ALGEBRA ÉS SZÁMELMÉLET 3

gyakorló és házifeladatok

2021 őszi félév, OT

1. feladat. Számítsa ki a $\pi \cdot \rho$ és $\rho \cdot \pi$ permutációkat. Végezze el a számolást kétsoros alakban és idegen ciklusok szorzatára bontott alakban is.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 6 & 4 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$$

Megoldás. Kétsoros alakban számolva:

$$\pi \cdot \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 6 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 5 & 4 \end{pmatrix}$$

$$\rho \cdot \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 6 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 3 & 2 & 4 & 6 \end{pmatrix}$$

Idegen ciklusok szorzataként felírva:

$$\pi \cdot \rho = (13)(2564) \cdot (123)(56) = (2643)$$
$$\rho \cdot \pi = (123)(56) \cdot (13)(2564) = (1542)$$

Láthatjuk, hogy $\pi \cdot \rho \neq \rho \cdot \pi$, azaz a permutációk szorzása nem kommutatív. (Ellenőrizzük, hogy a $\pi\rho$ permutációra mindkét módszerrel ugyanaz az eredmény jött ki, és hasonlóan a $\rho\pi$ permutációra is.)

---

2. feladat. Adja meg idegen ciklusok szorzataként az $(1234)^{-1}(1524)(1234) \in S_5$ permutációt.

Megoldás. $(1234)^{-1}(1524)(1234) = (4321)(1524)(1234) = (2531)$

---

3. feladat. Írja fel kétsoros alakban a π^{605} permutációt, ahol $\pi = (132)(5324) \in S_6$.

Megoldás. Itt arra kell vigyázni, hogy $\pi^{605} \neq (132)^{605} \cdot (5324)^{605}$, mert az (132) és (5324) permutációk nem cserélhetőek fel. Bontsuk a π permutációt idegen ciklusok szorzatára: $\pi = (12)(345)$. Így már tudunk tényezőnként hatványozni (felhasználva, hogy $(12)^2 = \mathrm{id}$ és $(345)^3 = \mathrm{id}$): $\pi^{605} = (12)^{605} \cdot (345)^{605} = (12) \cdot (345)^2 = (12)(354)$. Ezt a permutációt írjuk át kétsoros alakba (ne feledkezzünk el a 6-osról sem, hiszen S_6-ban vagyunk):

$$\pi^{605} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 4 & 6 \end{pmatrix}.$$

---

4. feladat. Adja meg idegen ciklusok szorzataként az $((1243)^{-6}(154)^{13})^{-4} \in S_7$ permutációt.

Megoldás. Először számítsuk ki a két ciklus hatványát külön-külön: $(1243)^{-6} = (3421)^6 = (3421)^2 = (32)(41)$ és $(154)^{13} = (154)^1 = (154)$. Ezután végezzük el a szorzást, azaz bontsuk idegen ciklusok szorzatára a a zárójelen belüli permutációt: $(32)(41)(154) = (23)(45)$. Végül ennek a permutációnak kell venni a (-4)-edik hatványát: $((23)(45))^{-4} = (23)^{-4} \cdot (45)^{-4} = \mathrm{id} \cdot \mathrm{id} = \mathrm{id}$.
Lehetett volna úgy is számolni, hogy először a külső inverzképzést végezzük el (a negyedik hatványra emelést azonban addig nem végezhetjük el, amíg a zárójelen belül nem idegenek a ciklusok!):

$$((1243)^{-6}(154)^{13})^{-4} = ((154)^{-13}(1243)^6)^4 = ((154)^2(1243)^6)^4 = ((145)(14)(23))^4 = ((45)(23))^4 = \mathrm{id}\,.$$

---

5. feladat. Határozza meg a következő három permutáció paritását (a π permutációt lásd a 3. feladatban):

$$\alpha = (12)(45)(1245), \quad \beta = \big((1346)(45761)(352)(41625)\big)^{2019}, \quad \gamma = \pi^{33550336}.$$

Megoldás. Számítsuk ki a permutációk előjeleit az 1.22. Tétel és az 1.27. Következmény segítségével:

- $\mathrm{sgn}(\alpha) = \mathrm{sgn}((12)) \cdot \mathrm{sgn}((45)) \cdot \mathrm{sgn}((1245)) = (-1) \cdot (-1) \cdot (-1) = -1$,
  tehát α páratlan permutáció.
- $\mathrm{sgn}(\beta) = \big(\mathrm{sgn}((1346)) \cdot \mathrm{sgn}((45761)) \cdot \mathrm{sgn}((352)) \cdot \mathrm{sgn}((41625))\big)^{2019} = \big((-1) \cdot (+1) \cdot (+1) \cdot (+1)\big)^{2019} = (-1)^{2019} = -1$,
  tehát β páratlan permutáció.
- $\mathrm{sgn}(\gamma) = \big(\mathrm{sgn}(\pi)\big)^{33550336} = 1$ (függetlenül attól, hogy mi is volt a π permutáció!),
  tehát γ páros permutáció.

Egy másik megoldási lehetőség, hogy a permutációkat transzpozíciók szorzatára bontjuk, és használjuk az 1.28. Tételt. Pontosabban nem is kell felbontani őket transzpozíciók szorzatára, elég elképzelni egy felbontást, és megszámolni a transzpozíciókat. Nem kell a lehető legrövidebb felbontásra törekedni (bár az is érdekes feladat); bármilyen felbontás jó, mert minden

felbontásban ugyanaz lesz a transzpozíciók számának paritása. Felhasználjuk, hogy egy k hosszúságú ciklus felbontható $k-1$ transzpozíció szorzatára (lásd az 1.25. Tétel bizonyítását).

α: $1+1+3=5$ páratlan

β: $2019\cdot(3+4+2+4)=2019\cdot 13$ páratlan

γ: $33550336\cdot(2+3)=33550336\cdot 5$ páros

---

6. feladat. Oldja meg S_6-ban az $(123)(2345)\pi(456)=(134)$ egyenletet.

7. feladat. Oldja meg S_5-ben a $\pi^2=(134)$ egyenletet. (Több megoldás van; az összeset keressük meg!)

8. feladat. Milyen lehet egy S_4-beli permutáció ciklusszerkezete? Sorolja fel az összes lehetőséget, és minden ciklusszerkezetnél adja meg, hogy hány olyan permutáció van (nem kell felsorolni őket!), és hogy milyen a paritásuk. (Egy permutáció ciklusszerkezetén azt értjük, hogy az idegen ciklusok szorzatára bontott alakjában hány ciklus szerepel és milyen hosszúak ezek. Pl. bármely két transzpozíciónak ugyanolyan a ciklusszerkezete.)

9. feladat. Egy 32 lapos magyarkártya-pakli „tökéletes" keverésénél a paklit pontosan középen kettéosztjuk, és a két felet „fésűsen" egyesítjük (az eredetileg felül lévő lap kerül felülre, és az eredetileg alul lévő lap kerül alulra). Milyen a ciklusszerkezete a keverést leíró permutációnak? Mi történik, ha többször egymás után végrehajtjuk ezt a keverést?

10. feladat. Döntse el, hogy igazak-e az alábbi állítások. (A választ természetesen indokolni kell!)

(a) Minden $\pi\in S_3$ permutációra $\pi^6=\mathrm{id}$.

(b) Tetszőleges $\pi\in S_{10}$ permutációra, ha $\pi^2=\mathrm{id}$, akkor π transzpozíció.

(c) Négy S_7-beli permutáció szorzata mindig páros.

---

11. feladat. Írja fel az $A=\{1,2,3,4,5\}$ halmazon az alábbi ρ relációhoz tartozó osztályozást:

$$\rho=\big\{(1,1),(1,3),(1,4),(2,2),(2,5),(3,1),(3,3),(3,4),(4,1),(4,3),(4,4),(5,2),(5,5)\big\}.$$

Megoldás. Először írjuk fel az egyes elemek ekvivalenciaosztályait (segíthet, ha felrajzoljuk a reláció gráfját):

$$\overline{1}=\{1,3,4\},\ \ \overline{2}=\{2,5\},\ \ \overline{3}=\{1,3,4\},\ \ \overline{4}=\{1,3,4\},\ \ \overline{5}=\{2,5\}.$$

Ennek alapján a ρ-hoz tartozó osztályozás:

$$A/\rho=\Big\{\{1,3,4\},\{2,5\}\Big\}.$$

---

12. feladat. Írja fel az $A=\{u,v,w,z\}$ halmazon a $\mathcal{C}=\Big\{\{u,w\},\{v,z\}\Big\}$ osztályozáshoz tartozó ekvivalenciarelációt (vagyis azt a ρ ekvivalenciarelációt, amelyre $A/\rho=\mathcal{C}$).

Megoldás. Egy elempár akkor és csak akkor lesz benne a ρ halmazban, ha a két elem ugyanabba az osztályba esik:

$$\rho=\big\{(u,u),(w,w),(u,w),(w,u),\ \ (v,v),(z,z),(v,z),(z,v)\big\}.$$

---

13. feladat. Legyen ρ az $A=\{u,v,w,z\}$ halmazon a $\mathcal{C}=\Big\{\{u,w\},\{v,z\}\Big\}$ osztályozáshoz tartozó ekvivalenciareláció (vagyis $A/\rho=\mathcal{C}$). Melyek igazak az alábbi állítások közül?

(a) $(u,v)\in\rho$ (d) $\{u,w\}\in\rho$ (g) $\{u,v\}\in\mathcal{C}$

(b) $(u,w)\in\rho$ (e) $(u,v)\in\mathcal{C}$ (h) $\{u,w\}\in\mathcal{C}$

(c) $\{u,v\}\in\rho$ (f) $(u,w)\in\mathcal{C}$ (i) $\{u,w\}\subseteq\mathcal{C}$

Megoldás. Az előző feladatban felírtuk a ρ reláció elemeit, de próbáljuk meg anélkül kitalálni a válaszokat.

(a) $(u,v)\in\rho$: Hamis, mert u és v nincsenek egy osztályban.

(b) $(u,w)\in\rho$: Igaz, mert u és w egy osztályban vannak.

(c) $\{u,v\}\in\rho$: Hamis, mert ρ elemei elempárok, nem pedig halmazok.

(d) $\{u,w\}\in\rho$: Hamis, mert ρ elemei elempárok, nem pedig halmazok.

(e) $(u,v)\in\mathcal{C}$: Hamis, mert $\mathcal{C}$ elemei halmazok, nem pedig elempárok.

(f) $(u,w)\in\mathcal{C}$: Hamis, mert $\mathcal{C}$ elemei halmazok, nem pedig elempárok.

(g) $\{u,v\}\in\mathcal{C}$: Hamis, mert a $\mathcal{C}$ halmaz két eleme közül egyik sem $\{u,v\}$.

(h) $\{u,w\}\in\mathcal{C}$: Igaz, mert a $\mathcal{C}$ halmaz két eleme közül az egyik éppen $\{u,w\}$.

(i) $\{u,w\}\subseteq\mathcal{C}$: Hamis, mert $\{u,w\}\subseteq\mathcal{C}$ azt jelenti, hogy $u\in\mathcal{C}$ és $w\in\mathcal{C}$, de se u, se w nem eleme $\mathcal{C}$-nek.

14. feladat. Határozza meg az $A/\ker f$ osztályozást, ahol $A = \{-2, \dots, 3\}$ és $f\colon A \to \mathbb{Z}$, $x \mapsto |x|$. Írja fel az osztályozást akkor is, ha az abszolútérték-függvényt az egész számok halmazán értelmezzük.

Megoldás. Két elem akkor és csak akkor kerül egy osztályba, ha f ugyanazt rendeli hozzájuk. Számítsuk ki minden elem f melletti képét:

$$(-2)f = 2,\ \ (-1)f = 1,\ \ 0f = 0,\ \ 1f = 1,\ \ 2f = 2,\ \ 3f = 3.$$

Ennek alapján már fel tudjuk írni a mag szerinti osztályozást:

$$A/\ker f = \Big\{\{0\},\ \{-1,1\},\ \{-2,2\},\ \{3\}\Big\}.$$

Figyeljük, meg, hogy f értékkészlete $\{0,1,2,3\}$, és a mag szerinti ekvivalenciaosztályok megfelelnek az értékkészlet elemeinek: $\{0\}$ azon elemek halmaza, amelyekhez 0-t rendel az f leképezés, $\{-1,1\}$ azon elemek halmaza, amelyekhez 1-et rendel az f leképezés, $\{-2,2\}$ azon elemek halmaza, amelyekhez 2-t rendel az f leképezés, $\{3\}$ pedig azon elemek halmaza, amelyekhez 3-at rendel az f leképezés.
Ha az egész számok halmazát vesszük alaphalmaznak, akkor az értékkészlet $\mathbb{N}_0$, és adott $k \in \mathbb{N}_0$ esetén azon elemek halmaza, amelyekhez k-t rendel az f leképezés: $\{-k,k\}$ ($k = 0$ esetén ez egyelemű halmaz, egyébként kételemű). Tehát

$$\mathbb{Z}/\ker f = \Big\{\{0\},\{-1,1\},\{-2,2\},\dots\Big\} = \Big\{\,\{-k,k\} : k \in \mathbb{N}_0\Big\}.$$

---

15. feladat. Legyen $A = \{0, \dots, 7\}$ és $\psi\colon A \to \mathbb{Z}$, $x \mapsto \lfloor x/3 \rfloor$. Határozza meg az $A/\ker\psi$ osztályozást.

Megoldás. $A/\ker\psi = \Big\{\{0,1,2\},\ \{3,4,5\},\ \{6,7\}\Big\}$.

---

16. feladat. Határozza meg az $A/\ker\xi$ osztályozást, ahol $A = \{-2, \dots, 3\}$ és $\xi\colon A \to \mathbb{Z}$, $x \mapsto \operatorname{sgn} x$. Írja fel az osztályozást akkor is, ha a szignum függvényt a valós számok halmazán értelmezzük.

Megoldás. $A/\ker\xi = \Big\{\{-2,-1\},\ \{0\},\ \{1,2,3\}\Big\}$ és $\mathbb{R}/\ker\xi = \Big\{\,\mathbb{R}^-,\ \{0\}\,,\ \mathbb{R}^+\,\Big\}$.

---

17. feladat. Az alábbi linken található játékban adjon egy stratégiát, amivel mindig sikerül sorba rakni a számokat *amikor egyáltalán lehetséges*. Mikor nem lehetséges kirakni? (A választ indokolni is kell!)
`http://www.math.u-szeged.hu/~twaldha/tanitas/algszam3ot_2021osz/cserebere3.html`

18. feladat. Egy szigeten bennszülött törzsek élnek. Ha két azonos törzsbeli bennszülött találkozik, akkor „Umpa!” kiáltással üdvözlik egymást. Ha két különböző törzsbeli találkozik, azok úgy köszönnek, hogy „Lumpa!”. Egyszer 10 bennszülött találkozott. Mindenki köszönt mindenkinek, es így összesen 42 „Umpa!” hangzott el. Hány „Lumpa!” hangzott el? Hányféle törzsből jöhettek az emberek, és melyikből hányan?

19. feladat. Legyen $A = \{a,b,c,d,e,f,g,h\}$. Adjon meg egy B halmazt és egy $\varphi\colon A \to B$ leképezést, amelyre $|A/\ker\varphi| = 4$, $(c,e) \in \ker\varphi$ és $\{c,e\} \notin A/\ker\varphi$.

20. feladat. Legyen $A = \{1,2,3,4,5\}$, $B = \{p,q,r,s\}$, $C = \{\star, \bullet, \triangledown\}$, és tekintsük az alábbi három leképezést:

$$f_1\colon A \to B,\quad 1f_1 = p,\quad 2f_1 = q,\quad 3f_1 = r,\quad 4f_1 = s,\quad 5f_1 = s;$$
$$f_2\colon A \to B,\quad 1f_2 = p,\quad 2f_2 = q,\quad 3f_2 = r,\quad 4f_2 = r,\quad 5f_2 = s;$$
$$h\colon A \to C,\quad 1h = \star,\quad 2h = \star,\quad 3h = \bullet,\quad 4h = \triangledown,\quad 5h = \triangledown.$$

Van-e olyan $g_1\colon B \to C$ leképezés, amelyre $h = f_1 \cdot g_1$? Ha van, akkor adjon meg egyet; ha nincs, akkor bizonyítsa be, hogy valóban nincs. Ugyanígy vizsgálja meg a $h = f_2 \cdot g_2$ függvényegyenlet megoldhatóságát (az ismeretlen g_2 függvényre nézve).

21. feladat. Döntse el, hogy igazak-e az alábbi állítások. (A választ természetesen indokolni kell!)

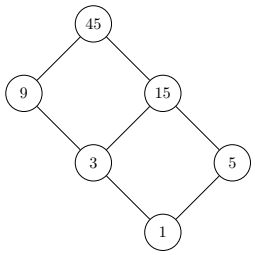
(a) Tetszőleges $\rho \subseteq A \times A$ ekvivalenciareláció esetén, ha $a\rho b$ és $a\rho c$, akkor $b\rho c$.

(b) Ha $\rho \subseteq A \times A$ ekvivalenciareláció és $\{a,b,c\} \in A/\rho$, akkor $(a,b) \in \rho$.

(c) Ha az $f\colon A \to B$ leképezés injektív, akkor $\ker f = \omega_A$.

22. feladat. Jelölje D_n az n pozitív egész szám pozitív osztóinak halmazát. Rajzolja fel a $(D_{45}; |)$ részbenrendezett halmaz Hasse-diagramját.

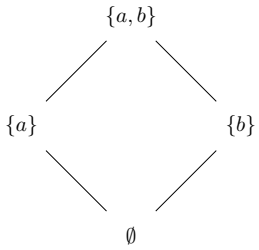
Megoldás.



---

23. feladat. Rajzolja fel a $(\mathcal{P}(\{a, b\}); \subseteq)$ részbenrendezett halmaz Hasse-diagramját.

Megoldás.



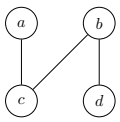
---

24. feladat. Rajzolja fel az (A, ρ_1), (A, ρ_2) és (A, ρ_3) részbenrendezett halmazok Hasse-diagramját, ahol $A = \{a, b, c, d\}$ és

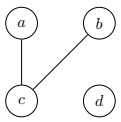
$$\rho_1 = \big\{(a,a), (b,b), (c,c), (d,d), (c,a), (c,b), (d,b)\big\}$$
$$\rho_2 = \big\{(a,a), (b,b), (c,c), (d,d), (c,a), (c,b)\big\}$$
$$\rho_3 = \big\{(a,a), (b,b), (c,c), (d,d), (b,a), (c,a), (d,a)\big\}$$

Mindegyiknél határozza meg a legkisebb, legnagyobb, minimális, maximális elemeket (ha vannak).

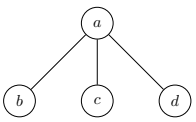
Megoldás.



minimális: c, d
legkisebb: nincs
maximális: a, b
legnagyobb: nincs



minimális: c, d
legkisebb: nincs
maximális: a, b, d(!)
legnagyobb: nincs



minimális: b, c, d
legkisebb: nincs
maximális: a
legnagyobb: a

---

25. feladat. Rajzolja fel a $(D_{36}; |)$, $(D_{100}; |)$ és $(D_{225}; |)$ részbenrendezett halmazok Hasse-diagramját, figyelje meg a köztük lévő hasonlóságot, és magyarázza meg a hasonlóság okát.

26. feladat. Rajzolja fel a $(D_{30}; |)$ és $(\mathcal{P}(\{a, b, c\}); \subseteq)$ részbenrendezett halmazok Hasse-diagramját, figyelje meg a köztük lévő hasonlóságot, és magyarázza meg a hasonlóság okát.

27. feladat. Rajzolja fel az összes lehetséges 4-pontú Hasse-diagramot (16 db van) és mindegyiknél határozza meg a legkisebb, legnagyobb, minimális, maximális elemeket (ha vannak).

28. feladat. Döntse el, hogy igazak-e az alábbi állítások. (A választ természetesen indokolni kell!)

(a) Egy reláció nem lehet egyszerre szimmetrikus és antiszimmetrikus is.

(b) Ha egy részbenrendezett halmazban csak egy minimális elem van, akkor az legkisebb elem is.

(c) Minden véges részbenrendezett halmazban van maximális elem.

29. feladat. Zsömlét és kiflit vásároltam 400 forintért. Egy zsömle 36 forintba kerül, egy kifli pedig 28 forintba. Hány zsömlét és hány kiflit vettem? Keressük meg az összes megoldást!

Megoldás. A zsömlék számát x-szel, a kiflik számát y-nal jelölve a $36x + 28y = 400$ egyenletet kapjuk; ennek keressük a pozitív egész megoldásait. Hajtsuk végre az euklideszi algoritmust az $a = 36$ és $b = 28$ számokra, és fejezzük ki minden osztásból (az utolsó kivételével) a maradékot a és b segítségével:

$$\begin{aligned} 36 &= 1 \cdot 28 + 8 \quad \Longrightarrow \quad 8 = 36 - 28 = a - b \\ 28 &= 3 \cdot 8 + 4 \quad \Longrightarrow \quad 4 = 28 - 3 \cdot 8 = b - 3(a-b) = -3a + 4b \\ 8 &= 2 \cdot 4 + 0 \end{aligned}$$

Tehát $\text{lnko}(a, b) = 4$, és ez így fejezhető ki a és b „lineáris kombinációjaként": $4 = -3a + 4b$. Mindkét oldalt 100-zal szorozva kapjuk, hogy $-300a + 400b = 400$, vagyis $x_0 = -300, y_0 = 400$ egy partikuláris megoldása az egyenletünknek. A diofantoszi egyenlet általános megoldása:

$$x_t = -300 + 7t, \quad y_t = 400 - 9t \qquad (t \in \mathbb{Z}).$$

Keressük meg a pozitív megoldásokat:

$$x_t > 0 \iff t > \frac{300}{7} = 42,8\ldots \iff t \geq 43,$$
$$y_t > 0 \iff t < \frac{400}{9} = 44,4\ldots \iff t \leq 44.$$

Csak $t = 43$ és $t = 44$ esetén lesz x és y is pozitív, azaz két pozitív megoldásunk van:

$$x_{43} = 1, y_{43} = 13 \quad \text{és} \quad x_{44} = 8, y_{44} = 4.$$

A feladat kérdésére a válasz: vagy 1 zsömlét és 13 kiflit vettünk, vagy pedig 8 zsömlét és 4 kiflit.
A diofantoszi egyenlet megoldásait táblázatba is foglalhatjuk; innen is kiolvashatók a pozitív megoldások:

t	$\cdots$	-1	0	1	2	$\cdots$	42	43	44	45	$\cdots$
x_t	$\cdots$	-307	-300	-293	-286	$\cdots$	-6	1	8	15	$\cdots$
y_t	$\cdots$	409	400	391	382	$\cdots$	22	13	4	-5	$\cdots$

---

30. feladat. Határozzuk meg a $H = \{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}\colon 21x - 57y = 30 \text{ és } 20 \leq x \leq 90\}$ halmaz elemeit.

Megoldás. Hajtsuk végre az euklideszi algoritmust az $a = 57$ és $b = 21$ számokra, és fejezzük ki minden osztásból (az utolsó kivételével) a maradékot a és b segítségével:

$$\begin{aligned} 57 &= 2 \cdot 21 + 15 \quad \Longrightarrow \quad 15 = 57 - 2 \cdot 21 = a - 2b \\ 21 &= 1 \cdot 15 + 6 \quad \Longrightarrow \quad 6 = 21 - 15 = b - (a - 2b) = -a + 3b \\ 15 &= 2 \cdot 6 + 3 \quad \Longrightarrow \quad 3 = 15 - 2 \cdot 6 = (a - 2b) - 2(-a + 3b) = 3a - 8b \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

Tehát $\text{lnko}(21, 57) = 3$, és $3 \cdot 57 - 8 \cdot 21 = 3$. Ebből következik, hogy $-80 \cdot 21 + 30 \cdot 57 = 30$, és így a $21x - 57y = 30$ egyenlet egy partikuláris megoldása $x_0 = -80, y_0 = -30$ (figyeljünk az előjelekre!). A diofantoszi egyenlet általános megoldása (itt is figyeljünk az előjelekre!):

$$x_t = -80 + 19t, \quad y_t = -30 + 7t \qquad (t \in \mathbb{Z}).$$

Azokra a megoldásokra van szükségünk, ahol $20 \leq x \leq 90$. Nézzük meg, hogy a t paraméter mely értékeire teljesül ez a két egyenlőtlenség:

$$x_t \geq 20 \iff t \geq \frac{100}{19} = 5,2\ldots \iff t \geq 6,$$
$$x_t \leq 90 \iff t \leq \frac{170}{19} = 8,9\ldots \iff t \leq 8.$$

Látjuk, hogy csak $t = 6, 7, 8$ esetén teljesül mindkét egyenlőtlenség, tehát a H halmaz a következő:

$$H = \{x_6, x_7, x_8\} = \{34, 53, 72\}.$$

A diofantoszi egyenlet megoldásait táblázatba is foglalhatjuk; innen is kiolvashatók a 20 és 90 közé eső x értékek:

t	$\cdots$	-1	0	1	$\cdots$	5	6	7	8	9	$\cdots$
x_t	$\cdots$	-99	-80	-61	$\cdots$	15	34	53	72	91	$\cdots$
y_t	$\cdots$	-37	-30	-23	$\cdots$	5	12	19	26	33	$\cdots$

31. feladat. Melyek azok a z komplex számok, amelyekre $z^{100} = z^{76} = 1$ teljesül? (Az összes megoldást keressük meg!)

32. feladat. Egy nyúl ugrál egy szabályos m-szög csúcsain; egy ugrással a csúcsnyival kerül arrébb. Hány csúcsba képes eljutni, ha elég sokáig ugrál? A megsejtett választ be is kell bizonyítani!

33. feladat. Egy nyúl ugrál a számegyenesen a 0-ból indulva. Kétféle ugrásra képes, amelyek hossza 26, illetve 38 egység. Hogyan tud eljutni a lehető legkevesebb ugrással 1000-be úgy, hogy

(a) mindig csak előre (jobbra) haladhat?

(b) szabad visszafelé (balra) is ugrania?

34. feladat. Valaki a következőket mondta: „A barátnőm 22. születésnapjára 22 szál virágból álló csokrot vettem 2000 forintért. A csokor fréziából, nárciszból és rózsából állt, amelyekből egy szál 50 forintba, 70 forintba, illetve 130 forintba került." Hány szál virágot tartalmazott az egyes fajtákból a csokor, ha azt is tudjuk, hogy mindegyikből legalább két szál volt, és semelyik kettőből sem volt ugyanannyi?

35. feladat. Döntse el, hogy igazak-e az alábbi állítások. (A választ természetesen indokolni kell!)

(a) Ha $a \perp b$, akkor az $ax + by = c$ diofantoszi egyenletnek minden $c \in \mathbb{Z}$ esetén van megoldása.

(b) Minden $x \in \mathbb{Z}$ esetén $56x \mid 60 \implies x \mid 14$.

(c) Ha (u, v) megoldása az $ax + by = c$ diofantoszi egyenletnek, akkor $(u - b, v + a)$ is megoldás.

---

36. feladat. Mit ad 7-tel osztva maradékul $2^{102} + 3^{201}$?

Megoldás. Számítsuk ki először 2^{102} maradékát. Ehhez készítsünk táblázatot 2 hatványainak modulo 7 maradékairól, és figyeljük meg, hogy van-e valami szabályszerűség a kapott sorozatban:

n	0	1	2	3	4	5	6	7	8	9	$\cdots$	102	$\cdots$
$2^n \bmod 7$	1	2	4	1	2	4	1	2	4	1	$\cdots$	1	$\cdots$

Látható, hogy a maradékok hármasával ismétlődnek, azaz 2^n maradéka 7-tel osztva csak attól függ, hogy n mit ad maradékul 3-mal osztva. Formálisan: $2^{n_1} \equiv 2^{n_2} \pmod 7 \iff n_1 \equiv n_2 \pmod 3$. Mivel $102 \equiv 0 \pmod 3$, azt kapjuk, hogy $2^{102} \equiv 2^0 = 1 \pmod 7$.

Hasonló módon számítjuk ki 3 hatványainak maradékait 7-tel osztva:

n	0	1	2	3	4	5	6	7	8	9	$\cdots$	201	$\cdots$
$3^n \bmod 7$	1	3	2	6	4	5	1	3	2	6	$\cdots$	6	$\cdots$

Itt a maradékok hatosával ismétlődnek: $3^{n_1} \equiv 3^{n_2} \pmod 7 \iff n_1 \equiv n_2 \pmod 6$. Mivel $201 \equiv 3 \pmod 3$, azt kapjuk, hogy $3^{201} \equiv 3^3 = 6 \pmod 7$.

Már csak össze kell adni a kiszámolt maradékokat: $2^{102} + 3^{201} \equiv 1 + 6 \equiv 0 \pmod 7$, tehát $2^{102} + 3^{201}$ osztható 7-tel.

Íme egy másik, rövidebb megoldás, ahol úgy bizonyítjuk be a fent megfigyelt oszthatóságot, hogy nem számítjuk ki külön-külön a két tag maradékát:

$$2^{102} + 3^{201} = 4 \cdot 2^{100} + 3 \cdot 9^{100} \equiv 4 \cdot 2^{100} + 3 \cdot 2^{100} = 7 \cdot 2^{100} \equiv 0 \pmod 7.$$

37. feladat. Oldjuk meg a $114x \equiv 6 \pmod{52}$ kongruenciát. Adjuk meg az összes megoldást modulo 52!

Megoldás. A kongruenciát át lehetne írni a $114x - 52y = 6$ diofantoszi egyenletre, amelynek megoldásából $x = 11 + 26t$, azaz $x \equiv 11 \pmod{26}$ adódik, de számoljunk inkább kongruenciákkal (ellenőrizzük, hogy minden lépésben ekvivalens átalakítást végzünk!):

$$\begin{aligned}
114x &\equiv 6 && \pmod{52} \\
19x &\equiv 1 && \pmod{26} \\
45x &\equiv -25 && \pmod{26} \\
9x &\equiv -5 && \pmod{26} \\
9x &\equiv 21 && \pmod{26} \\
3x &\equiv 7 && \pmod{26} \\
3x &\equiv 33 && \pmod{26} \\
x &\equiv 11 && \pmod{26}
\end{aligned}$$

Mivel $\text{lnko}(114, 52) = 2$ (azaz a modulus a számolás végére a felére csökkent), modulo 52 két megoldás van: $x \equiv 11, 37 \pmod{52}$.

38. feladat. Melyek azok a 32-re végződő négyjegyű számok, amelyek oszthatóak 47-tel?

Megoldás. A 32-re végződő négyjegyű számokat $100x + 32$ alakban lehet felírni, ahol x kétjegyű szám. Tehát meg kell oldanunk a $100x + 32 \equiv 0 \pmod{47}$ lineáris kongruenciát:

$$\begin{aligned} 100x + 32 &\equiv 0 \pmod{47} \\ 100x &\equiv -32 \pmod{47} \\ 50x &\equiv -16 \pmod{47} \\ 3x &\equiv 78 \pmod{47} \\ x &\equiv 26 \pmod{47} \end{aligned}$$

Azt kaptuk, hogy a $47t + 26$ alakú számok elégítik ki a kongruenciát. Ezek közül csak 26 és 73 kétjegyű, tehát a feladatban kérdezett négyjegyű számra két lehetőség van: 2632 és 7332.

---

39. feladat. Bizonyítsa be (kongruenciák segítségével), hogy $27 \mid 2^{5n+1} + 5^{n+2}$ minden n természetes szám esetén.

40. feladat. Mi az utolsó két számjegye az 1995^{1995} számnak?

41. feladat. Oldja meg az $52x \equiv 8 \pmod{124}$ kongruenciát. Adja meg az összes megoldást modulo 124!

42. feladat. Egy nyúl ugrál egy szabályos 58-szög csúcsain. Mekkorákat ugorjon, hogy a 24. ugrással a 2. csúcsba érkezzen? Az összes megoldást keressük, és próbálgatni nem ér, a játékot csak ellenőrzésre szabad használni!

43. feladat. Döntse el, hogy igazak-e az alábbi állítások. (A választ természetesen indokolni kell!)

(a) Ha $187 \equiv 5 \pmod{m}$ és $311 \equiv 3 \pmod{m}$, akkor $m = 14$.

(b) Ha $a \equiv 1423 \pmod{2021}$, akkor a nem lehet osztható 13-mal.

(c) Ha $a \equiv b \pmod{m}$ és $n \mid m$, akkor $a \equiv b \pmod{n}$.

---

44. feladat. Oldjuk meg az alábbi kongruenciarendszert:

$$\left.\begin{aligned} 6x &\equiv 2 \pmod{8} \\ 15x &\equiv 3 \pmod{18} \\ 16x &\equiv 4 \pmod{28} \end{aligned}\right\}$$

Megoldás. *Első megoldás.* Először külön-külön megoldjuk a kongruenciákat:

$$\left.\begin{aligned} 6x &\equiv 2 \pmod{8} &&\iff x \equiv 3 \pmod{4} \\ 15x &\equiv 3 \pmod{18} &&\iff x \equiv 5 \pmod{6} \\ 16x &\equiv 4 \pmod{28} &&\iff x \equiv 2 \pmod{7} \end{aligned}\right\}$$

Megoldjuk az első két kongruenciából álló részrendszert (pl. diofantoszi egyenletre való átírással):

$$\left.\begin{aligned} x &\equiv 3 \pmod{4} \\ x &\equiv 5 \pmod{6} \end{aligned}\right\} \iff x \equiv 11 \pmod{12}$$

Végül ezt a kongruenciát hasonló módon „összeolvasztjuk” az eredeti rendszer harmadik kongruenciájával:

$$\left.\begin{aligned} x &\equiv 11 \pmod{12} \\ x &\equiv 2 \pmod{7} \end{aligned}\right\} \iff \underline{\underline{x \equiv 23 \pmod{84}}}$$

Második megoldás. Csak az első kongruenciát oldjuk meg, és a megoldását megfogalmazzuk „milyen alakú szám x” módon:

$$\begin{aligned} 6x \equiv 2 \pmod{8} &\iff x \equiv 3 \pmod{4} \\ &\iff x = 4y + 3 \quad \text{(alkalmas } y \text{ egész számmal).} \end{aligned}$$

Az x-re kapott kifejezést behelyettesítjük a második kongruenciába, és megoldjuk y-ra:

$$\begin{aligned} 15 \cdot (4y + 3) \equiv 3 \pmod{18} &\iff 60y \equiv -42 \pmod{18} \\ &\iff y \equiv 2 \pmod{3} \\ &\iff y = 3z + 2 \quad \text{(alkalmas } z \text{ egész számmal).} \end{aligned}$$

Fejezzük ki x-et z segítségével: $x = 4y + 3 = 4 \cdot (3z + 2) + 4 = 12z + 11$. Ezt helyettesítjük be a harmadik kongruenciába, és megoldjuk z-re:

$$\begin{aligned} 16 \cdot (12z + 11) \equiv 4 \pmod{28} &\iff 192z \equiv -172 \pmod{28} \\ &\iff z \equiv 1 \pmod{7} \\ &\iff z = 7t + 1 \quad \text{(alkalmas } t \text{ egész számmal).} \end{aligned}$$

Fejezzük ki x-et t segítségével: $x = 12z + 11 = 12 \cdot (7t + 1) + 11 = 84t + 23$. Ez azt jelenti, hogy $\underline{\underline{x \equiv 23 \pmod{84}}}$.

45. feladat. A 3.d osztály kirándulni ment. Ötfős szobákban szállásolták el őket, így négy gyerek kénytelen volt Marcsi nénivel egy szobában aludni. Éjszaka Bence olyan rosszul viselkedett, hogy Marcsi néni felhívta a szüleit, akik már hajnalban hazavitték. Így a reggelinél szépen elfértek a gyerekek a hétszemélyes asztaloknál (Marcsi néni külön asztalnál ült). Panka gyomorrontást kapott a reggelitől, ezért délelőtt őt is hazavitték. Ebédnél az étteremben minden asztalnál kilenc gyerek ült (Marcsi néni külön asztalnál). Hányan járnak a 3.d osztályba?

Megoldás. Az osztály létszámát x-szel jelölve, az alábbi kongruenciarendszert írhatjuk fel:

$$\left.\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 1 \pmod 7 \\ x &\equiv 2 \pmod 9 \end{aligned}\right\}$$

Az első kongruenciából kapjuk, hogy $x = 5y + 4$ (alkalmas y egész számmal). Ezt helyettesítjük a második kongruenciába, és megoldjuk y-ra:

$$\begin{aligned} 5y + 4 \equiv 1 \pmod 7 &\iff 5y \equiv -3 \pmod 7 \\ &\iff y \equiv -2 \pmod 7 \\ &\iff y = 7z - 2 \quad \text{(alkalmas } z \text{ egész számmal).} \end{aligned}$$

Fejezzük ki x-et z segítségével: $x = 5y + 4 = 5 \cdot (7z - 2) + 4 = 35z - 6$. Ezt helyettesítjük be a harmadik kongruenciába, és megoldjuk z-re:

$$\begin{aligned} 35z - 6 \equiv 2 \pmod 9 &\iff 35z \equiv 8 \pmod 9 \\ &\iff z \equiv 1 \pmod 9 \\ &\iff z = 9t + 1 \quad \text{(alkalmas } t \text{ egész számmal).} \end{aligned}$$

Fejezzük ki x-et t segítségével: $x = 35z - 6 = 35 \cdot (9t + 1) - 6 = 315t + 29$, azaz $x \equiv 29 \pmod{315}$. Ha $t < 0$, akkor x negatív lesz, $t > 0$ esetén meg több, mint 300-an járnának az osztályba. Tehát az egyetlen reális megoldást $t = 0$ adja: 29-en járnak a 3.d osztályba.

---

46. feladat. Oldjuk meg az alábbi lineáris kongruenciarendszert.

$$\left.\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 1 \pmod 6 \\ x &\equiv 7 \pmod 9 \end{aligned}\right\}$$

Megoldás. A végeredmény $x \equiv 43 \pmod{90}$; a levezetés megnézhető ebben a videóban: `https://youtu.be/Mt1eWRo3mV8`.

---

47. feladat. Oldjuk meg az alábbi lineáris kongruenciarendszert.

$$\left.\begin{aligned} 10x &\equiv 16 \pmod 9 \\ 6x &\equiv 3 \pmod{21} \\ 3x &\equiv 2 \pmod 5 \end{aligned}\right\}$$

Megoldás. A végeredmény $x \equiv 214 \pmod{315}$; a levezetés megnézhető ebben a videóban: `https://youtu.be/ENqm2oqMmR0`.

---

48. feladat. Egy labdarúgó-mérkőzésre azonos számú férőhellyel rendelkező buszokkal érkeznek a szurkolók, akiket biztonsági okokból kisebb csoportokban engednek be a stadionba. Először 4 busznyi szurkoló érkezett, és 5 fős csoportokban engedték be őket, így az utolsó csoportban csak 3 szurkoló maradt. Máskor 13 busszal érkeztek, és 8-as csoportokban nyertek bebocsátást, és ekkor szintén 3 szurkoló maradt az utoljára beengedett csoportban. Amikor pedig 16 busszal érkeztek szurkolók, és egyszerre 9-et léptettek be, akkor végül 5 szurkoló maradt. Hány személyesek a buszok, ha tudjuk, hogy egy buszba legfeljebb 100-an férnek, és a buszok minden esetben tele voltak?

Megoldás. A végeredmény 47; a levezetés megnézhető ebben a videóban: `https://youtu.be/VW7nCtXrgjY`.

---

49. feladat. Oldja meg az alábbi lineáris kongruenciarendszert.

$$\left.\begin{aligned} 3x &\equiv 5 \pmod{10} \\ 3x &\equiv 17 \pmod 8 \\ 14x &\equiv 10 \pmod 6 \end{aligned}\right\}$$

50. feladat. Ha egy kosár tojást 2, 3, 4, 5 vagy 6-osával ürítünk ki, rendre 1, 2, 3, 4, 5 tojás marad benne. Ha azonban 7-esével vesszük ki a tojásokat, akkor egy sem marad benne. Legalább hány tojás van a kosárban?

51. feladat. Mennyi a maradék, ha a $2012^{2013} + 2013^{2012}$ összeget elosztjuk $2012 \cdot 2013$-mal? (Útmutatás: Könnyen kiszámolható a modulo 2012 és a modulo 2013 maradék (ugye?). Ezekből egy kongruenciarendszerrel ki lehet számítani a modulo $2012 \cdot 2013$ maradékot.)

52. feladat. Döntse el, hogy igazak-e az alábbi állítások. (A választ természetesen indokolni kell!)

(a) A $6, 39, 72, 105, \ldots$ számtani sorozatnak és a $6, 132, 258, 384, \ldots$ számtani sorozatnak a *második* közös tagja 4164.

(b) Ha m és n relatív prímek, akkor van megoldása az alábbi kongruenciarendszernek:

$$\left.\begin{array}{rcl} ax & \equiv & b \pmod{m} \\ cx & \equiv & d \pmod{n} \end{array}\right\}$$

(c) Ha $a \equiv 1423 \pmod{2021}$, akkor a nem lehet osztható 13-mal.

---

53. feladat. Oldjuk meg az alábbi paraméteres lineáris kongruenciarendszert.

$$\left.\begin{array}{rcl} x & \equiv & c_1 \pmod{6} \\ x & \equiv & c_2 \pmod{5} \\ x & \equiv & c_3 \pmod{7} \end{array}\right\}$$

Megoldás. A végeredmény: $x \equiv -35c_1 - 84c_2 - 90c_3 \pmod{210}$. (Ha a segéd-kongruenciarendszerek legkisebb nemnegatív megoldásait vesszük, akkor azt kapjuk, hogy $x \equiv 175c_1 + 126c_2 + 120c_3 \pmod{210}$, és ez ekvivalens az előbbi megoldással.)

---

54. feladat. Teljes maradékrendszerek-e az alábbiak modulo 7?

(a) $0, 1, 2, 3, 4, 5, 6$

(b) $1, 2, 3, 4, 5, 6, 7$

(c) $0, 1, 2, 3, 4, 5, 6, 7$

(d) $1, 2, 3, 5, 8, 13, 21$

(e) $1001, 2001, 3001, 4001, 5001, 6001, 7001$

Megoldás.

(a) igen

(b) igen ($\overline{7} = \overline{0}$)

(c) nem (8 eleme van, nem 7)

(d) nem (egyrészt van ismétlődés a maradékok között (hol?), másrészt $\overline{4}$ nincs reprezentálva)

(e) igen (7 szám van, és páronként inkongruensek modulo 7, mert $1000i \equiv 1000j \pmod{7} \iff i \equiv j \pmod{7}$)

---

55. feladat. Számoljunk $\mathbb{Z}_{15}$-ben:

(a) $\overline{8} + \overline{10} =?$

(b) $\overline{8} - \overline{10} =?$

(c) $\overline{8} \cdot \overline{10} =?$

(d) $\overline{8}/\overline{10} =?$

(e) $\overline{6}/\overline{9} =?$

(f) $\overline{2}^{-1} =?$

(g) $\overline{3}^{-1} =?$

(h) $\overline{4}^{-1} =?$

(i) $\overline{5}/\overline{2} =?$

Megoldás.

(a) $\overline{8} + \overline{10} = \overline{18} = \overline{3}$

(b) $\overline{8} - \overline{10} = \overline{-2} = \overline{13}$

(c) $\overline{8} \cdot \overline{10} = \overline{80} = \overline{5}$

(d) $\overline{8}/\overline{10}$ nem értelmezett

(e) $\overline{6}/\overline{9}$ nem egyértelmű (lehetne $\overline{4}$, $\overline{9}$ vagy $\overline{14}$ is)

(f) $\overline{2}^{-1} = \overline{8}$

(g) $\overline{3}^{-1}$ nem értelmezett

(h) $\overline{4}^{-1} = \overline{4}$

(i) $\overline{5}/\overline{2} = \overline{5} \cdot \overline{2}^{-1} = \overline{5} \cdot \overline{8} = \overline{40} = \overline{10}$ (vagy $\overline{5}/\overline{2} = \overline{20}/\overline{2} = \overline{10}$)

---

56. feladat. Oldja meg az alábbi paraméteres lineáris kongruenciarendszert.

$$\left.\begin{array}{rcl} x & \equiv & c_1 \pmod{3} \\ x & \equiv & c_2 \pmod{5} \\ x & \equiv & c_3 \pmod{11} \end{array}\right\}$$

57. feladat. Számítsa ki $\mathbb{Z}_{23}$-ban az $\overline{1}^{-1} + \overline{2}^{-1} + \cdots + \overline{22}^{-1}$ összeget (a végeredményül kapott maradékosztályt a legkisebb nemnegatív elemével reprezentáljuk). Útmutatás: többet ésszel, mint erővel!

58. feladat. Mit ad 2021-gyel osztva 2020! maradékul? És mit ad 625-tel osztva 624! maradékul? Útmutatás: többet ésszel, mint erővel!

59. feladat. Milyen szabály szerint vannak beírva a számok az alábbi mátrixba? Jelölje $a_{i,j}$ az i-edik sor j-edik elemét, de most ne 1-től, hanem 0-tól számozzuk a sorokat és oszlopokat (például $a_{0,0} = 0, a_{0,8} = 8, a_{3,0} = 27, a_{3,8} = 35$). Adja meg az

$a_{i,j}$ számot i és j függvényében egyetlen (minél egyszerűbb) képlettel.

$$\begin{pmatrix} 0 & 28 & 20 & 12 & 4 & 32 & 24 & 16 & 8 \\ 9 & 1 & 29 & 21 & 13 & 5 & 33 & 25 & 17 \\ 18 & 10 & 2 & 30 & 22 & 14 & 6 & 34 & 26 \\ 27 & 19 & 11 & 3 & 31 & 23 & 15 & 7 & 35 \end{pmatrix}$$

Egy kis segítség: `http://www.math.u-szeged.hu/~twaldha/tanitas/algszam3ot_2021osz/torusz.html`.

---

60. feladat. Számítsuk ki a $\mathbb{Z}_{52}$ gyűrűben a $\overline{111}^{50}$ elemet.

Megoldás. A kérdést úgy is megfogalmazhatjuk, hogy mit ad 52-vel osztva maradékul 111^{50}. Először az alapot redukáljuk modulo 52: mivel $111 \equiv 7 \pmod{52}$, ezért $111^{50} \equiv 7^{50} \pmod{52}$. Ellenőrizzük, hogy az alap és a modulus relatív prím (különben nem használhatjuk az Euler–Fermat-tételt): $\text{lnko}(7, 52) \sim 1$. Számítsuk ki $\varphi(52)$ értékét: $\varphi(52) = \varphi(4) \cdot \varphi(13) = 2 \cdot 12 = 24$. A kitevőt modulo $\varphi(52)$ redukálhatjuk: $50 \equiv 2 \pmod{24}$, tehát $7^{50} \equiv 7^2 \equiv 49 \pmod{52}$, és így $\overline{111}^{50} = \overline{49}$.

---

61. feladat. Mit ad $80^{(111^{50})}$ maradékul 53-mal osztva?

Megoldás. Először az alapot redukáljuk: $80 \equiv 27 \pmod{53}$. Ellenőrizzük, hogy az alap és a modulus relatív prím: $\text{lnko}(27, 53) \sim 1$. Számítsuk ki $\varphi(53)$ értékét: $\varphi(53) = 52$. Most a kitevőt kell kiszámítanunk modulo 52. Szerencsére ezt az előző feladatban már megtettük: $111^{50} \equiv 49 \pmod{52}$. Mindezek alapján $80^{(111^{50})} \equiv 27^{49} \pmod{53}$. Ez még mindig túl nagy szám. Vegyük inkább a kitevőnél a legkisebb abszolút értékű maradékot: $111^{50} \equiv 49 \equiv -3 \pmod{52}$. Így tehát $80^{(111^{50})} \equiv 27^{-3} \equiv (27^{-1})^3 \pmod{53}$. Szükségünk van 27 multiplikatív inverzére modulo 53. Ezt megkapjuk a $27x \equiv 1 \pmod{53}$ kongruencia megoldásából: $x \equiv 2 \pmod{53}$. Tehát a számolást így fejezhetjük be: $80^{(111^{50})} \equiv 27^{-3} \equiv (27^{-1})^3 \equiv 2^3 \equiv 8 \pmod{53}$, vagyis a keresett maradék 8.

---

62. feladat. Oldja meg a $\varphi(n) = 4$ egyenletet a természetes számok halmazán. (Az összes megoldást keressük meg, de ne „nyers erőszakkal”!).

63. feladat. Mi az utolsó két számjegye az 1997^{1998} számnak?

64. feladat. Milyen nap lesz $\underbrace{11\ldots11}_{99}$ nap múlva?

65. feladat. Mit ad maradékul *googolplex* 21-gyel osztva?

---

66. feladat. Határozzuk meg az összes olyan háromjegyű számot, amelynek 21 osztója van.

Megoldás. A $\tau(n) = 21$ egyenlet 100 és 999 közé eső megoldásait keressük. Legyen n prímhatványtényezős felbontása $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Ekkor $\tau(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1) = 21$. Itt minden tényező legalább 2 (miért?), tehát 21-et fel kell bontanunk minden lehetséges módon 1-nél nagyobb számok szorzatára. Két lehetőség van: **1.** 21 ($k = 1$), és **2.** $3 \cdot 7$ ($k = 2$).

1. eset: $k = 1$ és $\tau(p_1^{\alpha_1}) = 21$.
Ez akkor és csak akkor teljesül, ha $\alpha_1 = 20$, azaz $n = p_1^{20}$. Ebben az esetben nem kapunk megoldást, mert már 2^{20} is (jóval) nagyobb, mint 999.

2. eset: $k = 2$ és $\tau(p_1^{\alpha_1}) = 3$, $\tau(p_2^{\alpha_2}) = 7$.
Ez akkor és csak akkor teljesül, ha $\alpha_1 = 2$ és $\alpha_2 = 6$, tehát $n = p_1^2 \cdot p_2^6$. Mivel $3^6 > 999$, csak $p_2 = 2$ lehetséges, vagyis $n = p_1^2 \cdot 2^6 = p_1^2 \cdot 64$. Itt p_1 csak 2 vagy 3 lehet, mert $p_1 = 5$ esetén már túl nagy számot kapunk. A $p_1 = 2$ eset nem lehetséges, mert p_1 és p_2 két különböző prímszám. Az egyetlen megoldás tehát $3^2 \cdot 2^6 = 576$.

---

67. feladat. Melyik a legkisebb olyan természetes szám, amelynek 18 osztója van?

Megoldás. A $\tau(n) = 18$ egyenlet legkisebb megoldását keressük. Az előző feladathoz hasonlóan 18 szorzatfelbontásait vizsgáljuk. Most négy lehetőség van.

1. eset: $k = 1$ és $\tau(p_1^{\alpha_1}) = 18$.
Ez akkor és csak akkor teljesül, ha $\alpha_1 = 17$, azaz $n = p_1^{17}$. A legkisebb ilyen szám $2^{17} = 131\,072$.

2. eset: $k = 2$ és $\tau(p_1^{\alpha_1}) = 9$, $\tau(p_2^{\alpha_2}) = 2$.
Ez akkor és csak akkor teljesül, ha $\alpha_1 = 8$ és $\alpha_2 = 1$, tehát $n = p_1^8 \cdot p_2$. A legkisebb ilyen szám $2^8 \cdot 3 = 768$.

3. eset: $k = 2$ és $\tau(p_1^{\alpha_1}) = 6$, $\tau(p_2^{\alpha_2}) = 3$.
Ez akkor és csak akkor teljesül, ha $\alpha_1 = 5$ és $\alpha_2 = 2$, tehát $n = p_1^5 \cdot p_2^2$. A legkisebb ilyen szám $2^5 \cdot 3^2 = 288$.

4. eset: $k = 3$ és $\tau(p_1^{\alpha_1}) = 3$, $\tau(p_2^{\alpha_2}) = 3$, $\tau(p_3^{\alpha_3}) = 2$.
Ez akkor és csak akkor teljesül, ha $\alpha_1 = 2$, $\alpha_2 = 2$ és $\alpha_3 = 1$, tehát $n = p_1^2 \cdot p_2^2 \cdot p_3$. A legkisebb ilyen szám $2^2 \cdot 3^2 \cdot 5 = 180$.

A legkisebb megoldás tehát 180.

68. feladat. Oldjuk meg a $\sigma(n) = 42$ egyenletet.

Megoldás. Legyen n prímhatványtényezős felbontása $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Ekkor $\sigma(n) = \sigma(p_1^{\alpha_1}) \cdot \ldots \cdot \sigma(p_k^{\alpha_k}) = 42$. Itt minden tényező legalább 3 (miért?), tehát 42-t fel kell bontanunk minden lehetséges módon 2-nél nagyobb számok szorzatára. Erre három lehetőség van: **1.** 42 ($k = 1$), **2.** $3 \cdot 14$ ($k = 2$) és **3.** $6 \cdot 7$ ($k = 2$).

1. eset: $k = 1$ és $\sigma(p_1^{\alpha_1}) = 42$.

- ▶ $1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = 42 \implies p_1 \mid 41$. Mivel 41 prímszám, csak egy lehetőség van p_1-re:
  - $p_1 = 41 \implies 1 + 41 + 41^2 + \cdots + 41^{\alpha_1} = 42$, és így $\alpha_1 = 1$.

1. megoldás: $p_1 = 41, \alpha_1 = 1$, tehát $n = 41$.

2. eset: $k = 2$ és $\sigma(p_1^{\alpha_1}) = 3$, $\sigma(p_2^{\alpha_2}) = 14$.

Külön-külön meg kell vizsgálnunk a két egyenletet.

- ▶ $1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = 3 \implies p_1 \mid 2$. Mivel 2 prímszám, csak egy lehetőség van p_1-re:
  - $p_1 = 2 \implies 1 + 2 + 2^2 + \cdots + 2^{\alpha_1} = 3$, és így $\alpha_1 = 1$.
- ▶ $1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2} = 14 \implies p_2 \mid 13$. Mivel 13 prímszám, csak egy lehetőség van p_2-re:
  - $p_2 = 13 \implies 1 + 13 + 13^2 + \cdots + 13^{\alpha_2} = 14$, és így $\alpha_2 = 1$.

2. megoldás: $p_1 = 2, \alpha_1 = 1$ és $p_2 = 13, \alpha_2 = 1$, tehát $n = 2 \cdot 13 = 26$.

3. eset: $k = 2$ és $\sigma(p_1^{\alpha_1}) = 6$, $\sigma(p_2^{\alpha_2}) = 7$.

Külön-külön meg kell vizsgálnunk a két egyenletet.

- ▶ $1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = 6 \implies p_1 \mid 5$. Mivel 5 prímszám, csak egy lehetőség van p_1-re:
  - $p_1 = 5 \implies 1 + 5 + 5^2 + \cdots + 5^{\alpha_1} = 6$, és így $\alpha_1 = 1$.
- ▶ $1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2} = 7 \implies p_2 \mid 6$. Mivel $6 = 2 \cdot 3$, két lehetőség van p_2-re:
  - $p_2 = 2 \implies 1 + 2 + 2^2 + \cdots + 2^{\alpha_2} = 7$, és így $\alpha_2 = 2$.
  - $p_2 = 3 \implies 1 + 3 + 3^2 + \cdots + 3^{\alpha_2} = 7$, de ilyen α_2 nem létezik.

3. megoldás: $p_1 = 5, \alpha_1 = 1$ és $p_2 = 2, \alpha_2 = 2$, tehát $n = 5 \cdot 2^2 = 20$.

Az egyenletnek tehát három megoldása van: $n = 20, 26, 41$.

---

69. feladat. Oldjuk meg a $\sigma(n) = 93$ egyenletet.

Megoldás. Legyen n prímhatványtényezős felbontása $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Ekkor $\sigma(n) = \sigma(p_1^{\alpha_1}) \cdot \ldots \cdot \sigma(p_k^{\alpha_k}) = 93$. Itt minden tényező legalább 3 (miért?), tehát 93-at fel kell bontanunk minden lehetséges módon 2-nél nagyobb számok szorzatára. Erre két lehetőség van: **1.** 93 ($k = 1$) és **2.** $3 \cdot 31$ ($k = 2$).

1. eset: $k = 1$ és $\sigma(p_1^{\alpha_1}) = 93$.

- ▶ $1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = 93 \implies p_1 \mid 92$. Mivel $92 = 2^2 \cdot 23$, két lehetőség van p_1-re:
  - $p_1 = 2 \implies 1 + 2 + 2^2 + \cdots + 2^{\alpha_1} = 93$, de ilyen α_1 nem létezik.
  - $p_1 = 23 \implies 1 + 23 + 23^2 + \cdots + 23^{\alpha_1} = 93$, de ilyen α_1 nem létezik.

Az 1. esetben tehát sajnos nem kaptunk megoldást. Sebaj, nézzük a $3 \cdot 31$ esetet!

2. eset: $k = 2$ és $\sigma(p_1^{\alpha_1}) = 3$, $\sigma(p_2^{\alpha_2}) = 31$.

Külön-külön meg kell vizsgálnunk a két egyenletet.

- ▶ $1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1} = 3 \implies p_1 \mid 2$. Mivel 2 prímszám, csak egy lehetőség van p_1-re:
  - $p_1 = 2 \implies 1 + 2 + 2^2 + \cdots + 2^{\alpha_1} = 3$, és így $\alpha_1 = 1$.
- ▶ Az $1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2} = 31 \implies p_2 \mid 30$. Mivel $30 = 2 \cdot 3 \cdot 5$, három lehetőség van p_2-re:
  - $p_2 = 2 \implies 1 + 2 + 2^2 + \cdots + 2^{\alpha_2} = 31$, és így $\alpha_2 = 4$.
  - $p_2 = 3 \implies 1 + 3 + 3^2 + \cdots + 3^{\alpha_2} = 31$, de ilyen α_2 nem létezik.
  - $p_2 = 5 \implies 1 + 5 + 5^2 + \cdots + 5^{\alpha_2} = 31$, és így $\alpha_2 = 2$.

Most minden lehetséges módon kombinálnunk kell a kapott p_1, α_1 és p_2, α_2 értékeket, hogy megkapjuk az $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$ számot. Vigyázni kell arra, hogy p_1 és p_2 ne legyen egyenlő!

1. megoldás: $p_1 = 2, \alpha_1 = 1$ és $p_2 = 5, \alpha_2 = 2$, tehát $n = 2^1 \cdot 5^2 = 50$.

Az egyenletnek tehát $n = 50$ az egyetlen megoldása.

---

70. feladat. Határozza meg az összes olyan kétjegyű számot, amelynek 12 osztója van.

71. feladat. Oldja meg a $\sigma(n) = 56$ egyenletet.

72. feladat. Mennyi 10^{100} osztóinak szorzata?

73. feladat. Hány olyan derékszögű háromszög van, amelynek oldalai egész számok, és egyik befogója 1000? (Egybevágó háromszögeket nem különböztetünk meg.)

74. feladat. Döntse el, hogy igazak-e az alábbi állítások. (A választ természetesen indokolni kell!)

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

(b) Az Euler-féle φ függvény szürjektív.

(c) Bármely $n \geq 2$ és $a \in \mathbb{Z}$ esetén, ha $\operatorname{lnko}(a,n) = 1$, akkor $a^{n-1} \equiv 1 \pmod{n}$.

---

75. feladat. Bizonyítsuk be, hogy minden n természetes számra

$$\sum_{d|n} \tau(d)\frac{n}{d} = \sum_{d|n} \sigma(d).$$

Megoldás. Vegyük észre, hogy mindkét oldalon egy konvolúció áll:

$$\sum_{d|n} \tau(d)\,\mathrm{id}\left(\frac{n}{d}\right) \stackrel{?}{=} \sum_{d|n} \sigma(d)\mathbf{1}\left(\frac{n}{d}\right).$$

Tehát azt kell igazolni, hogy $\tau * \mathrm{id} = \sigma * \mathbf{1}$. Ez könnyen kijön a konvolúció asszociativitásából és kommutativitásából, felhasználva, hogy $\tau = \mathbf{1} * \mathbf{1}$ és $\sigma = \mathrm{id} * \mathbf{1}$:

$$\tau * \mathrm{id} = (\mathbf{1} * \mathbf{1}) * \mathrm{id} = \mathbf{1} * (\mathbf{1} * \mathrm{id}) = \mathbf{1} * (\mathrm{id} * \mathbf{1}) = \mathbf{1} * \sigma = \sigma * \mathbf{1}.$$

---

76. feladat. A *Mangoldt-féle függvény* a következőképpen van definiálva:

$$\Lambda(n) = \begin{cases} \log p, & \text{ha } n = p^\alpha \text{ (prímhatvány)}, \\ 0, & \text{ha } n \text{ nem prímhatvány.} \end{cases}$$

Határozzuk meg Λ összegzési függvényét.

Megoldás. Legyen n prímhatványtényezős alakja $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. A $\sum_{d|n} \Lambda(n)$ összegben elegendő a prímhatvány osztókat tekinteni, mert a többin úgyis nulla lesz Λ értéke:

$$\sum_{d|n} \Lambda(n) = \Lambda(p_1) + \Lambda(p_1^2) + \cdots + \Lambda(p_1^{\alpha_1}) + \cdots + \Lambda(p_k) + \Lambda(p_k^2) + \cdots + \Lambda(p_k^{\alpha_k}) =$$

$$= \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k = \log(p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}) = \log n.$$

A Λ függvény összegzési függvénye tehát a logaritmusfüggvény.

---

77. feladat. Az f számelméleti függvényről annyit tudunk, hogy $f(3) = 2$, $f(5) = 7$, $f(45) = 21$, és még azt, hogy f gyengén multiplikatív. Határozza meg $F(45)$ értékét, ahol – szokás szerint – F jelöli a f függvény összegzési függvényét. (A szükséges $f(n)$ értékeket ki lehet számolni a megadottakból a gyenge multiplikativitás segítségével, de $f(9)$ kiszámolásánál óvatosnak kell lenni!)

78. feladat. Tekintsük az $F(n) = \frac{\sigma(n)}{n}$ számelméleti függvényt, és legyen f ennek a függvénynek a megfordítási függvénye. Számítsa ki $f(20)$ értékét.

79. feladat. Bizonyítsa be, hogy minden n természetes szám esetén fennáll az alábbi gyönyörű összefüggés. Útmutatás: többet ~~ésszel~~ konvolúcióval, mint erővel!

$$\sum_{d|n} \varphi(d)\tau\left(\frac{n}{d}\right) = \sigma(n).$$

80. feladat. Bizonyítsa be, hogy a primitív n-edik egységgyökök összege $\mu(n)$.

---

81. feladat. 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.

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

Megoldás. Az euklideszi algoritmust végrehajtva azt kapjuk, hogy

$$\operatorname{lnko}(f,g) \sim x^2 + 2x + 3 = f \cdot \frac{1}{2} \;-\; g \cdot \frac{x+1}{2},$$

tehát $u = \frac{1}{2}$ és $v = -\frac{1}{2}x - \frac{1}{2}$.

82. feladat. Határozzuk meg a $\overline{\overline{2}x^3+\overline{4}x^2+\overline{4}x} \in \mathbb{Z}_7[x]/(x^4+\overline{2}x^3+\overline{5}x^2+\overline{2}x+\overline{5})$ maradékosztály multiplikatív inverzét.

Megoldás. Adjunk neveket a polinomoknak:

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

Az $\overline{f} \in \mathbb{Z}_7[x]/(m)$ maradékosztály inverzét kell kiszámolnunk. Jelöljük $\overline{u}$-sal ezt az inverzet; ekkor az inverz definíciója szerint $\overline{f}\cdot\overline{u} = \overline{\overline{1}}$. Ez az egyenlőség ekvivalens az $f\cdot u \equiv 1 \pmod{m}$ lineáris kongruenciával, azt pedig átírhatjuk az $fu - mv = \overline{1}$ „diofantoszi" egyenletre.
Hajtsuk végre az euklideszi algoritmust az m és f polinomokra (amelyik polinomnak van „neve", arra mindig a nevével hivatkozunk a jobb átláthatóság kedvéért):

	osztandó	$=$	hányados $\cdot$ osztó	$+$	maradék
(1)	m	$=$	$\overline{4}x\cdot f$	$+$	$\overline{3}x^2+\overline{2}x+\overline{5}$
(2)	f	$=$	$(\overline{3}x+\overline{4})\cdot(\overline{3}x^2+\overline{2}x+\overline{5})$	$+$	$\overline{2}x+\overline{1}$
(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: $\mathrm{lnko}(f,m) \sim \boxed{\overline{3}} \sim \overline{1}$.
A diofantoszi egyenlet megoldásához fejezzük ki a maradékot az euklideszi algoritmus során elvégzett mindegyik osztásnál (az utolsót kivéve):

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

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

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

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

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

Azt kaptuk, hogy

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

Már majdnem készen vagyunk, de nekünk nem $\overline{3}$-t, hanem $\overline{1}$-t kell felírnunk $fu+mv$ alakban. Ehhez be kell szoroznunk az egyenlőséget $\overline{3}$ multiplikatív inverzével, vagyis $\overline{5}$-sal:

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

Ebből leolvashatjuk az $fu-mv=\overline{1}$ egyenlet egy megoldását: $u = x^3+\overline{5}x^2+\overline{5}x+\overline{4}$, $v = \overline{2}x^2+\overline{3}x+\overline{4}$. Tehát $\overline{f}$ multiplikatív inverze $\overline{x^3+\overline{5}x^2+\overline{5}x+\overline{4}}$.

---

83. feladat. Határozzuk meg a $\overline{\overline{3}x^2+\overline{2}} \in \mathbb{Z}_5[x]/(x^3+x+\overline{1})$ maradékosztály multiplikatív inverzét.

Megoldás. Az $fu+mv=\overline{1}$ egyenletet kell megoldanunk, ahol $f=\overline{3}x^2+\overline{2}$ és $m=x^3+x+\overline{1}$ (az inverzet az u polinom fogja adni). Az euklideszi algoritmusból kapjuk, hogy

$$\mathrm{lnko}(f,g) \sim \overline{4} = f\cdot(\overline{3}x^2+x+\overline{1}) \; + \; m\cdot(x+2).$$

Be kell szoroznunk $\overline{4}=\overline{-1}$-sal, hogy a bal oldalon $\overline{1}$ álljon, és ezután már leolvasható, hogy $u=\overline{2}x^2+\overline{4}x+\overline{4}$ és $v=\overline{4}x+\overline{3}$. Tehát $\overline{\overline{3}x^2+\overline{2}}^{-1} = \overline{2}x^2+\overline{4}x+\overline{4}$.

84. feladat. Bontsuk irreducibilis tényezők szorzatára az $f = x^6 + \overline{3}x^4 - x^3 + \overline{2}x^2 + x - \overline{1} \in \mathbb{Z}_5[x]$ polinomot.

Megoldás. Sorra kipróbáljuk, hogy $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$ valamelyike gyöke-e a polinomnak, és amelyik igen, annál kiemeljük a megfelelő gyöktényezőt (pl. Horner-módszerrel), figyelve arra, hogy lehetnek többszörös gyökök is. Így azt kapjuk, hogy $f = (x-\overline{1})^2(x-\overline{3})(x-\overline{4})(x^2+\overline{4}x+\overline{2})$. Az elsőfokú tényezők nyilván irreducibilisek, és a másodfokú tényező is irreducibilis, mert nincs gyöke (hiszen minden lehetséges gyököt kipróbáltunk már).

---

85. feladat. Bontsuk irreducibilis tényezők szorzatára az $f = x^5 + x^4 + \overline{2}x^3 + x^2 + \overline{1} \in \mathbb{Z}_3[x]$ polinomot.

Megoldás. Az előző feladat módszerét követve kapjuk a felbontást: $f = (x-\overline{1})(x-\overline{2})(x^3+x^2+\overline{2})$. (Indokoljuk meg, hogy miért irreducibilisek a tényezők!)

---

86. feladat. Számítsa ki az f és g polinomok legnagyobb közös osztóját és adja meg az $fu + gv = \text{lnko}(f,g)$ egyenlet egy megoldását az $\mathbb{R}[x]$ polinomgyűrűben. (A megoldást tessék számítógéppel ellenőrizni!)

$$f = x^6 - x^4 + x^2 - 1, \quad g = x^4 + x^3$$

87. feladat. Határozza meg a $\overline{\overline{2}x^2 + \overline{3}x + \overline{2}} \in \mathbb{Z}_5[x]/(x^3 + \overline{4}x)$ maradékosztály multiplikatív inverzét. (A megoldást tessék számítógéppel ellenőrizni!)

88. feladat. Bontsa irreducibilis tényezők szorzatára az $f = x^5 + x^4 + \overline{2}x^3 + \overline{1} \in \mathbb{Z}_5[x]$ polinomot, és indokolja is meg, hogy miért irreducibilisek a kapott tényezők. (A megoldást tessék számítógéppel ellenőrizni!)

89. feladat. Hány irreducibilis másodfokú főpolinom van $\mathbb{Z}_p[x]$-ben (p tetszőleges prímszám)?

---

90. feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az $f = x^6 - x^5 - 2x^3 - 3x^2 - x - 2$ polinomot.

Megoldás. A Rolle(?)-tétel szerint racionális gyök csak $\pm 1, \pm 2$ lehet. Ezek közül 1 és -2 valóban gyök. Horner-módszerrel leválasztva a gyöktényezőket azt kapjuk, hogy $f = (x+1)(x-2)(x^4+2x^2+1)$. Az x^4+2x^2+1 polinomnak nincs racionális gyöke (ha lenne, megtaláltuk volna), de mivel negyedfokú, ebből még nem derül ki, hogy irreducibilis-e. Valójában nem is irreducibilis, hiszen teljes négyzet: $x^4+2x^2+1 = (x^2+1)^2$, az x^2+1 polinom viszont már irreducibilis $\mathbb{Q}$ felett (miért?). Tehát f irreducibilis faktorizációja $\mathbb{Q}$ felett:

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

---

91. feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az $f = 2x^7 + 5x^6 + 4x^5 + 13x^4 + 54x^3 + 84x^2 + 54x + 12$ polinomot.

Megoldás. A Rolle(?)-tétel szerint racionális gyök csak $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm\frac{1}{2}, \pm\frac{3}{2}$ lehet. Ezek közül -1 és $-\frac{1}{2}$ valóban gyök. Horner-módszerrel leválasztva a gyöktényezőket azt kapjuk, hogy

$$f = \left(x + \frac{1}{2}\right)(x+1)^2(2x^4+12x+24) = (2x+1)(x+1)^2(x^4+6x+12).$$

Az $x^4+6x+12$ polinomnak nincs racionális gyöke (ha lenne, megtaláltuk volna), de mivel negyedfokú, ebből még nem derül ki, hogy irreducibilis-e. Használható viszont a Schönemann–Eisenstein-tétel ($p=3$), tehát a fenti felbontásban már valóban irreducibilis minden tényező.

---

92. feladat. Irreducibilis-e $\mathbb{Q}$ felett az $f = x^4 + 1$ polinom?

Megoldás. A polinomnak nincs racionális gyöke (még valós sincs), de mivel negyedfokú, ebből nem következik semmi. Sajnos a Schönemann–Eisenstein-tétel nem alkalmazható, viszont a polinom elég szép ahhoz, hogy meg tudjuk határozni a komplex gyökeit: $\pm\frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}i$. Az $\alpha = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$ és $\beta = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$ jelölést használva, így fest f gyöktényezős alakja, azaz $\mathbb{C}$ feletti irreducibilis felbontása:

$$f = (x-\alpha)(x-\overline{\alpha})(x-\beta)(x-\overline{\beta}).$$

A komplex konjugált gyökökhöz tartozó gyöktényezőket összeszorozva kapjuk az $\mathbb{R}$ feletti felbontást:

$$f = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1).$$

(Ehhez nem kell sokat számolni, ha használjuk a következő formulát: $(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\,\mathrm{Re}\,\alpha \cdot x + |\alpha|^2$.)
Ha az f polinom felbomlana $\mathbb{Q}$ felett kisebb fokú polinomok szorzatára, akkor $\mathbb{Q} \subseteq \mathbb{R}$ miatt az a felbontás egyúttal $\mathbb{R}$ feletti felbontás is lenne. Node $\mathbb{R}$ felett csak így bomlik fel: $f = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$. Ebből következik, hogy f irreducibils $\mathbb{Q}$ felett.

---

93. feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az $f = x^6 - 27$ polinomot.

Megoldás. Sajnos se a Rolle(?)-tétel a Schönemann–Eisenstein-tétel nem segít. Viszont a polinom elég szép ahhoz, hogy meg tudjuk határozni a komplex gyökeit: $\pm\sqrt{3}, \pm\frac{\sqrt{3}}{2} \pm \frac{3}{2}i$. Az $\alpha = \frac{\sqrt{3}}{2} \pm \frac{3}{2}i$ és $\beta = -\frac{\sqrt{3}}{2} \pm \frac{3}{2}i$ jelölést használva, így fest f gyöktényezős alakja, azaz $\mathbb{C}$ feletti irreducibilis felbontása:

$$f = (x - \sqrt{3})(x + \sqrt{3})(x - \alpha)(x - \overline{\alpha})(x - \beta)(x - \overline{\beta}).$$

A komplex konjugált gyökökhöz tartozó gyöktényezőket összeszorozva kapjuk az $\mathbb{R}$ feletti felbontást:

$$f = (x - \sqrt{3})(x + \sqrt{3})(x^2 - \sqrt{3}x + 3)(x^2 + \sqrt{3}x + 3).$$

Mivel $\mathbb{Q} \subseteq \mathbb{R}$, ha egy $\mathbb{Q}[x]$-beli polinom irreducibilis $\mathbb{R}$ felett, akkor irreducibilis $\mathbb{Q}$ felett is. Fordítva ez nem igaz: előfordulhat, hogy egy $\mathbb{Q}$ felett irreducibilis polinom $\mathbb{R}$ felett már felbontható. Ezért a (még egyelőre ismeretlen) $\mathbb{Q}$ feletti felbontásból úgy kapható az $\mathbb{R}$ feletti felbontás, hogy bizonyos tényezőket tovább bontuk. Fordítva, az $\mathbb{R}$ feletti felbontásból úgy kapható a $\mathbb{Q}$ feletti felbontás, hogy bizonyos tényezőket összeszorzunk. A lehető legkevesebb szorzást kell elvégezni, épp csak annyit, hogy eltűnjön minden irracionális szám (különben „túl nagy" tényezőket kapunk, amelyek már nem lesznek irreducibilisek $\mathbb{Q}$ felett). Így kapjuk a fenti $\mathbb{R}$ feletti felbontásból a $\mathbb{Q}$ feletti irreducibilis faktorizációt:

$$f = (x^2 - 3)(x^4 + 3x^2 + 9).$$

A fenti gondolatmenetből következik, hogy itt mindkét tényező irreducubilis $\mathbb{Q}$ felett. Az $x^4 + 3x^2 + 9$ polinom például azért, mert ha $\mathbb{Q}$ felett felbomlana, akkor $\mathbb{Q} \subseteq \mathbb{R}$ miatt az a felbontás egyúttal $\mathbb{R}$ feletti felbontás is lenne, node $\mathbb{R}$ felett csak így bomlik fel: $x^4 + 3x^2 + 9 = (x^2 - \sqrt{3}x + 3)(x^2 + \sqrt{3}x + 3)$, és ez nem $\mathbb{Q}$ feletti felbontás. Az $x^2 - 3$ polinomra hasonló gondolatmenet alkalmazható, de van egyszerűbb indoklás is: $x^2 - 3$ azért irreducibils $\mathbb{Q}$ felett, mert nincs racionális gyöke és csak másodfokú.

---

94. feladat. Milyen alakú elemi törtek összegére lehet felbontani $\mathbb{R}$ illetve $\mathbb{C}$ felett az alábbi racionális törtet? (A számlálókat nem kell kiszámolni, csak a nevezőket.)

$$\frac{3x^7 - 6x^5 + 11x^4 - 2x^3 + 4x^2 - 17}{x^{12} + 16x^6 + 64}$$

95. feladat. Bontsa $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az $f = x^6 + x^5 + 2x^4 + 4x^3 - 4x^2 + 4x - 8$ polinomot, és indokolja is meg, hogy a kapott tényezők miért irreducibilisek. (A megoldást tessék számítógéppel ellenőrizni!)

96. feladat. Bontsa $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az $f = 5x^8 - 5x^7 + 4x^2 - 2x - 2$ polinomot, és indokolja is meg, hogy a kapott tényezők miért irreducibilisek. (A megoldást tessék számítógéppel ellenőrizni!)

97. feladat. Bontsa $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az $f = x^8 - 81$ polinomot, és indokolja is meg, hogy a kapott tényezők miért irreducibilisek. (A megoldást tessék számítógéppel ellenőrizni!)

98. feladat. Mely p prímszámok esetén van racionális gyöke az $x^4 + 2x^3 - 16x^2 + 2x + p$ polinomnak?

99. feladat. Döntse el, hogy igazak-e az alábbi állítások. (A választ természetesen indokolni kell!)

(a) Ha egy $f \in \mathbb{Q}[x]$ polinom irreducibilis $\mathbb{Q}$ felett, akkor nincs valós gyöke.

(b) Az $f = 7x_1^3x_2 + 7x_1x_2^3 \in \mathbb{R}[x_1, x_2, x_3]$ polinom szimmetrikus.

(c) Van olyan $f \in \mathbb{R}[x_1, x_2, x_3]$ szimmetrikus polinom, amelynek tagjai között szerepel $5x_1x_2^4x_3^{13}$.

---

100. feladat. Fejezze ki a $\sigma_1, \sigma_2, , \sigma_3 \in \mathbb{R}[x_1, x_2, x_3]$ elemi szimmetrikus polinomok segítségével az alábbi polinomot. (Útmutatás: többet ésszel, mint erővel!)

$$(x_1 + x_2 - x_3)(x_1 + x_3 - x_2)(x_2 + x_3 - x_1).$$
