Kétismeretlenes lineáris „diofantoszi” egyenlet megoldása test feletti polinomgyűrűben

Tetszőleges T test és $f, g, h \in T[x]$ polinomok esetén az $fu+gv = h$ egyenletet hasonlóan lehet megoldani az ismeretlen $u, v \in T[x]$ polinomokra, mint egész számok körében az $ax + by = c$ kétismeretlenes lineáris diofantoszi egyenletet. Az 1.8. Tétel (és a bizonyítása) szinte szó szerint lemásolható (3.16. Tétel), és az egyenlet megoldási módszere (euklideszi algoritmus) is pontosan ugyanaz, mint az egész számok körében, csak sokkal többet kell számolni. Ezért itt megelégszünk egyetlen megoldás kiszámolásával, és csak olyan egyenleteket nézünk, ahol $h \sim \operatorname{lnko}(f, g)$.

Az euklideszi algoritmus lépései maradékos osztások, tehát nem árt a polinomok maradékos osztását átismételni, például a `http://www.math.u-szeged.hu/~twaldha/practmath/mpract.html?sub:7` oldalon a „Polinomok: maradékos osztás” feladattípussal. A $\mathbb{Z}_p$ feletti polinomok maradékos osztása során figyelni kell arra, hogy észrevegyük, ha nulla lett a maradék (például $\mathbb{Z}_5$-ben $\overline{15} = \overline{0}$). Szükség lehet modulo p multiplikatív inverzre is, például, ha $\mathbb{Z}_7$ felett egy $f = \overline{3}x^8 + \cdots$ alakú polinomot osztunk egy $g = \overline{2}x^2 + \cdots$ alakú polinommal, akkor a hányados első tagja $\overline{5}x^6$ lesz (ellenőrzés: $\overline{2}x^2 \cdot \overline{5}x^6 = \overline{10}x^8 = \overline{3}x^8$). Az $\overline{5}$ együttható így jött ki: $\overline{3} \cdot \overline{2}^{-1} = \overline{3} \cdot \overline{4} = \overline{12} = \overline{5}$, ahol a $\overline{2}^{-1} = \overline{4}$ multiplikatív inverz a $2 \cdot ? \equiv 1 \pmod 7$ kongruencia megoldásából adódik.

Példa. Számítsuk ki az f és g polinomok legnagyobb közös osztóját, és adjuk meg az $fu + gv = \operatorname{lnko}(f, g)$ egyenlet egy megoldását az $\mathbb{R}[x]$ polinomgyűrűben.

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

Megoldás: Hajtsuk végre az euklideszi algoritmust az f és g polinomokra (amelyik polinomnak van „neve”, arra mindig a nevével hivatkozunk a jobb átláthatóság kedvéért):

	osztandó	$=$	hányados $\cdot$ osztó	$+$	maradék
(1)	f	$=$	$1 \cdot g$	$+$	$x^3 - 2x$
(2)	g	$=$	$(x+1) \cdot \left(x^3 - 2x\right)$	$+$	$\boxed{x^2 - 2}$
(3)	$x^3 - 2x$	$=$	$x \cdot \left(x^2 - 2\right)$	$+$	0

A legnagyobb közös osztó az utolsó nemnulla maradék: $\operatorname{lnko}(f, g) \sim \boxed{x^2 - 2}$.

A „diofantoszi” egyenlet megoldásához fejezzük ki a maradékot az euklideszi algoritmus során elvégzett mindegyik osztásnál (az utolsót kivéve):

	maradék	$=$	osztandó	$-$	hányados $\cdot$ osztó
(1)	$x^3 - 2x$	$=$	f	$-$	$1 \cdot g$
(2)	$\operatorname{lnko}(f, g) \sim \boxed{x^2 - 2}$	$=$	g	$-$	$(x+1) \cdot \left(x^3 - 2x\right)$

Az a célunk, hogy mindegyik maradékot f és g segítségével írjuk fel ($fu + gv$ alakban). Az első osztás maradéka máris ilyen alakban van: $x^3 - 2x = f - g$. Ezt behelyettesíthetjük a második osztás maradékának fenti felírásában $x^3 - 2x$ helyére:

$$\operatorname{lnko}(f, g) \sim \boxed{x^2 - 2} = g - (x+1) \cdot \left(x^3 - 2x\right) = g - (x+1) \cdot (f - g) = (-x - 1) \cdot f + (x + 2) \cdot g.$$

Ebből leolvashatjuk az $fu + gv = \operatorname{lnko}(f, g)$ egyenlet egy megoldását: $u = -x - 1$, $v = x + 2$.

Megjegyzés. A legnagyobb közös osztó segítségével meghatározhatjuk f és g komplex gyökeit. Nyilván f és g is osztható $\operatorname{lnko}(f, g)$-vel:

$$f = \left(x^2 - 2\right) \cdot \left(x^2 + 2x + 1\right) \quad \text{és} \quad g = \left(x^2 - 2\right) \cdot \left(x^2 + x + 1\right).$$

Ebből rögtön megkapjuk f és g gyökeit (multiplicitással):

$$f \text{ gyökei: } \sqrt{2},\ -\sqrt{2},\ -1,\ -1; \qquad g \text{ gyökei: } \sqrt{2},\ -\sqrt{2},\ -\frac{1}{2} + \frac{\sqrt{3}}{2}i,\ -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Megfigyelhetjük, hogy f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

Példa. Adjuk meg az $fu+gv=\overline{1}$ egyenlet egy megoldását a $\mathbb{Z}_7[x]$ polinomgyűrűben.

$$f=x^4+\overline{2}x^3+\overline{5}x^2+\overline{2}x+\overline{5}, \qquad g=\overline{2}x^3+\overline{4}x^2+\overline{4}x$$

Megoldás: Hajtsuk végre az euklideszi algoritmust az f és g polinomokra (amelyik polinomnak van „neve”, arra mindig a nevével hivatkozunk a jobb átláthatóság kedvéért):

	osztandó	$=$	hányados $\cdot$ osztó	$+$	maradék
(1)	f	$=$	$\overline{4}x\cdot g$	$+$	$\overline{3}x^2+\overline{2}x+\overline{5}$
(2)	g	$=$	$(\overline{3}x+\overline{4})\cdot(\overline{3}x^2+\overline{2}x+\overline{5})$	$+$	$\overline{2}x+\overline{1}$
(3)	$\overline{3}x^2+\overline{2}x+\overline{5}$	$=$	$(\overline{5}x+\overline{2})\cdot(\overline{2}x+\overline{1})$	$+$	$\boxed{\overline{3}}$
(4)	$\overline{2}x+\overline{1}$	$=$	$(\overline{3}x+\overline{5})\cdot\overline{3}$	$+$	$\overline{0}$

(Az utolsó osztást ki is hagyhattuk volna, mert $\overline{3}\sim\overline{1}$, tehát bármilyen polinomot osztunk is $\overline{3}$-sal, mindig $\overline{0}$ lesz a maradék.) A legnagyobb közös osztó az utolsó nemnulla maradék: $\operatorname{lnko}(f,g)\sim\boxed{\overline{3}}\sim\overline{1}$.

A „diofantoszi” egyenlet megoldásához fejezzük ki a maradékot az euklideszi algoritmus során elvégzett mindegyik osztásnál (az utolsót kivéve):

	maradék	$=$	osztandó	$-$	hányados $\cdot$ osztó
(1)	$\overline{3}x^2+\overline{2}x+\overline{5}$	$=$	f	$-$	$\overline{4}x\cdot g$
(2)	$\overline{2}x+\overline{1}$	$=$	g	$-$	$(\overline{3}x+\overline{4})\cdot(\overline{3}x^2+\overline{2}x+\overline{5})$
(3)	$\operatorname{lnko}(f,g)\sim\boxed{\overline{3}}$	$=$	$\overline{3}x^2+\overline{2}x+\overline{5}$	$-$	$(\overline{5}x+\overline{2})\cdot(\overline{2}x+\overline{1})$

Az a célunk, hogy mindegyik maradékot f és g segítségével írjuk fel ($fu+gv$ alakban). Az első osztás maradéka már ilyen alakban van. Ezt behelyettesíthetjük a második osztás maradékának fenti felírásába:

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

A harmadik osztás maradékának fenti felírásába behelyettesítjük az első két osztás maradékának f és g segítségével felírt alakját:

$$\begin{aligned}\operatorname{lnko}(f,g)\sim\boxed{\overline{3}}&=\overline{3}x^2+\overline{2}x+\overline{5}-(\overline{5}x+\overline{2})\cdot(\overline{2}x+\overline{1})=\\&=(f-\overline{4}x\cdot g)-(\overline{5}x+\overline{2})\cdot\Big((\overline{4}x+\overline{3})\cdot f+(\overline{5}x^2+\overline{2}x+\overline{1})\cdot g\Big)=\\&=(x^2+\overline{5}x+\overline{2})\cdot f+(\overline{3}x^3+x^2+x+\overline{5})\cdot g.\end{aligned}$$

Azt kaptuk, hogy

$$(x^2+\overline{5}x+\overline{2})\cdot f+(\overline{3}x^3+x^2+x+\overline{5})\cdot g=\overline{3}$$

Már majdnem készen vagyunk, de nekünk nem $\overline{3}$-t, hanem $\overline{1}$-t kell felírnunk $fu+gv$ alakban. (Mivel $\overline{3}\sim\overline{1}$, mindkettő „egyformán jó” legnagyobb közös osztónak, de a feladatban most konkrétan $\overline{1}$ szerepelt.) Ehhez be kell szoroznunk az egyenlőséget $\overline{3}$ multiplikatív inverzével, vagyis $\overline{5}$-sal:

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

Ebből leolvashatjuk az $fu+gv=\overline{1}$ egyenlet egy megoldását: $u=\overline{5}x^2+\overline{4}x+\overline{3}$, $v=x^3+\overline{5}x^2+\overline{5}x+\overline{4}$.

Mindezt lehet (sőt, kell!) gyakorolni a `http://www.math.u-szeged.hu/~twaldha/practmath/mpract.html?sub:7` weboldalon a „Polinomok: lnko” és „Polinomok: diofantoszi egyenlet” feladattípusokban.