Algebra és számelmélet 3 előadás
Kongruenciák

Waldhauser Tamás
2014 őszi félév

Tartalom

Tartalom

Emlékeztető

1. Definíció.

A d egész számot az a és b egész számok **legnagyobb közös osztójának** nevezzük, ha kielégíti a következő két feltételt:

(1) $d \mid a$ és $d \mid b$;

(2) $\forall k \in \mathbb{Z} : (k \mid a \text{ és } k \mid b) \implies k \mid d$.

A t egész szám **legkisebb közös többszöröse** a-nak és b-nek, ha kielégíti a következő két feltételt:

(1) $a \mid t$ és $b \mid t$;

(2) $\forall k \in \mathbb{Z} : (a \mid k \text{ és } b \mid k) \implies t \mid k$.

Jelölés.

Az a és b számok legnagyobb közös osztóját $\operatorname{lnko}(a, b)$ vagy (a, b), legkisebb közös többszörösüket pedig $\operatorname{lkkt}(a, b)$ vagy $[a, b]$ jelöli.

2. Megjegyzés.

A legnagyobb közös osztó nem egyértelmű: ha d legnagyobb közös osztója a-nak és b-nek, akkor $-d$ is az (de e két számon kívül nincs más legnagyobb közös osztó). Általában a két érték közül a nemnegatívat szoktuk tekinteni.

Az lnko rendezéselméleti megközelítése

3. Megjegyzés.

Az 1. Definíció szerint lnko (a, b) nem más, mint $(D_a \cap D_b; |)$ legnagyobb eleme. Nem triviális, hogy létezik legnagyobb eleme ennek a részbenrendezett halmaznak (miért?), de az euklideszi algoritmus garantálja, hogy létezik.

Az „iskolás definíció" szerint az $a, b \in \mathbb{N}$ számok legnagyobb közös osztója nem más, mint $(D_a \cap D_b; \leq)$ legnagyobb eleme. Erről világos, hogy létezik, de az nem világos, hogy lnko (a, b) nem csak nagyobb minden más közös osztónál, de *többszöröse* is minden más közös osztónak.

Tegyük fel, hogy $d = \text{lnko}\,(a, b)$ az 1. Definíció értelmében. Ha $k \in D_a \cap D_b$, akkor $k \mid d$ és így $k \leq d$, azaz d legnagyobb eleme a $(D_a \cap D_b; \leq)$ részben-rendezett halmaznak is. Tehát az „egyetemi definíció" és az „iskolás definíció" ekvivalens egymással — legalábbis pozitív egész számokra.

Mennyi lnko $(0, 0)$?

- „iskolás definíció": $(D_0 \cap D_0; \leq) = (\mathbb{N}_0 \cap \mathbb{N}_0; \leq) = (\mathbb{N}_0; \leq)$ legnagyobb eleme, ami nem létezik!
- „egyetemi definíció": $(D_0 \cap D_0; |) = (\mathbb{N}_0 \cap \mathbb{N}_0; |) = (\mathbb{N}_0; |)$ legnagyobb eleme, azaz 0.

Euklideszi algoritmus

4. Tétel (euklideszi algoritmus).

Bármely két természetes számnak van legnagyobb közös osztója, és az az euklideszi algoritmussal megkapható. Az $a = r_0, b = r_1$ természetes számokon végrehajtott **euklideszi algoritmus** *maradékos osztások ismételt elvégzését jelenti:*

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 && (0 \leq r_2 < r_1)\,; \\
r_1 &= q_2 r_2 + r_3 && (0 \leq r_3 < r_2)\,; \\
r_2 &= q_3 r_3 + r_4 && (0 \leq r_4 < r_3)\,; \\
&\vdots \\
r_{i-1} &= q_i r_i + r_{i+1} && (0 \leq r_{i+1} < r_i)\,; \\
&\vdots
\end{aligned}$$

Az eljárás véges számú lépés után véget ér: létezik olyan $n \in \mathbb{N}$, hogy $r_{n+1} = 0$. A legnagyobb közös osztó az utolsó nemnulla maradék, azaz $\mathsf{lnko}\,(a, b) = r_n$.

A legnagyobb közös osztó kifejezhető a két szám „lineáris kombinációjaként”: léteznek olyan x, y egész számok, melyekre $ax + by = \mathsf{lnko}\,(a, b)$.

Euklideszi algoritmus

Példa.

$\text{lnko}\,(66, 51) = ? = ? \cdot 66 + ? \cdot 51$ $\text{lnko}(66, 51) = 3 = 7 \cdot 66 - 9 \cdot 51$

Házi feladat.

- $\text{lnko}\,(438, 126) = ? = ? \cdot 438 + ? \cdot 126$
- $\text{lnko}\,(754, 221) = ? = ? \cdot 754 + ? \cdot 221$

while $b \neq 0$ **do**
  $b_0 := b$
  $b := \text{maradék}(a, b)$
  $a := b_0$
end while
return a

while $a \neq b$ **do**
  if $a > b$ **then**
    $a := a - b$
  else
    $b := b - a$
  end if
end while
return a

Relatív prímség

5. Definíció.

Azt mondjuk, hogy az a, b egész számok **relatív prím**ek, ha $\operatorname{lnko}(a, b) = 1$.

Graham, Knuth, Patashnik: Concrete mathematics

4.5 RELATIVE PRIMALITY

When $\gcd(m, n) = 1$, the integers m and n have no prime factors in common and we say that they're *relatively prime*.

This concept is so important in practice, we ought to have a special notation for it; but alas, number theorists haven't agreed on a very good one yet. Therefore we cry: HEAR US, O MATHEMATICIANS OF THE WORLD! LET US NOT WAIT ANY LONGER! WE CAN MAKE MANY FORMULAS CLEARER BY ADOPTING A NEW NOTATION NOW! LET US AGREE TO WRITE '$m \perp n$', AND TO SAY "m IS PRIME TO n," IF m AND n ARE RELATIVELY PRIME. In other words, let us declare that

Like perpendicular lines don't have a common direction, perpendicular numbers don't have common factors.

$$m \perp n \iff m, n \text{ are integers and } \gcd(m, n) = 1. \qquad (4.26)$$

Euklidesz lemmája

6. Tétel.

Tetszőleges a, b nemnulla egész számok esetén $\frac{a}{\text{lnko}(a,b)}$ *és* $\frac{b}{\text{lnko}(a,b)}$ *relatív prím.*

7. Tétel.

Tetszőleges $a, b, c \in \mathbb{Z}$ esetén ha $a \perp b$, akkor $a \mid bc \iff a \mid c$.

8. Tétel (Euklidesz lemmája).

Tetszőleges a, b, c egész számok esetén ha $\text{lnko}(a, b) \neq 0$, *akkor*

$$a \mid bc \iff \frac{a}{\text{lnko}(a, b)} \mid c.$$

Példa.

- $21 \mid 9k \iff ? \mid k$ $_{? = 7}$
- $48 \mid 84k \iff ? \mid k$ $_{? = 4}$
- $84 \mid 48k \iff ? \mid k$ $_{? = 4}$

Házi feladat.

- $125 \mid 150k \iff ? \mid k$
- $150 \mid 125k \iff ? \mid k$
- $143 \mid 78k \iff ? \mid k$

Diofantoszi egyenlet

9. Tétel.

Tetszőleges adott a, b, c nemnulla egész számok esetén az $ax + by = c$ **kétismeretlenes lineáris diofantoszi egyenlet** *akkor és csak akkor oldható meg, ha* $\text{lnko}(a, b) \mid c$. *Ha (x_0, y_0) egy megoldás, akkor bármely $t \in \mathbb{Z}$ esetén az alábbi (x_t, y_t) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a t szám alkalmas megválasztásával:*

$$x_t = x_0 + \frac{b}{\text{lnko}(a, b)} \cdot t; \quad y_t = y_0 - \frac{a}{\text{lnko}(a, b)} \cdot t.$$

Házi feladat.

Befejezni a bizonyítást (y kiszámítása).

Példa.

- $6x + 9y = 51$ (összes mo., nemnegatív megoldások) $x = -17 + 3t, y = 17 - 2t, \quad (1, 5), (4, 3), (7, 1)$
- $6x - 10y = 14$ (összes mo., 0 és 20 közötti megoldások) $x = 14 + 5t, y = 7 + 3t, (4, 1), (9, 4), (14, 7), (19, 10)$

Házi feladat.

- $20x + 45y = 245$ (összes mo., nemnegatív megoldások)
- $117x - 63y = 36$ (összes mo., 0 és 50 közötti megoldások)

Polinomokra minden ugyanúgy megy

Test fölötti polinomokra ugyanúgy elvégezhető a maradékos osztás és az arra épülő euklideszi algoritmus, akárcsak az egész számokra. Az előbbi tételek (és azok bizonyítása) szinte szó szerint lemásolhatók (HF végiggondolni!). Íme a diofantoszi egyenletekről szóló tétel polinomos megfelelője:

10. Tétel.

Legyen T egy test és $f, g, h \in T[x]$ nemnulla polinomok.

Ekkor az $fu + gv = h$ kétismeretlenes lineáris „diofantoszi" egyenlet akkor és csak akkor oldható meg az ismeretlen $u, v \in T[x]$ polinomokra nézve, ha $\operatorname{Inko}(f, g) \mid h$.

Ha (u_0, v_0) egy megoldás, akkor bármely $t \in T[x]$ esetén az alábbi (u_t, v_t) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a t polinom alkalmas megválasztásával:

$$u_t = u_0 + \frac{g}{\operatorname{Inko}(f, g)} \cdot t;$$

$$v_t = v_0 - \frac{f}{\operatorname{Inko}(f, g)} \cdot t.$$

Polinomokra minden ugyanúgy megy

Példa.

Adjuk meg az $fu + gv = \text{lnko}(f, g)$ polinomegyenlet egy megoldását.

- $f = x^5 + 3x^4 + 6x^3 + 6x^2 + 4x + 1,$
  $g = x^3 + 4x^2 + 4x + 3$ $\text{lnko}(f,g) = -17x^2 - 17x - 17, \quad u = -1, \ v = -x^2 + x - 6$
- $f = x^4 + x^3 + x^2 + 1,$
  $g = x^3 + 1$ $\text{lnko}(f,g) = 2, \quad u = x^2 - x - 1, \ v = -x^3 + x + 3$

Házi feladat.

Adja meg az $fu + gv = \text{lnko}(f, g)$ polinomegyenlet egy megoldását.

- $f = x^4 + 2x^3 - x^2 - 4x - 2,$
  $g = x^4 + x^3 - x^2 - 2x - 2$
- $f = x^4 + 4x^3 + (5 + 5i)\,x^2 + (1 + 10i)\,x - 4 + i,$
  $g = x^3 + 2x^2 + (1 + 5i)\,x - 2$

Tartalom

A kongruenciareláció definíciója

11. Definíció.

Legyen $m \geq 2, a, b \in \mathbb{Z}$. Ha $a - b$ osztható m-mel, akkor azt mondjuk, hogy a **kongruens** b**-vel modulo** m. Az m számot a kongruencia **modulusának** nevezzük.

Jelölés.

A kongruenciát $\equiv$ jelöli, a modulust utána zárójelben tüntetjük fel a mod rövidítést használva (de ezt időnként elhagyjuk). Tehát $a \equiv b \pmod{m} \iff m \mid a - b$.

12. Tétel.

Tetszőleges $m \geq 2, a, b \in \mathbb{Z}$ *esetén* $a \equiv b \pmod{m}$ *akkor és csak akkor teljesül, ha* a *és* b *ugyanazt a maradékot adja* m*-mel osztva.*

A kongruenciareláció tulajdonságai

13. Tétel.

Tetszőleges $m, m_1, m_2 \geq 2, a, b, c, a_1, b_1, a_2, b_2 \in \mathbb{Z}$ *esetén érvényesek az alábbiak:*

(1) $a \equiv a \pmod{m}$ *(reflexivitás);*

(2) $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ *(szimmetria);*

(3) $(a \equiv b \pmod{m}$ *és* $b \equiv c \pmod{m}) \implies a \equiv c \pmod{m}$ *(tranzitivitás);*

(4) $\left.\begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array}\right\} \implies a_1 \pm a_2 \equiv b_1 \pm b_2, \quad a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}$;

(5) *ha* $c \neq 0$, *akkor* $ca \equiv cb \pmod{m} \iff a \equiv b \left(\mathrm{mod}\ \frac{m}{\mathrm{lnko}(m,c)}\right)$;

(6) *ha* $\mathrm{lnko}(m, c) = 1$, *akkor* $ca \equiv cb \pmod{m} \iff a \equiv b \pmod{m}$;

(7) $\left.\begin{array}{l} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \end{array}\right\} \iff a \equiv b \pmod{[m_1, m_2]}$;

(8) *ha* $a \equiv b \pmod{m}$, *akkor* $\mathrm{lnko}(a, m) = \mathrm{lnko}(b, m)$.

Házi feladat.

(1)–(3) bizonyítása.

Oszthatósági feladatok megoldása kongruenciával

Példa.

Kongruenciák segítségével igazoljuk az alábbi oszthatóságokat:

- $24 \mid 5^{20} - 1$;
- $19 \mid 3^{111} + 2^{444}$;
- $7 \mid 3^{201} + 2^{102}$;
- $7 \mid 3^{2n+1} + 2^{n+2}$.

Házi feladat.

Kongruenciák segítségével igazolja az alábbi oszthatóságokat:

- $29 \mid 3^{333} + 2^{111}$;
- $40 \mid 29^{98} - 1$;
- $13 \mid 4^{2n+1} + 3^{n+2}$;
- $27 \mid 2^{5n+1} + 5^{n+2}$.

Oszthatósági feladatok megoldása kongruenciával

Példa.

Mikor osztható $5^n - 1$ tizenhárommal? Acsa, ha $4 \mid n$.

Házi feladat.

Mikor osztható $2^n - 1$ héttel? No és $2^n + 1$?

Példa.

Kongruenciák segítségével igazoljuk a 9-cel való oszthatóság szabályát:

$$\overline{a_n \cdots a_2 a_1 a_0} \equiv a_0 + a_1 + a_2 + \cdots + a_n \pmod 9 .$$

Házi feladat.

Kongruenciák segítségével igazolja a 11-gyel való oszthatóság szabályát:

$$\overline{a_n \cdots a_2 a_1 a_0} \equiv a_0 - a_1 + a_2 - \cdots + (-1)^n a_n \pmod{11} .$$

Házi feladat.

Mikor lehet egy csupa 9-es számjegyekből álló szám négyzetszám? (Útmutatás: vizsgáljuk a modulo 4 maradékot.)

Maradékosztályok

14. Definíció.

Egy a egész szám modulo m **maradékosztályán** az $\overline{a} = \{b \in \mathbb{Z} \colon a \equiv b \pmod{m}\}$ halmazt értjük.

Jelölés.

A modulo m maradékosztályok halmazát $\mathbb{Z}_m$ jelöli. Tehát

$$\mathbb{Z}_m = \{\overline{a} : a \in \mathbb{Z}\} = \left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}.$$

15. Definíció.

A modulo m maradékosztályok halmazán értelmezzük az első három alapműveletet a következőképpen: tetszőleges $a, b \in \mathbb{Z}$ esetén legyen

$$\overline{a} + \overline{b} = \overline{a+b},\ \overline{a} - \overline{b} = \overline{a-b},\ \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

16. Tétel.

A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (különbsége, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik számot választjuk reprezentánsnak. Ezekkel a műveletekkel $\mathbb{Z}_m$ kommutatív egységelemes gyűrűt alkot (modulo m **maradékosztály-gyűrű**).

Házi feladat.

Befejezni a bizonyítást.

Számolás maradékosztályokkal

Példa.

Számoljunk $\mathbb{Z}_7$-ben!

- $\overline{3}+\overline{6}=?$ $?=\overline{2}$
- $\overline{3}-\overline{6}=?$ $?=\overline{4}$
- $\overline{3}\cdot\overline{6}=?$ $?=\overline{4}$
- $\overline{2}^5=?$ $?=\overline{4}$

Házi feladat.

Számoljon $\mathbb{Z}_{12}$-ben!

- $\overline{6}+\overline{8}=?$
- $\overline{6}-\overline{8}=?$
- $\overline{6}\cdot\overline{8}=?$
- $\overline{5}^3=?$

Példa.

$\mathbb{Z}_4$ összeadó- és szorzótáblája:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Házi feladat.

Írja fel $\mathbb{Z}_5$ összeadó- és szorzótábláját.

Polinomok $\mathbb{Z}_p$ felett

Ha p prím, akkor $\mathbb{Z}_p$ test, és így beszélhetünk $\mathbb{Z}_p$ feletti polinomokról. Ezekkel ugyanúgy (vagy könnyebben!) lehet számolni, mint számtest feletti polinomokkal.

Példa.

Adjuk meg az $fu + gv = \text{lnko}(f, g)$ polinomegyenlet egy megoldását a $\mathbb{Z}_2[x]$ polinomgyűrűben.

$$f = x^4 + x^3 + x^2 + \overline{1},\ g = x^3 + \overline{1}$$ $\text{lnko}(f,g) = x + \overline{1},\quad u = x + \overline{1},\ v = x^2$

Házi feladat.

Adja meg az $fu + gv = \text{lnko}(f, g)$ polinomegyenlet egy megoldását a $\mathbb{Z}_2[x]$ polinomgyűrűben.

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

Példa.

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

$$f = x^4 + \overline{6}x^3 + \overline{3}x^2 + \overline{2}x + \overline{4},\ g = x^2 + \overline{6}x + \overline{3}$$ $u = \overline{5}x + \overline{6},\ v = \overline{2}x^3 + x^2 + \overline{4}$

Házi feladat.

Adja meg az $fu + gv = \overline{1}$ polinomegyenlet egy megoldását a $\mathbb{Z}_5[x]$ polinomgyűrűben.

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

Redukált maradékosztályok

17. Megjegyzés.

A 13. Tételbeli utolsó állítás szerint van értelme egy mod m maradékosztály és az m modulus legnagyobb közös osztójáról beszélni (hiszen nem függ a reprezentáns választásától). Később fontos szerepet játszanak majd azok a maradékosztályok, amelyek relatív prímek a modulushoz, ezért erre külön elnevezést és jelölést vezetünk be.

18. Definíció.

Az $\overline{a} \in \mathbb{Z}_m$ maradékosztályt **redukált maradékosztálynak** hívjuk, ha $\text{lnko}(a, m) = 1$.

Jelölés.

A mod m redukált maradékosztályok halmazát $\mathbb{Z}_m^*$ jelöli. Tehát

$$\mathbb{Z}_m^* = \left\{\overline{a} \in \mathbb{Z}_m : \text{lnko}\,(a, m) = 1\right\}.$$

Példa.

$\mathbb{Z}_5^* = ?$, $? = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ $\mathbb{Z}_6^* = ?$, $? = \{\overline{1}, \overline{5}\}$ $\mathbb{Z}_{10}^* = ?$ $? = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$

Házi feladat.

$\mathbb{Z}_{12}^* = ?$, $\mathbb{Z}_{13}^* = ?$, $\mathbb{Z}_{16}^* = ?$

Tartalom

Lineáris kongruenciák

19. Definíció.

Lineáris kongruenciának nevezzük az $ax \equiv b \pmod{m}$ alakú „egyenletet”, ahol a, b, m adott egész számok, és az x ismeretlent is az egész számok körében keressük.

Példa.

Oldjuk meg az alábbi lineáris kongruenciákat.

- $3x \equiv 4 \pmod{5}$ $x \equiv 3 \pmod{5}$.
- $6x \equiv 21 \pmod{9}$ $x \equiv 2, 5, 8 \pmod{9}$.
- $40x \equiv 28 \pmod{62}$ $x \equiv 10, 41 \pmod{62}$.

Házi feladat.

Oldja meg az alábbi lineáris kongruenciákat.

- $12x \equiv 44 \pmod{10}$
- $24x \equiv 84 \pmod{45}$
- $104x \equiv 74 \pmod{60}$
- $13x \equiv 6 \pmod{41}$

Lineáris kongruenciák

20. Tétel.

Az $ax \equiv b \pmod{m}$ *lineáris kongruencia akkor és csak akkor oldható meg, ha* $\operatorname{lnko}(a, m) \mid b$.

Ha ez teljesül, akkor a megoldások egyetlen modulo $\frac{m}{\operatorname{lnko}(a,m)}$ *maradékosztályt alkotnak, modulo* m *pedig* $\operatorname{lnko}(a, m)$ *a megoldások száma.*

Ha x_0 *egy megoldás, akkor az összes megoldás:*

$$x \equiv x_0 + t \cdot \frac{m}{\operatorname{lnko}(a, m)} \pmod{m} \quad (t = 0, 1, \ldots, \operatorname{lnko}(a, m) - 1).$$

Multiplikatív inverz

21. Definíció.

Azt mondjuk, hogy az a, b egész számok egymás **multiplikatív inverzei** modulo m, ha $ab \equiv 1 \pmod{m}$.
Hasonlóan $\overline{a}, \overline{b} \in \mathbb{Z}_m$ egymás multiplikatív inverzei, ha $\overline{a} \cdot \overline{b} = \overline{1}$.

Jelölés.

Ha nem fenyeget a félreértés veszélye, akkor az a egész szám mod m multiplikatív inverzét a^{-1}-gyel jelöljük. Hasonlóan $\overline{a} \in \mathbb{Z}_m$ multiplikatív inverzét $\overline{a}^{-1}$ jelöli.

22. Tétel.

Az a egész számnak akkor és csak akkor van multiplikatív inverze modulo m, ha $\operatorname{lnko}(a, m) = 1$. *Ilyenkor a multiplikatív inverz* mod m *egyértelműen meghatározott. Hasonlóan, $\overline{a} \in \mathbb{Z}_m$ akkor és csak akkor rendelkezik multiplikatív inverzzel, ha $\overline{a} \in \mathbb{Z}_m^*$. Ilyenkor a multiplikatív inverz egyértelműen meghatározott.*

23. Következmény.

A $\mathbb{Z}_m$ maradékosztály-gyűrű akkor és csak akkor test, ha m prímszám.

Multiplikatív inverz

Példa.

Határozza meg $\mathbb{Z}_{14}$ elemeinek multiplikatív inverzét. $\overline{1}^{-1} = \overline{1}$, $\overline{3}^{-1} = \overline{5}$, $\overline{5}^{-1} = \overline{3}$, $\overline{9}^{-1} = \overline{11}$, $\overline{11}^{-1} = \overline{9}$, $\overline{13}^{-1} = \overline{13}$

Házi feladat.

Határozza meg $\mathbb{Z}_{15}$ elemeinek multiplikatív inverzét.

24. Tétel (Wilson tétele).

Ha p prímszám, akkor $(p-1)! \equiv -1 \pmod{p}$.

Házi feladat.

Mit ad $(n-1)!$ maradékul n-nel osztva, ha n összetett szám?

Negatív kitevős hatványozás

25. Definíció.

Ha a és m relatív prímek, akkor tetszőleges $k \in \mathbb{N}$ esetén értelmezzük az a^{-k} negatív kitevőjű hatványt modulo m: legyen $a^{-k} \equiv \left(a^k\right)^{-1} \pmod{m}$.

Hasonlóképpen $\overline{a} \in \mathbb{Z}_m^*$ esetén legyen $(\overline{a})^{-k} = \left(\overline{a}^k\right)^{-1}$.

26. Megjegyzés.

Meg lehet mutatni, hogy a hatványozás szokásos azonosságai érvényben maradnak az egész kitevős mod m hatványok fenti értelmezése mellett.

Példa.

Számítsuk ki $\mathbb{Z}_{11}$-ben a $\overline{2}^{-3}$ hatványt. $\overline{2}^{-3} = (\overline{2}^{-1})^3 = \overline{6}^3 = \overline{7}$ vagy $\overline{2}^{-3} = (\overline{2}^3)^{-1} = \overline{8}^{-1} = \overline{7}$

Házi feladat.

Számítsa ki $\mathbb{Z}_{13}$-ban a $\overline{2}^{-3}$ hatványt.

Házi feladat.

Számítsa ki $\mathbb{Z}_{17}$-ben a $\overline{3}^{-4}$ hatványt.

Polinomokra minden ugyanúgy megy

Ha T egy test (például $T = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ vagy $\mathbb{Z}_p$) és $f \in T[x]$, akkor a modulo f kongruencia és a modulo f maradékosztályok ugyanúgy definiálhatóak, mint az egész számok körében, és hasonló tulajdonságokkal rendelkeznek (HF végiggondolni!). A maradékosztály-gyűrűt itt $T[x]/(f)$ jelöli.

27. Tétel.

Ha f egy n-edfokú polinom a T test felett, akkor a $T[x]/(f)$ maradékosztály-gyűrű kommutatív egységelemes gyűrű, melyenek elemei egyértelműen felírhatók az alábbi alakban:

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \qquad (a_{n-1}, \ldots, a_1, a_0 \in T).$$

28. Tétel.

Az $\overline{u} \in T[x]/(f)$ maradékosztálynak akkor és csak akkor van multiplikatív inverze, ha u és m relatív prímek.

29. Következmény.

A $T[x]/(f)$ maradékosztály-gyűrű akkor és csak akkor test, ha m irreducibilis T felett.

Házi feladat.

A fenti tételek bizonyítása.

Egy fontos maradékosztálytest

Az $\mathbb{R}[x] / (x^2+1)$ maradékosztály-gyűrű test, mert x^2+1 irreducibilis a valós számok teste felett. Mik az elemei ennek a testnek, és hogyan kell számolni velük?

- Elemek: Az $\mathbb{R}[x] / (x^2+1)$ test minden eleme egyértelműen felírható a következő alakban:
$$\overline{a+bx} \qquad (a, b \in \mathbb{R}).$$
- Összeadás: $\overline{a+bx} + \overline{c+dx} = \overline{(a+c)+(b+d)x}.$
- Szorzás:
$$\begin{aligned} \overline{a+bx} \cdot \overline{c+dx} &= \overline{ac+(ad+bc)x+cdx^2} = \\ &= \overline{ac+(ad+bc)x+cd(-1)} = \\ &= \overline{(ac-bd)+(ad+bc)x}. \end{aligned}$$

Ez szinte szó szerint ugyanaz, mint a komplex számok teste: $\mathbb{R}[x] / (x^2+1) \cong \mathbb{C}$.

30. Megjegyzés.

A fenti példához hasonlóan minden $f \in T[x]$ irreducibilis polinomnak lehet „gyököt csinálni”: a $T[x] / (f)$ maradékosztálytest egy olyan kibővítése a T testnek, amelyben f-nek van gyöke.

Egy véges test

Példa.
Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + \overline{1}\right)$ testben! Ennek 8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+\overline{1}},\ \overline{x^2},\ \overline{x^2+\overline{1}},\ \overline{x^2+x},\ \overline{x^2+x+\overline{1}}.$$

$$\overline{x+\overline{1}} + \overline{x^2+x} = \overline{x^2+\overline{2}x+\overline{1}} = \overline{x^2+\overline{1}} \qquad \text{(semmi vész)}$$

$$\overline{x+\overline{1}} \cdot \overline{x^2+x} = \overline{x^3+\overline{2}x^2+x} = \overline{x^3+x} = \overline{\overline{1}} \qquad \text{(redukció mod } x^3+x+\overline{1}\text{)}$$

Házi feladat.
Sorolja fel a $\mathbb{Z}_2[x] / \left(x^2 + x + \overline{1}\right)$ négyelemű test elemeit, és írja fel az összeadás és a szorzás művelettáblázatát.

A nyolcelemű test művelettáblázatai

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Számolás véges testekben

Példa.

Számítsuk ki a $\mathbb{Z}_5[x] / (x^3 + x + 1)$ gyűrűben a $\overline{3x^2 + 2}$ elem inverzét. (Hány eleme van ennek a gyűrűnek? Test-e ez a gyűrű?)

Igen, test (mert $x^3 + x + 1$ irreducibilis $\mathbb{Z}_5$ felett), és 125 eleme van. $\overline{2x^2 + 4x + 4}$

Házi feladat.

Számítsa ki a $\mathbb{Z}_5[x] / (x^3 + x^2 + x + 1)$ gyűrűben a $\overline{2x^2 + 4}$ elem inverzét. (Hány eleme van ennek a gyűrűnek? Test-e ez a gyűrű?)

Házi feladat.

Számítsa ki a $\mathbb{Z}_3[x] / (x^2 + 1)$ gyűrűben az $u \cdot v$, u/v, v/u elemeket, ahol $u = \overline{x}$ és $v = \overline{x + 1}$. (Hány eleme van ennek a gyűrűnek? Test-e ez a gyűrű?)

Számolás $\mathbb{Q}[x]$ faktortesteiben

Példa.

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$\begin{aligned}
\overline{2 - x}^{-1} = \overline{u} &\iff \overline{2 - x} \cdot \overline{u} = \overline{1} \\
&\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2 - x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7} \\
&\iff \overline{u} = \overline{x^2 + 2x + 4}
\end{aligned}$$

Tehát $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$.

Hab a tortán

Példa (folyt.).

Az előző számolás eredménye összefoglalva:

$$(2-x)(x^2+2x+4) = 1 + (x^3-7)\cdot(\ldots \text{valami polinom} \ldots).$$

Írjunk x helyébe $\sqrt[3]{7}$-et:

$$(2-\sqrt[3]{7})(\sqrt[3]{49}+2\sqrt[3]{7}+4) = 1 + (7-7)\cdot(\ldots \text{valami szám} \ldots).$$

Tehát azt kapjuk, hogy

$$\frac{1}{2-\sqrt[3]{7}} = \sqrt[3]{49}+2\sqrt[3]{7}+4.$$

Ezzel a módszerrel (lényegében az euklideszi algoritmussal) lehet bonyolult nevezőket gyöktelenníteni.

Számolás $\mathbb{Q}[x]$ faktortesteiben

Házi feladat.
Határozza meg a $K = \mathbb{Q}[x] / \left(x^3 - 2\right)$ testben az $\overline{x^2 + 3x + 4}$ elem multiplikatív inverzét. Értelmezze az eredményt tört nevezőjének gyöktelenítéseként.

Házi feladat.
Határozza meg a $K = \mathbb{Q}[x] / \left(x^3 + x + 1\right)$ testben az $\overline{x^2}$ elem multiplikatív inverzét.

Tartalom

Lineáris kongruenciarendszerek

31. Definíció.

Adott $a_i, b_i, n_i \ \ (i = 1, 2, \ldots, k)$ egész számok esetén az alábbi „egyenletrendszert" **lineáris kongruenciarendszer**nek nevezzük (az x ismeretlent is természetesen az egész számok körében keressük):

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{n_k} \end{aligned}\right\}$$

32. Megjegyzés.

A 20. Tétel segítségével a kongruenciarendszerbeli kongruenciákat külön-külön megoldhatjuk (ha van megoldásuk), és így a kongruenciarendszert a következő alakra hozhatjuk:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}\right\} \qquad (*)$$

Lineáris kongruenciarendszerek

Példa.

Oldjuk meg az alábbi kongruenciarendszert.

$$\left.\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 6 \end{aligned}\right\} \quad x \equiv 9 \pmod{12}.$$

Házi feladat.

Oldja meg az alábbi kongruenciarendszert.

$$\left.\begin{aligned} 4x &\equiv 7 \pmod 9 \\ 10x &\equiv 4 \pmod{12} \end{aligned}\right\}$$

Példa.

Oldjuk meg az alábbi kongruenciarendszert.

$$\left.\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 6 \\ x &\equiv 1 \pmod 8 \end{aligned}\right\} \quad x \equiv 9 \pmod{24}.$$

Házi feladat.

Oldja meg az alábbi kongruenciarendszert.

$$\left.\begin{aligned} 5x &\equiv 11 \pmod 6 \\ 2x &\equiv 5 \pmod 9 \\ 4x &\equiv 7 \pmod 5 \end{aligned}\right\}$$

Lineáris kongruenciarendszerek

33. Tétel.

Ha a $(*)$ *lineáris kongruenciarendszernek van megoldása, akkor megoldásai egyetlen* $\mathrm{mod}\,[m_1, m_2, \ldots, m_k]$ *maradékosztályt alkotnak.*

34. Tétel.

A $(*)$ *lineáris kongruenciarendszer* $k = 2$ *esetén pontosan akkor oldható meg, ha* $\mathrm{lnko}\,(m_1, m_2) \mid c_1 - c_2$.

35. Tétel.

A $(*)$ *lineáris kongruenciarendszer akkor és csak akkor oldható meg, ha bármely két kongruenciából álló részrendszere megoldható. Speciálisan, páronként relatív prím modulusok esetén mindig van megoldás.*

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}\right\} \qquad (*)$$

Kínai maradéktétel

Példa.

Oldjuk meg az alábbi kongruenciarendszert.

$$\left.\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}\right\} \quad x \equiv 53 \pmod{60}.$$

Példa.

Oldjuk meg az alábbi kongruenciarendszert.

$$\left.\begin{aligned} x &\equiv a \pmod 3 \\ x &\equiv b \pmod 4 \\ x &\equiv c \pmod 5 \end{aligned}\right\} \quad x \equiv 40a + 45b + 36c \pmod{60}.$$

Házi feladat.

Oldja meg az alábbi kongruenciarendszert.

$$\left.\begin{aligned} x &\equiv a \pmod 3 \\ x &\equiv b \pmod 5 \\ x &\equiv c \pmod 7 \end{aligned}\right\}$$

Kínai maradéktétel

36. Tétel (kínai maradéktétel).

Tegyük fel, hogy az $m_1, m_2, \ldots, m_k$ *modulusok páronként relatív prímek, jelölje a szorzatukat* M*, továbbá legyen* $M_i = \frac{M}{m_i}$ $(i = 1, 2, \ldots, k)$.

Jelölje y_i *az* $M_i y_i \equiv 1 \pmod{m_i}$ *segédkongruencia egy megoldását* $(i = 1, \ldots, k)$.

Ekkor a $(*)$ *lineáris kongruenciarendszer megoldása:*

$$x \equiv \sum_{i=1}^{k} c_i M_i y_i \pmod{M}.$$

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_k \pmod{m_k} \end{aligned}\right\} \qquad (*)$$

Megértést ellenőrző kérdések

Igazak-e az alábbi állítások?

- Az $ax \equiv b \pmod{m}$ lineáris kongruenciának akkor és csak akkor van megoldása, ha $\text{lnko}(a, b) \mid m$.
- A $30x \equiv 48 \pmod{58}$ kongruencia ekvivalens a $30x \equiv 48 \pmod{29}$ kongruenciával.
- Az $1, 133, 265, 397, \ldots$ és az $1, 151, 301, 451, \ldots$ számtani sorozatok második közös tagja 19801.
- Minden p prímszámra $(p-1)! \equiv p-1 \pmod{p}$.
- Az egész számok halmazán a modulo m kongruencia antiszimmetrikus reláció.
- $|\mathbb{Z}_{15}^*| = |\mathbb{Z}_8|$
- Léteznek olyan a, b, c egész számok, amelyekre az $ax + by = c$ diofantoszi egyenletnek pontosan 2014 megoldása van (az egész számok körében).
- Tetszőleges a, b, c egész számokra $a \mid bc \implies a \mid b$ vagy $a \mid c$.