthatós polinomnak, akkor $p|12$ és $q|1$. A polinom lehetséges gyökei $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$. Horner-elrendezéssel megvizsgálhatjuk, hogy ezek közül melyik gyök valóban. Ha valamelyik c szám gyök, akkor ezt a gyököt a Horner-elrendezésben előálló hányados polinomba is behelyettesítjük, és a továbbiakban ezzel a hányadospolinommal dolgozunk.

	1	-4	-6	16	29	12	$f(c)$
1		1	-3	-9	7	36	48
-1		1	-5	-1	17	12	0
-1			1	-6	5	12	0
-1				1	-7	12	0
-1					1	-8	20
2					1	-5	2
-2					1	-9	30
3					1	-4	0
4						1	0

Az f polinom gyökei $-1,\ 3,\ 4$. A -1 háromszoros gyök, így

$f(x) = (x+1)^3(x-3)(x-4)$. ■

2.6-26. Mik az
$$f(x) = \frac{5}{4}x^3 - \frac{15}{2}x^2 + \frac{55}{4}x - \frac{15}{2}$$
polinom racionális gyökei?

Megoldás. Az együtthatók nevezőinek legkisebb közös többszörösével (4-gyel) megszorozzuk az f-et, s az így kapott polinomnak ugyanazok a gyökei, mint f-nek. (f-nek az egyik assszociáltját állítjuk elő $\mathbb{Q}$ fölött.)

$$4 \cdot f = f_1 = 5x^3 - 30x^2 + 55x - 30$$

Most az együtthatók legnagyobb közös osztójával osztunk, és az így kapott polinomnak szintén ugyanazok a gyökei, mint f-nek.

$$\frac{1}{5} \cdot f_1 = x^3 - 6x^2 + 11x - 6$$

Ennek a polinomnak az együtthatói relatív prímek egymáshoz.

Ha $\frac{p}{q}$ $(p,\ q \in \mathbb{Z},\ (p,\ q) = 1)$ gyöke ennek az egész együtthatós polinomnak, akkor $p|6$ és $q|1$. (Lásd 22. példa.)A polinom lehetséges gyökei $\pm1, \pm2, \pm3, \pm6$. Horner-elrendezéssel megvizsgálhatjuk, hogy ezek közül melyik gyök valóban. Ha valamelyik c szám gyök, akkor ezt a gyököt a Horner-elrendezésben előálló hányados polinomba is behelyettesítjük, és a továbbiakban ezzel a hányados-polinommal dolgozunk.

	1	-6	11	-6	$f(c)$
1		1	-5	6	0
1			1	-4	2
-1			1	-6	12
2			1	-3	0
3				1	0

Az f polinom gyökei $1,\ 2,\ 3$. Így $f(x) = (x-1)(x-2)(x-3)$ ■

2.6-27. Mik az $f(x) = x^3 + x^2 - 5x + 3$ polinom racionális gyökei?

Megoldás. Ha $\dfrac{p}{q}$ $(p,\ q \in \mathbb{Z},\ (p,\ q) = 1)$ gyöke ennek az egész együtthatós polinomnak, akkor $p|3$ és $q|1$. (Lásd 22. példa.)A polinom lehetséges gyökei $\pm 1,\ \pm 3$. Horner-elrendezéssel megvizsgálhatjuk, hogy ezek közül melyik gyök valóban. Ha valamelyik c szám gyök, akkor ezt a gyököt a Horner-elrendezésben előálló hányados polinomba is behelyettesítjük, és a továbbiakban ezzel a hányadospolinommal dolgozunk.

	1	1	-5	3	$f(c)$
1		1	2	-3	0
1			1	3	0
-3				1	0

Az f polinom gyökei $1,\ -3$. Az 1 kétszeres gyök, így $f(x) = (x-1)^2(x+3)$.

■

2.6-28. Adjuk meg az összes olyan c egész számot, amelyre a

$$81x^{100} + c \cdot x^{65} + 64 = 0$$

egyenletnek van racionális gyöke.

Megoldás. Legyen $\dfrac{p}{q}$ $p,\ q \in \mathbb{Z},\ \ (p,\ q) = 1$ gyöke az egyenletnek, ekkor

$$81\left(\frac{p}{q}\right)^{100} + c \cdot \left(\frac{p}{q}\right)^{65} + 64 = 0$$

Szorozzuk végig az egyenletet q^{100}-nal.

$$81p^{100} + c \cdot p^{65}q^{35} + 64q^{100} = 0$$

Rendezzük az egyenletet.

$$81p^{100} + c \cdot p^{65}q^{35} = -64q^{100}$$

Mivel a bal oldalnak osztója p^{65}, osztója a jobb oldalnak is.

$$p^{65} | -64q^{100}$$

$(p,\ q) = 1$ miatt $p^{65}|64$, amiből $p = \pm 1$.

Most másként rendezzük az egyenletet.

$$c \cdot p^{65}q^{35} + 64q^{100} = -81p^{100}$$

Mivel a bal oldalnak osztója q^{35}, osztója a jobb oldalnak is.

$$q^{35}| - 81p^{100}$$

$(p,\ q) = 1$ miatt $q^{35}|81$, amiből $q = \pm 1$.

Ha tehát van racionális gyöke az egyenletnek, akkor az csak 1 vagy -1 lehet. Nézzük meg, hogy ezek a számok lehetnek-e gyökök.

$f(1) = 81 + c + 64 = 0$ teljesül, ha $c = -145$. $f(-1) = 81 - c + 64 = 0$ pedig akkor teljesül, ha $c = 145$. A keresett értékek tehát $c = \pm 145$. ■

2.6-29. Bizonyítsuk be, hogy ha k és n pozitív egészek, és $\sqrt[k]{n}$ nem egész, akkor $\sqrt[k]{n}$ irracionális.

Megoldás. Legyen $\alpha = \sqrt[k]{n}$. Ebből $\alpha^k = n$, tehát α gyöke az

$$x^k - n$$

egyenletnek. Azonban ennek az egyenletnek minden racionális gyöke egész (lásd a 22. példa állítását), s így $\sqrt[k]{n}$ irracionális. ■

2.6.1. Gauss-tétel és Schönemann–Eisenstein tétel.

Gauss-tétel. Ha valamely f egész együtthatós polinom felbontható racionális együtthatós polinomok szorzatára, akkor felbontható egész együtthatós polinomok szorzatára is. Ha tehát

$$f(x) = g(x) \cdot h(x),$$

$f \in Z[x]$, $g, h \in Q[x]$, $1 \leq \deg g < \deg f$ és $1 \leq \deg h < \deg f$, akkor léteznek $G,\ H \in Z[x]$, $\deg G = \deg g$, $\deg H = \deg h$ polinomok, amelyekkel

$$f(x) = G(x) \cdot H(x).$$

Schönemann–Eisenstein tétel. Legyen $f(x) = a_0 + a_1x + \ldots + a_nx^n$, $f(x) \in \mathbb{Z}[x]$. Ha létezik p prím, amelyre

(i) $p \not| a_n$,

(ii) $p | a_i \quad (i = 0, \ \ldots, \ n-1)$,

(iii) $p^2 \not| a_0$,

akkor $f(x)$ felbonthatatlan $\mathbb{Z}$ fölött.

Megjegyzés. Ha egy egész együtthatós polinom felbonthatatlan $\mathbb{Z}$ fölött, akkor a Gauss-tétel következményeként $\mathbb{Q}$ fölött is felbonthatatlan.

Megjegyzés. A feltétel nem szükséges. Ha nem alkalmazható a tétel, akkor még lehet, hogy a polinom irreducibilis.

2.6-30. Bizonyítsuk be, hogy minden $n \in \mathbb{N}$ esetén létezik $f(x) \in \mathbb{Q}[x]$ n-edfokú irreducibilis polinom.

Megoldás. Elég az egész együtthatós polinomokat vizsgálni. Például

$$x^n - p$$

$p = 2$, vagy tetszőleges más prím esetén irreducibilis $\mathbb{Z}$ fölött a Schönemann–Eisenstein tétel szerint, a Gauss-tétel következményeként pedig $\mathbb{Q}$ fölött is felbonthatatlan. ■

2.6-31. Az $f(x) = 3x^5 + 2x^3 - 12x^2 + 10x + 14$ polinomot bontsuk fel irreducibilis polinomok szorzatára $\mathbb{Z}$ és $\mathbb{Q}$ fölött.

Megoldás. A $p = 2$ választással alkalmazhatjuk a Schönemann–Eisenstein tételt.

(i) $2 \not| a_n = 3$,

(ii) $2|2, \ 2|12, \ 2|10, \ 2|14$,

(iii) $2^2 = 4 \not| a_0 = 14$.

Így f irreducibilis $\mathbb{Z}$ fölött, a Gauss-tétel következményeként pedig $\mathbb{Q}$ fölött is felbonthatatlan. ■

2.6-32. Az $f(x) = 20x^4 + 26x^3 + 65x^2 + 91$ polinomot bontsuk fel irreducibilis polinomok szorzatára $\mathbb{Z}$ és $\mathbb{Q}$ fölött.

Megoldás. A $p = 13$ választással alkalmazhatjuk a Schönemann–Eisenstein tételt.

(i) $13 \not| a_n = 20$,

(ii) $13|26,\ 13|65,\ 13|91$,

(iii) $13^2 = 169 \not| a_0 = 91$.

Így f felbonthatatlan $\mathbb{Z}$ fölött, a Gauss-tétel következményeként pedig $\mathbb{Q}$ fölött is felbonthatatlan. ∎

2.6-33. Mik az $f(x) = 40x^4 + 45x + 15$ polinom racionális gyökei?

Megoldás.

1. *megoldás.* Megvizsgálhatjuk, hogy az összes olyan $\dfrac{p}{q}$, $p,\ q \in \mathbb{Z}$, $(p,\ q) = 1$ szám, amelyre $p|15$, $q|40$, gyöke-e a polinomnak.

2. *megoldás.* Ebben az esetben hamarabb célhoz érünk, ha belátjuk, hogy ez a polinom $\mathbb{Q}$ felett irreducibilis. A $p = 3$ választással alkalmazhatjuk a Schönemann–Eisenstein tételt.

(i) $3 \not| a_n = 40$,

(ii) $3|45,\ 13|15$,

(iii) $3^2 = 9 \not| a_0 = 15$.

Így f felbonthatatlan $\mathbb{Z}$ fölött, a Gauss-tétel következményeként pedig $\mathbb{Q}$ fölött is felbonthatatlan. Ekkor azonban nem lehet racionális gyöke. Ha ugyanis valamilyen $\alpha \in \mathbb{Q}$ gyöke lenne az f-nek, akkor az $(x - \alpha)$ tényező leválasztható lenne f-ből. $f = (x - \alpha)q(x)$ lenne valamilyen q racionális polinommal, s így f nem lenne irreducibilis.

Megjegyzés. Beláttuk, hogy az 1-nél magasabb fokú egész együtthatós polinom irreducibilis $\mathbb{Q}$ fölött, s ebből az következik, hogy nincs racionális gyöke. Fordítva nem igaz a dolog. Ha egy legalább negyedfokú racionális együtthatós polinomnak nincs racionális gyöke, nem biztos, hogy felbonthatatlan. ■

2.7. Polinomok felbontása $\mathbb{C}$ és $\mathbb{R}$ fölött

Megjegyzés. $\mathbb{C}$ fölött minden legalább elsőfokú polinom elsőfokú tényezők szorzatára bontható, ami Gauss egyik tételéből következik. Ha egy valós együtthatós polinomnak c nem valós komplex gyöke, akkor $\overline{c}$ is gyöke, és $(x-c)(x-\overline{c})$ valós együtthatós másodfokú polinom.

$$(x-c)(x-\overline{c}) = x^2 - (c+\overline{c})x + c\overline{c} = x^2 - 2\mathrm{Re}(c)x + |c|^2$$

Felhasználva a $\mathbb{C}$ fölötti gyöktényezős felbontást, és a megfelelő polinomokat összeszorozva megkapjuk az $\mathbb{R}$ fölötti előállítást irreducibilis polinomok szorzataként.

2.7-34. Bontsuk fel az x^4+1 polinomot irreducibilis polinomok szorzatára

a. $\mathbb{C}$ fölött,

b. $\mathbb{R}$ fölött.

Megoldás.

a. $\mathbb{C}$ fölött az $x^4 = -1$ egyenletet kell megoldanunk, tehát -1-ből negyedik gyököt kell vonnunk. Tudjuk a komplex számokkal való tanulmányainkból, hogy négy negyedik gyök van, s ezek:

$$\cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2}(1+i) \qquad \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = \frac{\sqrt{2}}{2}(-1+i)$$

$$\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = \frac{\sqrt{2}}{2}(-1-i) \qquad \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4} = \frac{\sqrt{2}}{2}(1-i)$$

Tehát a felbontás az alábbi:

$$x^4+1 =$$

$$= \left(x - \frac{\sqrt{2}}{2}(1+i)\right)\left(x - \frac{\sqrt{2}}{2}(-1+i)\right)\left(x - \frac{\sqrt{2}}{2}(-1-i)\right)\left(x - \frac{\sqrt{2}}{2}(1-i)\right)$$

b.

$$x^4+1=$$

$$=\left(\left(x-\frac{\sqrt{2}}{2}(1+i)\right)\left(x-\frac{\sqrt{2}}{2}(1-i)\right)\right)\cdot$$

$$\cdot\left(\left(x-\frac{\sqrt{2}}{2}(-1+i)\right)\left(x-\frac{\sqrt{2}}{2}(-1-i)\right)\right)=$$

$$=\left(x^2-\sqrt{2}x+1\right)\left(x^2+\sqrt{2}x+1\right)$$

■

2.7-35. Bontsuk fel $\mathbb{R}$ felett irreducibilis polinomok szorzatára az x^6+27 polinomot.

Megoldás. $\mathbb{C}$ fölött az $x^6=-27$ egyenletet kell megoldanunk, tehát -27-ből hatodik gyököt kell vonnunk. Tudjuk a komplex számokkal való tanulmányainkból, hogy hat hatodik gyök van, s ezek

$$z_1=\sqrt{3}\left(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}\right),$$

$$z_2=\sqrt{3}\left(\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}\right),$$

$$z_3=\sqrt{3}\left(\cos\frac{5\pi}{6}+i\sin\frac{5\pi}{6}\right),$$

valamint ezeknek a konjugáltjai. A polinom felbontása $\mathbb{C}$ fölött:

$$x^6+27=(x-z_1)(x-\overline{z_1})(x-z_2)(x-\overline{z_2})(x-z_3)(x-\overline{z_3})$$

$$z_1+\overline{z_1}=2\sqrt{3}\cos\frac{\pi}{6}=2\sqrt{3}\frac{\sqrt{3}}{2}=3 \qquad z_1\overline{z_1}=3$$

$$z_2+\overline{z_2}=0 \qquad z_2\overline{z_2}=3$$

$$z_3+\overline{z_3}=2\sqrt{3}\cos\frac{5\pi}{6}=2\sqrt{3}\frac{-\sqrt{3}}{2}=-3 \qquad z_3\overline{z_3}=3$$

A gyöktényezős előállítás összetartozó párjait összeszorozva megkapjuk az $\mathbb{R}$ fölötti előállítást.

$$x^6+27=((x-z_1)(x-\overline{z_1}))\,((x-z_2)(x-\overline{z_2}))\,((x-z_3)(x-\overline{z_3}))=$$

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

■

2.7-36. Bontsuk fel $\mathbb{R}$ felett irreducibilis polinomok szorzatára az x^4+4 polinomot.

Megoldás. $\mathbb{C}$ fölött az $x^4=-4$ egyenletet kell megoldanunk, tehát -4-ből negyedik gyököt kell vonnunk. Tudjuk a komplex számokkal való tanulmányainkból, hogy négy negyedik gyök van, s ezek

$$z_1=\sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right)=\sqrt{2}\left(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)=1+i,$$

$$z_2=\sqrt{2}\left(\cos\frac{3\pi}{4}+i\sin\frac{3\pi}{4}\right)=\sqrt{2}\left(-\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)=-1+i,$$

valamint ezeknek a konjugáltjai. A polinom felbontása $\mathbb{C}$ fölött:

$$x^4+4=(x-z_1)(x-\overline{z_1})(x-z_2)(x-\overline{z_2})$$

$$z_1+\overline{z_1}=2 \qquad z_1\overline{z_1}=2$$

$$z_2+\overline{z_2}=-2 \qquad z_2\overline{z_2}=2$$

A A gyöktényezős előállítás összetartozó párjait összeszorozva megkapjuk az $\mathbb{R}$ fölötti előállítást.

$$x^4+4=((x-z_1)(x-\overline{z_1}))\,((x-z_2)(x-\overline{z_2}))=$$

$$=(x^2-2x+2)(x^2+2x+2)$$

■

2.8. Gyökök és együtthatók közötti összefüggés

Vieta formulák

Legyen R egységelemes integritási tartomány, és tegyük fel, hogy az

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in R[x]$

n-edfokú polinom – multiplicitással együtt vett – n gyöke mind R-ben van. Legyenek ezek a gyökök $c_1,\ c_2,\ \ldots,\ c_n$. Ekkor

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = \\ &= a_n (x - c_1)(x - c_2) \cdots (x - c_n) = \\ &= a_n \big(x^n - (c_1 + c_2 + \ldots + c_n) x^{n-1} + \\ &\quad +(c_1 \cdot c_2 + c_1 \cdot c_3 + \ldots + c_{n-1} \cdot c_n) x^{n-2} + \\ &\vdots \\ &\quad +(-1)^n (c_1 \cdot c_2 \cdots c_n) \big) \end{aligned}$$

amiből

$$\begin{aligned} \frac{a_{n-1}}{a_n} &= -(c_1 + c_2 + \ldots + c_n) \\ \frac{a_{n-2}}{a_n} &= (c_1 \cdot c_2 + c_1 \cdot c_3 + \ldots + c_{n-1} \cdot c_n) \\ &\vdots \\ \frac{a_0}{a_n} &= (-1)^n (c_1 \cdot c_2 \cdots c_n) \end{aligned}$$

2.8-37. Határozzuk meg a d paraméter értékét a Vieta-formulák felhasználásával, ha a $2x^3 - x^2 - 7x + d = 0$ egyenlet két gyökének összege 1.

Megoldás. Legyenek a gyökök $c_1,\ c_2,\ c_3$. A feltétel szerint $c_1 + c_2 = 1$, a Vieta-formulákból $c_1 + c_2 + c_3 = -\frac{a_{n-1}}{a_n} = -\frac{a_2}{a_3} = \frac{1}{2}$. Ebből $c_3 = -\frac{1}{2}$.

Számítsuk ki az $f = 2x^3 - x^2 - 7x + d$ polinom helyettesítési értékét a $-\frac{1}{2}$ helyen.

	2	-1	-7	d	$f(c)$
$-\frac{1}{2}$		2	-2	-6	$d+3$

Mivel $-\frac{1}{2}$ gyök, $d+3=0$, amiből $d=-3$. ∎

2.8-38. Számtani sorozat egymás utáni három eleme-e a

$$8x^3 - 12x^2 - 2x + 3 = 0$$

egyenlet három gyöke? Alkalmazzuk a Vieta-formulákat.

Megoldás. Írjuk fel a három gyököt számtani sorozat egymás utáni három elemeként.

$$a-d,\ a,\ a+d$$

A három gyök összege

$$a-d+a+a+d = -\frac{a_{n-1}}{a_n} = -\frac{a_2}{a_3} = \frac{12}{8},$$

amiből $3a = \frac{12}{8}, \quad a = \frac{1}{2}$. A három gyök szorzata

$$(a-d)a(a+d) = -\frac{a_0}{a_n} = -\frac{a_0}{a_3} = -\frac{3}{8},$$

$a = \frac{1}{2}$ felhasználásával:

$$\left(\frac{1}{2}-d\right)\frac{1}{2}\left(\frac{1}{2}+d\right) = -\frac{3}{8}$$

amiből

$$\frac{1}{4} - d^2 = -\frac{3}{4}, \quad d^2 = 1, \quad d = \pm 1.$$

Ha $d=1$, akkor $a-d=-0.5, \quad a=0.5, \quad a+d=1.5$ a három gyök. Behelyettesítéssel meggyőződhetünk arról, hogy ezek valóban gyökei az egyenletnek. A $d=-1$ választással ugyanezeket a gyököket kapjuk fordított sorrendben. Tehát az egyenlet három gyöke számtani sorozat egymás utáni három eleme. ∎

2.8-39. Számítsuk ki az $x^3 + 2x - 3 = 0$ egyenlet gyökeinek négyzetösszegét a Vieta-formulák felhasználásával.

Megoldás. Legyenek a gyökök $c_1,\ c_2,\ c_3$. A Vieta-formulákból

$$c_1 + c_2 + c_3 = 0 \qquad c_1c_2 + c_1c_3 + c_2c_3 = 2 \qquad c_1c_2c_3 = 3$$

Nézzük a következő összefüggést:

$$(c_1 + c_2 + c_3)^2 = c_1^2 + c_2^2 + c_3^2 + 2(c_1c_2 + c_1c_3 + c_2c_3)$$

Behelyettesítve az ismert értékeket:

$$0 = c_1^2 + c_2^2 + c_3^2 + 2 \cdot 2$$

Ebből

$$c_1^2 + c_2^2 + c_3^2 = -4.$$

■

2.8-40. Számítsuk ki az $x^5 - 5x^3 + 5x + 2$ polinom gyökeinek négyzetösszegét a Vieta-formulák alkalmazásával.

Megoldás. Legyenek a gyökök $c_1,\ c_2,\ c_3,\ c_4,\ c_5$. A Vieta-formulákból

$$c_1 + c_2 + c_3 + c_4 + c_5 = 0 \qquad c_1c_2 + c_1c_3 + c_2c_3 + \ldots + c_4c_5 = -5$$

Nézzük a következő összefüggést:

$$(c_1 + c_2 + c_3 + c_4 + c_5)^2 = c_1^2 + c_2^2 + c_3^2 + c_4^2 + c_5^2 + 2(c_1c_2 + c_1c_3 + c_2c_3 + \ldots + c_4c_5)$$

Behelyettesítve az ismert értékeket:

$$0 = c_1^2 + c_2^2 + c_3^2 + c_4^2 + c_5^2 + 2 \cdot (-5)$$

Ebből

$$c_1^2 + c_2^2 + c_3^2 + c_4^2 + c_5^2 = 10.$$

■

3. Ajánlott irodalom

Bagyinszkiné Orosz Anna – Csörgő Piroska – Gyapjas Ferenc:
Példatár a bevezető fejezetek a matematikába c. tárgyhoz
Tankönyvkiadó, Budapest, 1983.
Dringó László – Kátai Imre: *Bevezetés a matematikába*
Tankönyvkiadó, Budapest, 1982
Freud Róbert: *Lineáris algebra.*
ELTE Eötvös Kiadó, Budapest, 1996
Gonda János: *Bevezető fejezetek a matematikába III.*
ELTE TTK, Budapest, 1998
Gonda János: *Gyakorlatok és feladatok a Bevezetés a matematikába c. tárgyhoz Polinomok, véges testek, kongruenciák, kódolás*
ELTE TTK, Budapest, 2001
Gonda János: *Polinomok, Példák és megoldások*
ELTE IK Digitális könyvtár, Budapest, 2007
Járai Antal: *Bevezetés a matematikába*
ELTE Eötvös Kiadó, 2005
Láng Csabáné: *Bevezető fejezetek a matematikába II.*
ELTE Budapest, 2000.
Surányi László: *Algebra. Testek, gyűrűk, polinomok.*
Typotex Kiadó, 1997