Számelmélet 2. Test fölötti polinomgyűrűk 1.

Klukovits Lajos

TTIK Bolyai Intézet

2020. október 17.

Oszthatósági tesztek egészekre 1.

Amit az iskolából tudunk, ill. nem tudunk.

Legyen $a \in \mathbb{Z}$ tetszőleges egész, $a = \sum_{k=0}^{n} 10^k a_k,\ 0 \leq a_k \leq 9$.

- a pontosan akkor osztható 2-vel, ill. 5-tel, ha utolsó számjegye osztható 2-vel, ill. 5-tel: $2, 5 | a_0$.
- a pontosan akkor osztható 3-mal, ill. 9-cel, ha $3, 9 | \sum_{k=0}^{n} a_k$.
- a pontosan akkor osztható 11-gyel, ha $11 | \sum_{k=0}^{n} (-1)^k a_k$.
- De az első kritériumot kivéve nem szokott arról szó esni, hogy miért igazak ezek az állítások.
- Pedig egyszerűen igazolhatók: azon múlnak, hogy $10 \equiv 1 \pmod 3$, ugyanez áll a 9 modulusra, ill. $10 \equiv -1 \pmod{11}$.

Oszthatósági tesztek egészekre 2.

Megadható hasonló teszt más prímekre is?

- A válasz: elméletileg igen, csak a használhatóság kérdéses nagyobb prímekre.
- A továbbiakban $p > 2$ prím, $a = \sum_{k=0}^{n} 10^k a_k,\ 0 \leq a_k \leq 9$ tetszőleges egész.
- Fermat tétele szerint $10^{p-1} \equiv 1 \pmod p$. Mivel p páratlan, ebből $p \left| \left(10^{\frac{p-1}{2}} - 1\right)\left(10^{\frac{p-1}{2}} + 1\right)\right.$.
- A prímtulajdonságból adódik, hogy p pontosan az egyik tényezőnek osztója.

Oszthatósági tesztek egészekre 3.

A $p \left| \left(10^{\frac{p-1}{2}} - 1\right)\right.$ eset.

- Ekkor $10^{\frac{p-1}{2}} \equiv 1 \pmod p$. Osszuk föl — az egyesektől indulva — az a számot $\frac{p-1}{2}$ jegyű számokra, majd e számokat összeadjuk. Ezt úgy is interpretálhatjuk, hogy ezen 10-hatványok helyébe 1-et írunk.
- A kapott összeg nyilván kongruens modulo p az eredeti számmal.
- Ha a kapott szám jegyeinek száma nagyobb $\frac{p-1}{2}$-nél, akkor addig ismételjük az eljárást, míg a kapott szám jegyeinek száma kisebb nem lesz $\frac{p-1}{2}$-nél. Legyen az így kapott szám b.
- Világos, hogy $a \equiv b \pmod p$.

Oszthatósági tesztek egészekre 4.

A $p \mid \left(10^{\frac{p-1}{2}}+1\right)$ eset.

- Az előbbihez hasonlóan tárgyalható, csak most a fölosztás révén kapott $\frac{p-1}{2}$ jegyű számokat váltakozó előjellel kell összeadni.
- A „használhatóság" azon múlik, hogy milyen az eredei szám jegyeinek számának és a $\frac{p-1}{2}$-nek a viszonya.
- Vegyük észre, hogy ha $\frac{p-1}{2}$ páros, akkor felére csökkenthető a beosztásnál figyelembe veendő jegyek száma. Sőt ...
- Például, ez a szám $p = 7,\ 13$ esetén 3,

Számolás maradékosztály-gyűrűkben.

Számolja ki a $\mathbb{Z}_{13}$ gyűrűben (testben) az $\overline{8}-\overline{11}$, $\overline{8}\cdot\overline{11}$, $\overline{8}^{11}$, $\overline{8}/\overline{11}$ elemeket.

$\overline{8}-\overline{11}=\overline{8}+\overline{2}=\overline{10}$.

$8\cdot 11=88\equiv 10 \pmod{13}$, így $\overline{8}\cdot\overline{11}=\overline{10}$.

Legyen $8^{11}\equiv x \pmod{13}$. Mivel $8^{12}\equiv 1 \pmod{13}$, $8x\equiv 1 \pmod{13}$, amiből $x\equiv 5 \pmod{13}$, azaz $\overline{8}^{11}=\overline{5}$.

Először $\overline{11}$ multiplikatív inverzét kell kiszámolni, megoldandó a $\overline{11}\overline{x}=\overline{1}$ egyenlet,

ez ekvivalens a $11x\equiv 1 \pmod{13}$ kongruencia megoldásával.

Ebből $x\equiv 6 \pmod{13}$, így $\overline{8}/\overline{11}=\overline{8}\cdot\overline{6}=\overline{48}=\overline{9}$.

Definíció.

R fölötti **polinomnak** nevezzük az olyan, R-beli elemekből képezett, $(a_0, a_1, \ldots)$ végtelen sorozatot, amelynek csak véges sok nemzéró tagja van. Az összes R fölötti polinomok halmazát $R[x]$ fogja jelölni.
Legyen $f=(a_0,a_1,\ldots)\in R[x]$ tetszőleges polinom, és $n\in\mathbb{N}$. Az f **polinom** n **edik tagja** e sorozat n indexű tagja: $(f)_n=a_n$.

Polinom fokszáma.

Az $f\in R[x]$ **polinom fokszáma** a legnagyobb olyan $n\in\mathbb{N}_0$, amelyre $a_n\neq 0$. Ha ilyen n nincs, azaz $f=(0,0,\ldots)$, akkor f fokszáma $-\infty$. Az f polinom fokszámát $\deg f$ fogja jelölni. Ha $\deg f=1,-\infty$, akkor azt mondjuk, hogy f **konstans polinom**. Ha $\deg f=n\geq 0$, akkor az a_n elemet f **főegyütthatójának** nevezzük, az 1 főegyütthatójú polinomokat pedig **főpolinomoknak**.
A konstans polinomokat általában főegyütthatójukkal jelöljük.

Műveletek polinomokkal.

Definíció.

Az $f,g\in R[x]$ **polinomok összege ill. szorzata** a következő két polinom:

$$(f+g)_n=(f)_n+(g)_n$$
$$(f\cdot g)_n=\sum_{i=0}^{n}(f)_i(g)_{n-i}$$

Lemma.

Tetszőleges $f,g\in R[x]$ polinomokra

$$\deg(f+g)\leq\max\{\deg f,\deg g\}\ \text{és}\ \deg(f\cdot g)=\deg f+\deg g.$$

Tétel.

Az iménti definícióbeli műveletekkel $R[x]$ integritástartomány, az R fölötti (egyhatározatlanos) polinomgyűrű.

Lemma.

Minden $a, b \in R$ esetén

$$(a,0,0,\ldots)+(b,0,0,\ldots)=(a+b,0,0,\ldots)$$
$$(a,0,0,\ldots)\cdot(b,0,0,\ldots)=(a\cdot b,0,0,\ldots)$$

Jelölés.

Az elkövetkezőkben az $(a,0,0,\ldots)$ polinom helyett egyszerűen a-t írunk, és nem különböztetjük meg az a gyűrűelemtől, azaz úgy tekintjük, hogy $R \subseteq R[x]$. A $(0,1,0,0,\ldots)$ polinomot pedig x jelöli a jövőben.

Tétel.

Minden polinom előáll $\sum_{i=0}^{n} a_n x^n$ $(a_n \neq 0)$ alakban, és ez az előállítás egyértelmű. Ha $f=(a_0,a_1,\ldots)$ egy n-edfokú polinom, akkor

$$f=(a_0,a_1,\ldots,a_n,0,\ldots)=a_0+a_1x+\ldots+a_nx^n.$$

Jelölések.

A polinomokat az elkövetkezőkben $a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$, vagy $\sum_{i=0}^{n} a_ix^i$ alakban írjuk, és hallgatólagosan mindig föltesszük, hogy $a_n \neq 0$, valamint azt, hogy e polinom n-edfokú, azaz $a_{n+1}=a_{n+2}=\ldots=0$. Az x szimbólum neve **határozatlan** (és nyilván $x \notin R$). A határozatlant természetesen más betű is jelölheti, leggyakrabban y, vagy pl. z. Ez esetekben a polinomgyűrűt $R[y]$, $R[z],\ldots$ jelöli.

Lemma.

Legyen F test. Az $F[x]$ polinomgyűrű egységei épp a nemzéró konstans polinomok.

A továbbiakban test fölötti polinomokkal/polinomgyűrűkkel foglalkozunk, DE számos tétel/állítás integritástartomány fölötti polinomkra is érvényes.

Számelmélet polinomgyűrűkben.

Definíció.

Legyenek $f,g \in F[x]$. Azt mondjuk, hogy az f polinom **osztója** a g polinomnak, ha létezik olyan $h \in F[x]$ polinom, hogy $g=fh$. Jelölése: $f|g$.

Definíció.

Azt mondjuk, hogy az $f,g \in R[x]$ polinomok **asszociáltak**, ha $f|g$ és $g|f$.

Tétel.

Legyen F test. Az asszociáltság ekvivalenciareláció $F[x]$-en. A nulla osztályt kivéve minden asszociáltsági osztály tartalmaz főpolinomot, mégpedig pontosan egyet.

Számelmélet polinomgyűrűkben.

Tétel.

Bármely $F[x]$ polinomgyűrűben az oszthatóság reflexív és tranzitív reláció, továbbá tetszőleges $f,g \in F[x]$ polinomokra

(1) $f \sim g \Leftrightarrow \exists c \in F^*: g=cf$, (2) $(f|g$ és $g \neq 0) \Rightarrow \deg f \leq \deg g$.

Tétel.

Legyen F test. tetszőleges $f,g,h \in F[x]$ polinomokra

(1) $f|f$;
(2) $(f|g$ és $g|h) \Rightarrow f|h$;
(3) $(f|g$ és $g|f) \Leftrightarrow \exists c \in F^*: g=cf$;
(4) $1|f$;
(5) $f|0$;
(6) $f|1 \Leftrightarrow f \in F^*$;
(7) $0|f \Leftrightarrow f=0$;
(8) $(f|g$ és $f|h) \Rightarrow f|g \pm h$;
(9) $f|g \Rightarrow f|gh$;
(10) $f|g \Leftrightarrow fh|gh$, ha $h \neq 0$;
(11) $f|g \Rightarrow \deg f \leq \deg g$, ha $g \neq 0$.

Számelmélet polinomgyűrűkben.

Emlékeztetők.

1. Polinomok legnagyobb közös osztója, legkisebb közös többszöröse.
2. Egyértelműségük.

Tétel.

Bármely két $f, g \in F[x]$ nemzéró polinomnak létezik legnagyobb közös osztója és legkisebb közös többszöröse. Ezek asszociáltság erejéig egyértelműen meghatározottak. A legnagyobb közös osztó előállítható az f és a g polinomok lineáris kombinációjaként, azaz léteznek olyan F fölötti u, v polinomok, hogy $\ln.\,k.\,o.(f, g) = fu + gv$.

Tétel. **a maradékos osztás tétele**

Legyenek $f, g \in F[x]$, és $g \neq 0$ polinomok. Léteznek olyan egyértelműen meghatározott $q, r \in F[x]$ polinomok, hogy $f = gq + r$, ahol $r = 0$, vagy $\deg r < \deg g$.

Bizonyítás.

- $f = a_n x^n + \ldots + a_0,\ g = b_m x^m + \ldots + b_0,\ a_n b_m \neq 0,\ n \geq m.$
- A $q_1 = f - a_n b_m^{-1} x^{n-m} g$ polinomra $\deg q_1 < n$.
- Ha $\deg q_1 \geq m$, akkor megismételjük ezt az eljárást az f helyett a q_1 polinomra, kapjuk a q_2 polinomot.
- Ezt addig ismételjük, amíg olyan q_i polinomhoz nem jutunk, amelyre $\deg q_i < m$.
- Ekkor a $q_1 + \ldots + q_i = q$ polinom, valamint az $r = f - qg$ polinom eleget tesz a tétel föltételeinek.
- Ha $f = qg + r = q'g + r'$, ahol $\deg r, \deg r' < m$, akkor $(q - q')g + (r - r') = 0$,
- amiből $g | r - r'$. Ez pedig csak úgy lehetséges, ha $r - r' = 0$.
- $q = q'$ a zérusosztó-mentességből adódik.

Számelmélet polinomgyűrűkben.

Euklideszi algoritmus.

Legyen $\deg f \geq \deg g$, és végezzünk maradékos osztásokat a következőképp.

$$\begin{aligned} f &= gq_1 + r_1 \\ g &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \end{aligned}$$

Alkalmazás.

Tudjuk, hogy

$$\deg g > \deg r_1 > \deg r_2 > \deg r_3 > \ldots \geq 0,$$

így e sorozat véges, az utolsó nemzéró maradék a legnagyobb közös osztó.

Számelmélet polinomgyűrűkben.

Tétel.

Tetszőleges $f, g, h \in F[x]$ polinomok esetén,

1. ha $fg \neq 0$, akkor

$$\ln.\,k.\,o.\left(\frac{f}{\ln.\,k.\,o.(f,g)}, \frac{g}{\ln.\,k.\,o.(f,g)}\right) \sim 1,$$

   azaz a két hányados relatív prím;
2. ha f és g relatív prím, akkor

$$f | gh \quad \Leftrightarrow \quad f | h;$$

3. ha $\ln.\,k.\,o.(f, g) \neq 0$, akkor

$$f | gh \quad \Leftrightarrow \quad \frac{f}{\ln.\,k.\,o.(f,g)} | h.$$

Számelmélet polinomgyűrűkben.

Tétel.

Legyenek $f, g, h \in F[x]$ nemzéró polinomok. Pontosan akkor léteznek olyan F fölötti u, v polinomok, hogy $fu + gv = h$, másképpen mondva, megoldható $F[x]$-ben u, v-re az előbbi egyenlet, ha $\text{ln. k. o.}(f, g) | h$. Ha (u_0, v_0) egy megoldás, akkor tetszőleges $t \in F[x]$-re

$$u = u_0 + \frac{g}{\text{ln. k. o.}(f, g)} t, \qquad v = v_0 - \frac{f}{\text{ln. k. o.}(f, g)} t$$

is megoldás, és minden megoldás ilyen alakban írható.

Bizonyítás.

Ugyanúgy, mint az klasszikus számelméletben, az euklideszi algoritmusban visszafelé haladva.

Példa.

Az $f = x^4 + x^3 + x^2 + 1$ és $g = x^3 + 1$ polinomokhoz határozzon meg olyan u, v polinomokat, amelyekre $fu + gv \sim \text{ln. k. o.}(f, g)$ előbb az $\mathbb{R}$ majd a $\mathbb{Z}_2$ testek fölött.

- Euklidesz algoritmussal azámolva:

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

- (3)-ból $(x+1)(x-2) = (x^2 - x) - 2$, ezt (2)-be helyettesítve
- $g(x-2) = (x^2-x)(x-2) + ((x^2-x) - 2) = (x^2-x)(x^2-x-1) - 2$.
- Folytatva a helyettesítést (1)-be: $f(x^2 - x - 1) = g(x^3 - x - 3) + 2$.
- $u = x^2 - x - 1, \ v = -(x^3 - x - 3)$.

A $\mathbb{Z}_2$ test fölött számolva.

- $f = x^4 + x^3 + x^2 + \overline{1}, \ g = x^3 + \overline{1}$.

$$f = g(x + \overline{1}) + (x^2 + x)$$
$$g = (x^2 + x)(x + \overline{1}) + (x + \overline{1})$$
$$x^2 + x = (x + \overline{1})x$$

- Az előbbi módon helyettesítgetve:

$$f(x + \overline{1}) + gx^2 = x + \overline{1}$$

Polinomgyűrűk faktorgyűrűi.

Definíció.

Legyenek $f, g, m \in F[x], \ m \neq 0$ tetszőleges polinomok. Azt mondjuk, hogy **f kongruens g-vel modulo m**, jelölése $f \equiv g \pmod{m}$, ha $m | f - g$, vagy ami ezzel ekvivalens: két polinom pontosan akkor kongruens modulo m, ha m-mel osztva ugyazazt a maradékot adja asszociáltság erejéig.

Tétel.

Az imént definiált „kongruenciareláció" ekvivakenciareláció és megőrzi a polinomgyűrű műveleteit.

Tétel.

Tetszőleges $f, g, m \in F[x]$ polinomok esetén az $fu \equiv g \pmod{m}$ lineáris kongruencia pontosan akkor oldható meg, ha $\text{ln. k. o.}(f, m) | g$.

Polinomgyűrűk faktorgyűrűi.

Bizonyítás.

A tétel állítása azonnal adódik abból az észrevételből hogy az $fu \equiv g \pmod m$ lineáris kongruencia pontosan akkor oldható meg, ha megoldható az $fu + mv = g$ egyenlet az $F[x]$ polinomgyűrűben.

Definíció.

A *mod m* kongruenciához tartozó ekvivalenciaosztályokat **modulo m maradékosztályoknak** nevezzük. Az $f \in F[x]$ polinomot tartalmazó modulo m maradékosztályt $\overline{f}$ jelöli, míg a maradékosztályok halmazát, másképpen mondva, a modulo m kongruenciához tartozó faktorhalmazt, pedig $F[x]/(m)$. Tehát $F[x]/(m) = \{\overline{f} : f \in F[x]\}$.

Számolás faktorgyűrűben.

Határozzon meg egy olyan $f \in \mathbb{R}[x]$ polinomot, amelyre $x^2 f \equiv x^2 - 2x \pmod{x^3 + x}$.

Az $x^2 f + (x^3 + x)g = x^2 - x$ egyenletet kell megoldanunk az $\mathbb{R}[x]$ polinomgyűrűben.

Euklideszi algoritmussal számolva: az $x^3 + x$ polinomot az x^2 polinommal osztva a hányados x és a maradék szintén x.

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

A keresett polinom: $f = -x^2 + 2x$.

Polinomgyűrűk faktorgyűrűi.

Definíció.

Az $F[x]/(m)$ faktorhalmazon bevezetünk két műveletet: összeadást és szorzást: tetszőleges $f, g \in F[x]$-re legyen

$$\overline{f} + \overline{g} = \overline{f + g}, \quad -\overline{f} = \overline{-f}, \quad \overline{f} \cdot \overline{g} = \overline{f \cdot g}.$$

Lemma.

Az előbbi műveletel jóldefiniáltak, azaz az eredmény nem függ attól, hogy az adott maradékosztály mely elemét választottuk reprezentánsnak, és e műveletekkel az $F[x]/(m)$ faktorhalmaz egységelemes kommutatív gyűrűt alkot.

Definíció.

Az előbbi gyűrűt **modulo m maradékosztály-gyűrűnek** nevezzük.

Polinomgyűrűk faktorgyűrűi.

Lemma

Tekintsük az $F[x]/(m)$ maradékosztálygyűrűt. Ha valamely $f \in F[x]$ polinomra $\ln.\,k.\,o.(f, m) \sim 1$, akkor bármely $g \in \overline{f}$ polinomra $\ln.\,k.\,o.(g, m) \sim 1$.

Megjegyzés.

Az előbbi állítás úgy is fogalmazható, hogy egy maradékosztálynak vagy minden eleme relatív prím a modulushor, vagy egyetlen eleme sem ilyen. Ezért beszélhetünk **relatív prím maradékosztályokról** is.

Tétel.

Az $\overline{f} \in F[x]/(m)$ maradékosztálynak pontosan akkor van multiplikatív inverze (pontosan akkor invertálható elem, azaz egység), ha $\ln.\,k.\,o.(f, m) \sim 1$. A multiplikatív inverz, ha létezik, egyértelműen meghatározott.

Polinomgyűrűk faktorgyűrűi.

Megjegyzés.

Gondolkozhatunk most is ugyanúgy, mint az elemi számelméletben, hiszen h absztraktan tekintünk rájuk, a polinomgyűrűk faktorgyűrűi ugyanolyan képződmények, mint a maradékosztály-gyűrűk.