5. feladatsor: megoldások
$\mathbb{Z}[x]$ számelmélete. Körosztási polinomok

1. *Osszuk el maradékosan az $x^4 + x^2 + 3x - 2$ polinomot az $x^2 - x + 1$ polinommal.*

Megoldás. A feladat azt várja tőlünk, hogy az $f(x) = x^4 + x^2 + 3x - 2$ és a $g(x) = x^2 - x + 1$ polinomhoz keressünk olyan $q(x)$ és $r(x)$ polinomokat, melyekkel:

$$f(x) = q(x)g(x) + r(x)$$

és itt $r(x)$ foka kisebb mint $g(x)$ foka, vagy $r(x) = 0$. Ezt nevezzük maradékos osztásnak; $f(x)$ az osztandó, $g(x)$ az osztó, $q(x)$ a hányadospolinom, $r(x)$ pedig a maradék. A maradékos osztás test fölötti polinomok esetén (illetve gyűrű fölötti polinomok között is abban az esetben, ha az osztó főegyütthatója egység) mindig elvégezhető. Maradékos osztásnál az (elvégezhetőség indukciós bizonyítását követve) mindig a polinomok főtagjait osztjuk el egymással, majd a kapott hányadossal beszorozzuk az osztópolinomot, s a szorzatot kivonjuk az eredeti polinomból; ezután a különbséggel folytatjuk az eljárást az eredeti osztandó helyett. Az alábbi táblázat mutatja az osztás folyamatát:

$$\begin{array}{rrrrrrrrrrl}
 & (\mathbf{x^4} & & + & \mathbf{x^2} & + & \mathbf{3x} & - & \mathbf{2}) & : & (\mathbf{x^2} - \mathbf{x} + \mathbf{1}) = \mathbf{x^2} + \mathbf{x} + \mathbf{1} \\
- & (x^4 & - \; x^3 & + & x^2) & & & & & & \\
\hline
 & & x^3 & & & + & 3x & - & 2 & & \\
 & - & (x^3 & - & x^2 & + & x) & & & & \\
\hline
 & & & & x^2 & + & 2x & - & 2 & & \\
 & & & - & (x^2 & - & x & + & 1) & & \\
\hline
 & & & & & & \mathbf{3x} & - & \mathbf{3} & &
\end{array}$$

A számolás tehát azt mutatja, hogy a hányadospolinom $q(x) = x^2 + x + 1$, a maradék pedig $r(x) = 3x - 3$.

2. **a)** *Hogyan lehet egyszerűen megállapítani, hogy egy $\mathbb{Z}_2$ fölötti polinomnak van-e gyöke?*
b) *Keressük meg $\mathbb{Z}_2[x]$-ben a legfeljebb harmadfokú irreducibilis polinomokat.*

Megoldás. a) A nulla pontosan akkor gyök, ha a konstans tag 0, az 1 pedig pontosan akkor gyök, ha páros sok nem nulla (azaz 1-es) együttható van.
b) A konstans polinomok alapértelmezés szerint nem irreducibilisek, mert $\mathbb{Z}_2$ test, és itt minden nem nulla konstans invertálható, azaz egység, az irreducibilisek definíciója pedig eleve úgy szól, hogy *„egy nullától és egységtől különböző polinom pontosan akkor irreducibilis. . . ”* (Valójában, persze, csupán egyetlen nem nulla konstans polinom van $\mathbb{Z}_2[x]$-ben. Ettől függetlenül a megjegyzés hasznos lehet más testek fölöttt.) Test fölötti polinomok esetében az elsőfokúak irreducibilisek, mert nem lehet őket alacsonyabb fokú tényezők szorzatára bontani (a tényezők alacsonyabb foka biztosítja ugyanis, hogy egyik se lehessen egység), így irreducibilis lesz x és $x + 1$. (Az n-edfokú polinomok száma 2^n, mert a főegyütthatót nem nullának választva már csak a maradék n együtthatót kell kiválasztani 0 és 1 közül.) A másodfokúak esetén pontosan azok lesznek irreducibilisek, amelyeknek nincs gyöke (test fölött: gyök = elsőfokú tényező), azaz – az a) rész alapján – ha a konstans tag 1 és páratlan sok nem nulla tagja van. Ilyenből egy van: $x^2 + x + 1$. A harmadfokúak közül is pontosan a „gyöktelenek" lesznek irreducibilisek (nem triviális fölbontás esetén ugyanis lenne nekik 1-fokú tényezőjük), és az előző rész kritériumát ismételten alkalmazva ezek: $x^3 + x + 1$ és $x^3 + x^2 + 1$. A legföljebb harmadfokú irreducibils polinomok halmaza tehát:

$$\left\{x, x + 1, x^2 + x + 1, x^3 + x + 1, x^3 + x^2 + 1\right\}.$$

3. **a)** *Legyen $f(x) = 2x^3 + 3x^2 + 1 \in \mathbb{Z}_7[x]$. Írjuk fel az $f(x + 6)$ polinomot.*
b) *Legyen R kommutatív, egységelemes, nullosztómentes gyűrű, $f \in R[x]$, $c \in R$. Mutassuk meg, hogy f pontosan akkor irreducibilis R fölött, ha az $f(x + c)$ polinom irreducibilis.*

Megoldás. a) $f(x + 6) = 2(x + 6)^3 + 3(x + 6)^2 + 1 = 2(x^3 + 18x^2 + 108x + 216) + 3(x^2 + 12x + 36) + 1 = 2x^3 + 39x^2 + 252x + 541$.
b) Vegyük először észre, hogy a behelyettesítés szorzattartó, azaz ha $f(x) = g(x)h(x)$ teljesül, akkor $f(x + c) = g(x + c)h(x + c)$. (Figyelem: itt használjuk az alapgyűrű kommutativitását.) Másrészt ha $p(x + c) = q(x)$, akkor $(p(x) = q(x - c)$, tehát az új polinomból a régit ugyanilyen típusú behelyettesítéssel kaphatjuk vissza. Ez azt jelenti, hogy elegendő megmutatni az ekvivalencia egyik irányát. Ehhez tegyük föl, hogy $f(x) = g(x)h(x)$. Az előbb mondottak szerint $f(x + c) = g(x + c)h(x + c)$. Azt kell csak igazolnunk, hogy ha az első fölbontás nem triviális, akkor a másik sem az. De az egységek $R[x]$-ben az R gyűrű invertálható elemei, tehát konstans polinomok. Márpedig azt könnyű látni, hogy $p(x)$ és $p(x + c)$ foka megegyezik, tehát akkor és csak akkor lehet egység az egyik polinom, pl. $g(x)$, ha invertálható konstans, s ekkor ugyanez igaz $g(x + c)$-re is. Ez azt jelenti, hogy ha a $g(x)h(x)$ szorzat nem triviális fölbontása az $f(x)$-nek, akkor nem triviális fölbontását adja az $f(x + c)$ polinomnak a $g(x + c)h(x + c)$ fölbontás is.

4. *Bontsuk fel az x^4+1 és az x^4+4 polinomokat $\mathbb{Z}$ fölött irreducibilis polinomok szorzatára.*

Megoldás. Az x^4+1 polinom a 8-adik körosztási polinom, $\Phi_8(x)$, és mint ilyen, irreducubilis a kimondott (de nem bizonyított) tétel szerint. Ennek a konkrét polinomnak az irreducibilitását azonban bizonyíthatjuk a $\Phi_p(x)$-re alkalmazott módszerrel is, azaz nézzük az eltolt polinomot, $\Phi_8(x+1)$-et: $\Phi_8(x+1) = (x+1)^4+1 = (x^4+4x^3+6x^2+4x+1)+1 = x^4+4x^3+6x^2+4x+2$. Erre pedig alkalmazhatjuk a Schönemann–Eisenstein-kritériumot, ami bizonyítja, hogy x^4+1 irreducibilis $\mathbb{Q}[x]$-ben. Mivel primitív polinomról van szó, ezért az irreducibilitás önnáll $\mathbb{Z}[x]$-ben is (az egész együtthatós irredicibilis polinomok klasszifikációjából adódóan). (*Másik megoldás:* Az x^4+1 polinomnak ismerjük a komplex gyöktényezős fölbontását: gyökei a primitív 8-adik egységgyökök, azaz az egységkörön az a négy komplex szám, ε_1, …, ε_4, amelynek argumentuma 45°, 135°, 225°, 315°. Ez azt jelenti, hogy $x^4+1 = (x-\varepsilon_1)\cdots(x-\varepsilon_4)$. Mivel $\mathbb{C}[x]$ fölött igaz a számelmélet alaptétele, bármely $\mathbb{Q}[x]$-beli vagy $\mathbb{Z}[x]$-beli fölbontás lényegében ebből adódik a tényezők $2+2$-es csoportosításából (hiszen a gyökök nem raconálisak, sőt nem is valósak). Az egymáshoz konjugált gyökök összepárosításával kapunk is egy valós fölbontást: $x^4+1 = x^4+2x^2+1-2x^2 = (x^2-\sqrt{2}x+1)(x^2+\sqrt{2}x+1)$, ez azonban nem $\mathbb{Q}[x]$-beli fölbontás, így $\mathbb{Q}[x]$-ben még ezt a két tényezőt is össze kell szoroznunk, hogy racionális (egész) együtthatós fölbontást kapjunk. Azaz, az eredeti polinom irreducibilis $\mathbb{Q}[x]$-ben és $\mathbb{Z}[x]$-ben. – A másik polinom nem irreducibilis, ahogy az alábbi egyszerű trükk mutat egy fölbontást: $x^4+4 = x^4+4x^2+4-4x^2 = (x^2+2)^2-(2x)^2 = (x^2-2x+2)(x^2+2x+2)$. Mivel ennél a fölbontásnál egyik tényezőnek sincs racionális gyöke (pl. racionális gyökteszt vagy a másodfokú egyenlet megoldóképlete alapján), ezért a faktorok itt irreducibilisek $\mathbb{Q}[x]$-ben, és mivel primitívek is, ezért $\mathbb{Z}[x]$-ben is irreducibilisek lesznek.

5. *Igazoljuk, hogy az x^4+x^2+x+1 polinom irreducibilis $\mathbb{Q}$ fölött.*

Megoldás. *Első megoldás:* Ha a $f(x) = x^4+x^2+x+1$ polinom reducibilis lenne $\mathbb{Q}[x]$-ben, akkor a második Gauss-lemma alapján fölbomlana két alacsonyabb fokú egész együtthatós polinom szorzatára is: $f(x) = g(x)h(x)$. Mivel a racionális gyökteszt alapján a polinomnak nincs racionális gyöke (csak ±1 lehetne, azok közül viszont egyik sem gyök), ezért nem lehet elsőfokú faktora. Ha tehát szorzatra bomlana, akkor csak két másodfokú polinom szorzatára bomolhatna. Mivel az f polinom főegyütthatója 1, ezért g és h főegyütthatója is csak ±1 lehet (egyszerre $+1$ vagy egyszerre -1). Mivel szükség esetén mindkettőt szorozhatnánk -1-gyel, ezért föltehető, hogy mindkét faktor főegyütthatója 1, továbbá a konstans tag vizsgálatából azt kapjuk, hogy mindkét tényező konstans tagja $+1$ vagy mindkettő -1. (Mivel a főegyütthatót rögzítettük, ezért most már nem válaszhatjuk meg szabadon a konstans tagot: mindkét esetet vizsgálnunk kell.) Ez tehát azt jelenti, hogy:

$$f(x) = x^4+x^2+x+1 = (x^2+ax+1)(x^2+bx+1) \qquad \text{vagy} \qquad f(x) = x^4+x^2+x+1 = (x^2+cx-1)(x^2+dx-1).$$

Ha a beszorzásokat elvégezzük, láthatjuk, hogy a köbös tag csak úgy eshet ki, ha $b=-a$, illetve $d=-c$, ugyanakkor viszont ez esetben az x-es tag együtthatója is 0 lenne, ami ellentmondás. *Második megoldás:* Ha $f(x) = g(x)h(x)$ fölbontás $\mathbb{Z}[x]$-ben, akkor nézzük ezt a fölbontást $\mathbb{Z}_3[x]$-ben is: $\bar{f} = \bar{g}\cdot\bar{h}$. Nyilván egyik tényező főegyütthatója sem osztható 3-mal mert f normált, és így $\bar{g}$ és $\bar{h}$ ugyanolyan fokúak, mint g, ill. h. De $\bar{f}$-nak nincs gyöke $\mathbb{Z}_3$-ban (ellenőrizzük: 0,1,2 nem gyök!), így csak az történhet, hogy $\bar{g}$ és $\bar{h}$ másodfokúak és irreducibilisek $\mathbb{Z}_3[x]$-ben. Az is föltehető, hogy mindkettőnek a főegyütthatója 1, hiszen $\bar{f}$ normált (ha $\bar{g}$ és $\bar{h}$ főegyütthatója 2 lenne, akkor mindkét tényezőt szorozhatnánk 2-vel). A $\mathbb{Z}_3$ fölötti másodfokú polinomokat viszont ismerjük: ezek azok, amelyeknek nincs gyöke. Ez azt jelenti, hogy a konstans tagja nem nulla (mivel a 0 nem gyök), továbbá az együtthatók összege (ill. váltott előjelű összege) nem nulla (mivel sem az 1, sem a 2, azaz a -1 nem gyök). Az ilyen normált polinomok: x^2+x+2, x^2+2x+2. Könnyű ellenőrizni, hogy ezeknek sem a négyzete, sem az egymással vett szorzata nem adja az eredeti polinomot (modulo 3). Ez azt jelenti, hogy f irreducibilis $\mathbb{Q}[x]$-ben. *Harmadik megoldás:* Érdemes végiggondolni modulo 2 ugyanezt. $\mathbb{Z}_2[x]$-ben $\bar{f}(x)$ egy elsőfokú és egy harmadfokú irreducibilis polinom szorzatára bomlik, azt viszont láttuk, hogy $\mathbb{Z}[x]$ fölött csak másodfokú irreducibilis faktorai lehetnének, ilyen fölbontása viszont $\mathbb{Z}_2[x]$-ben az előbbiek szerint nem lehet.

6. **a)** *Legyen $f\in\mathbb{Z}[x]$, $\deg f = k>0$. Tekintsük azokat az a egész számokat, melyekre $f(a)\in\{-1,1\}$. Igazoljuk, hogy legfeljebb $2k$ darab ilyen szám van.*

b) *Legyen $h\in\mathbb{Z}[x]$, $\deg h = n$. Tegyük fel, hogy $a_1,a_2,\ldots,a_{2n+1}$ olyan különböző egész számok, melyekre $h(a_i)$ prímszám. Igazoljuk, hogy h irreducibilis $\mathbb{Z}$ fölött.*

Megoldás. a) Tudjuk, hogy nullosztómentes gyűrű fölött egy nem nulla poliomnak legföljebb fokszámnyi gyöke van. Ez azt jelenti, hogy $n>0$ esetén egy n-edfokú $f(x)$ polinom tetszőleges c értéket legföljebb n-szer vesz föl, hiszen az $f(x)-c$ polinomnak legföljebb n gyöke van. Ez azt jelenti, hogy egy k-adfokú polinom a $+1$ és a -1 értéket is legföljebb k-szor veheti föl, azaz összesen legföljebb $2k$ ilyen értéket találhatunk.
b) Tegyük föl, hogy $h = f\cdot g$, ahol $f,g\in\mathbb{Z}[x]$, továbbá $\deg f = k$, $\deg g = \ell$ és $k+\ell = n$. Mivel $h(a_i)$ prímszám, továbbá $h(a_i) = f(a_i)g(a_i)$, ezért minden i-re vagy $f(a_i)$, vagy $g(a_i)\in\{+1,-1\}$. Az a) rész alapján ha f és g egyike sem konstans, akkor ilyen helyből legföljebb $2k+2\ell = 2n$ lehetne, ellentétben a föltevésünkkel. Ha viszont pl. f konstans, akkor két eset lehetséges. Első esetben $f=1$, vagy $f=-1$, és akkor a fölbontás triviális. Ha f nem ±1, akkor f valamilyen prím konstanssal egyenlő, és ekkor $g(a_i)=\pm1$ minden $1\le i\le 2n+1$, ami az a) rész miatt nem lehetséges.

7. *Legyenek $a_1, a_2, \ldots, a_n$ különböző egész számok. Igazoljuk, hogy az*

$$(x-a_1)(x-a_2)\cdots(x-a_n)-1$$

polinom irreducibilis $\mathbb{Z}$ fölött.

Megoldás. Vegyük először észre, hogy az $f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)-1$ polinomra $f(a_i)=-1$ minden $1\le i\le n$ esetén, és tegyük föl, hogy $f(x)=g(x)h(x)$, ahol $g,h\in\mathbb{Z}[x]$. Ha g vagy h konstans lenne, akkor az első megjegyzés alapján csak $+1$ vagy -1 lehetne, vagyis az f fölbontása triviális lenne. Tegyük föl tehát indirekt módon, hogy $\deg g, \deg h < n$. Akkor $g(a_i)h(a_i)=f(a_i)=-1$ miatt $g(a_i)$ és $h(a_i)$ közül az egyik $+1$, a másik -1 (különböző i-kre változhat, hogy melyik a $+1$ és melyik a -1, de ez most tkp. lényegtelen). Ebből az következik, hogy $g(a_i)+h(a_i)=0$, vagyis a $g+h$ polinomnak minden $1\le i\le n$-re gyöke az a_i. De $\deg(g+h)<n$ miatt ez csak akkor lehet, hogy $g+h$ a konstans 0 polinom, azaz $g=-h$. Ez viszont ellentmondás, mert ekkor gh főegyütthatója negatív, ellentétbenn f-ével, ami 1. Azt kaptuk tehát, hogy $f(x)$ irreducibilis $\mathbb{Z}[x]$-ben.

8. *Számítsuk ki a Φ_{45} és a Φ_{168} körosztási polinomok fokszámát.*

Megoldás. Tudjuk, hogy $\deg\Phi_n(x)=\varphi(n)$, ahol φ az Euler-féle függvény (aminél $\varphi(n)$ azt mondja meg, hány 1 és n közötti szám relatív prím n-hez). φ-ről azt is jó tudni, hogy multiplikatív függvény (ez azt jelenti, hogy egymáshoz relatív prím a és b egész számok esetén $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$). Ez azt jelenti, hogy elegendő prímhatványokra tudni φ értékét: $\varphi(p^k)=p^k-p^{k-1}$. Ezért $\deg\Phi_{45}=\varphi(45)=\varphi(5\cdot 9)=\varphi(5)\varphi(9)=4\cdot 6=24$, illetve $\deg\Phi_{168}=\varphi(168)=\varphi(8\cdot 3\cdot 7)=\varphi(8)\varphi(3)\varphi(7)=4\cdot 2\cdot 6=48$.

9. *Írjuk fel a Φ_6, a Φ_8 és a Φ_{15} körosztási polinomokat.*

Megoldás. Használjuk a rekurzív képletet Φ_n-re:

$$\Phi_n(x)=\frac{x^n-1}{\prod\limits_{\substack{d\mid n\\ d\neq n}}\Phi_d(x)}$$

Ekkor, persze, ismerni kell a kisebb indexű körosztási polinomokat, de néha még azt is meg lehet spórolni, ha az osztók közül csoportosítjuk azokat, amelyek egy valódi k osztó összes osztóját adják: ezekből kijön egy (x^k-1)-es faktor. Így tehát:

$$\Phi_6(x)=\frac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)}=\frac{x^6-1}{(x^3-1)\Phi_2(x)}=\frac{x^3+1}{x+1}=x^2-x+1$$
$$\Phi_8(x)=\frac{x^8-1}{\Phi_1(x)\Phi_2(x)\Phi_4(x)}=\frac{x^8-1}{x^4-1}=x^4+1$$
$$\Phi_{15}(x)=\frac{x^{15}-1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)}=\frac{x^{15}-1}{(x^5-1)\Phi_3(x)}=\frac{x^{10}+x^5+1}{x^2+x+1}=x^8-x^7+x^5-x^4+x^3-x+1$$

A legutóbbi körosztási polinomnál az utolsó osztáshoz, sajnos, számolnunk kell (pl. a maradékos osztás algoritmusával), hogy megkapjuk a hányadost.

10. *Írjuk fel a Φ_9 és a Φ_{27} polinomokat, majd igazoljuk, hogy ezek irreducibilisek $\mathbb{Q}$ fölött. Mely körosztási polinomok irreducibilitását lehetne még belátni az általad talált módszerrel?*

Megoldás. Mindkét esetben lehet venni az $x+1$-es helyettesítést (mint $\Phi_p(x)$-nél tettük az előadáson), és kiderül, hogy a Schönemann–Eisenstein-kritérium feltételei teljesülnek $p=3$-ra. Ezt kiszámolni, különösen a Φ_{27} esetén meglehetősen fáradságos. A sejtés, általánosan, hogy a módszert lehet alkalmazni prímhatvány indexű körosztási polinomokra. Általánosan, $\Phi_{p^k}(x)=\frac{x^{p^k}-1}{x^{p^{k-1}}-1}=x^{p^{k-1}(p-1)}+x^{p^{k-1}(p-2)}+\cdots+x^{p^{k-1}}+1$. Ahhoz, hogy bizonyítsuk, hogy alkalmazható a Schönemann–Eisenstein-kritérium eltolt változata, ügyesen kell végigvinnünk a számolást: modulo p a számolás kicsit könnyebb, mintha az egészek körében számolnánk a p-vel való oszthatóságot. A rekurzív képletből azt kapjuk, hogy $\Phi_{p^k}(x)(x^{p^{k-1}}-1)=x^{p^k}-1$. Vegyük ezt az egyenlőséget modulo p, és helyettesítsünk be x helyébe $x+1$-et. Vegyük észre, hogy $\mathbb{Z}_p[x]$-ben, mint tudjuk, $(a+b)^p=a^p+b^p$, és innen indukcióval $(a+b)^{p^t}=a^{p^t}+b^{p^t}$. Ez azt jelenti hogy $\mathbb{Z}_p[x]$-ben: $\Phi_{p^k}(x+1)\cdot x^{p^{k-1}}=x^{p^k}$, azaz $\Phi_{p^k}(x+1)=x^{p^k-p^{k-1}}$. Ez tehát azt jelenti, hogy $\Phi_{p^k}(x+1)$-nak minden együtthatója osztható p-vel, kivéve a főegyütthatóját. Ugyanakkor az eltolt polinom konstans tagja az explicit képletből jól láthatóan p, tehát nem osztható p^2-tel. Alkalmazhatjuk tehát a Schönemann–Eisenstein-kritériumot $\Phi_{p^k}(x+1)$-re, és ebből a körosztási polinom irreducibilitása is következik.