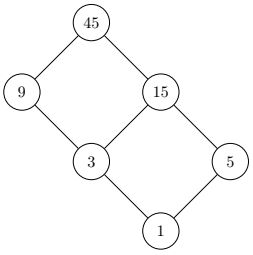
SZÁMELMÉLET

gyakorló és házifeladatok

2023 őszi félév, OT

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

Megoldás.



---

2. feladat. Bizonyítsuk be, hogy $5^{20} - 1$ osztható 24-gyel.

Megoldás. Az $a^n - b^n = (a-b) \cdot (a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} + ab^{n-2} + b^{n-1})$ nevezetes azonosságot használjuk az $a = 25$, $b = 1$, $n = 10$ „szereposztással”:

$$5^{20} - 1 = (5^2)^{10} - 1^{10} = 25^{10} - 1^{10} = (25-1) \cdot (\dots) = 24 \cdot (\dots).$$

Itt a $(\dots)$ helyén egy egész szám van; fel lehetne írni, de nem fontos, hogy mi ez a szám, mert így is látható, hogy $24 \mid 5^{20} - 1$.

---

3. feladat. Bizonyítsuk be, hogy $3^{111} + 2^{444}$ osztható 19-cel.

Megoldás. Páratlan n kitevő esetén érvényes az $a^n + b^n = (a+b) \cdot (a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots + a^2b^{n-3} - ab^{n-2} + b^{n-1})$ azonosság. Ezt használjuk az $a = 3$, $b = 16$, $n = 111$ „szereposztással”:

$$3^{111} + 2^{444} = 3^{111} + (2^4)^{111} = 3^{111} + 16^{111} = (3+16) \cdot (\dots) = 19 \cdot (\dots).$$

Itt a $(\dots)$ helyén egy egész szám van; fel lehetne írni, de nem fontos, hogy mi ez a szám, mert így is látható, hogy $19 \mid 3^{111} + 2^{444}$.

---

4. feladat. Bizonyítsuk be, hogy $2^{102} + 3^{201}$ osztható 7-tel.

Megoldás. A hatványozás azonosságit használva így alakíthatjuk át a számot: $2^{102} + 3^{201} = 4 \cdot 2^{100} + 3 \cdot 9^{100}$. Tudjuk, hogy $7 \mid 9^{100} - 2^{100}$, és ezt a következő módon tudjuk felhasználni:

$$2^{102} + 3^{201} = 4 \cdot 2^{100} + 3 \cdot 9^{100} = 7 \cdot 2^{100} - 3 \cdot 2^{100} + 3 \cdot 9^{100} = 7 \cdot 2^{100} + 3 \cdot (9^{100} - 2^{100}).$$

Itt a kisebbítendő és a kivonandó is osztható 7-tel (ugye?), így maga a különbség is osztható 7-tel.

---

5. feladat. Bizonyítsuk be, hogy $2^{n+2} + 3^{2n+1}$ osztható 7-tel minden n nemnegatív egész szám esetén.

Megoldás. Az előző feladat megoldását szinte szó szerint meg lehetne ismételni: $2^{n+2} + 3^{2n+1} = 7 \cdot 2^n + 3 \cdot (9^n - 2^n)$, de a változatosság kedvéért most bizonyítsunk teljes indukcióval.

- Kezdőlépés: $n = 0$ esetén $2^{n+2} + 3^{2n+1} = 7$, ami persze osztható 7-tel.
- Indukciós lépés: tfh. $7 \mid 2^{n+2} + 3^{2n+1}$, ez az indukciós hipotézis (IH); célunk belátni, hogy $7 \mid 2^{n+3} + 3^{2n+3}$.
  Alakítsuk át az utóbbi kifejezést, hogy be tudjuk „csempészni” azt a számot, amiről az indukciós hipotézis szól.
  $$2^{n+3} + 3^{2n+3} = 2 \cdot 2^{n+2} + 9 \cdot 3^{2n+1} = 2 \cdot (2^{n+2} + 3^{2n+1}) + 7 \cdot 3^{2n+1}.$$
  Itt mindkét tag osztható 7-tel (miért?), így maga az összeg is osztható 7-tel, és épp ezt kellett igazolnunk.

---

6. 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.

7. 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.

8. feladat. Bizonyítsa be (azonosságokkal vagy indukcióval), hogy $4^{2n+1} + 3^{n+2}$ osztható 13-mal minden n nemnegatív egész szám esetén.

9. feladat. Bizonyítsa be (azonosságokkal vagy indukcióval), hogy $n^5 - n$ osztható 5-tel minden n nemnegatív egész szám esetén.

10. feladat. Bizonyítsa be (azonosságokkal vagy indukcióval), hogy $7^n + 3n - 1$ osztható 9-cel minden n nemnegatív egész szám esetén.

11. feladat. Bizonyítsa be, hogy tetszőleges $a, b \in \mathbb{Z}$ esetén $7 \mid 10a + b \iff 7 \mid a - 2b$.

12. feladat. Döntse el, hogy igazak-e az alábbi állítások tetszőleges egész számok esetén. (A választ természetesen indokolni kell!)

(a) Ha $a \sim a'$ és $b \sim b'$, akkor $a \mid b \implies a' \mid b'$.

(b) Ha $a \mid k$ és $b \mid k$, akkor $ab \mid k$.

(c) Ha $a \mid bc$, akkor $a \mid b$ vagy $a \mid c$.

---

13. feladat. Határozzuk meg euklideszi algoritmussal 302 és 112 legnagyobb közös osztóját és fejezzük ki $302x+112y$ alakban (alkalmas x, y egész számokkal).

Megoldás. Használjuk az $a = 302$, $b = 112$ jelölést:

$$\begin{array}{rcl} 302 &=& 2\cdot 112 + 78 \\ 112 &=& 1\cdot\ 78 + 34 \\ 78 &=& 2\cdot\ 34 + 10 \\ 34 &=& 3\cdot\ 10 + \ 4 \\ 10 &=& 2\cdot\ \ 4 + \ 2 \\ 4 &=& 2\cdot\ \ 2 + \ 0 \end{array} \quad \begin{array}{rcl} \implies 78 &=& 302 - 2\cdot 112 \\ \implies 34 &=& 112 - 78 \\ \implies 10 &=& 78 - 2\cdot 34 \\ \implies 4 &=& 34 - 3\cdot 10 \\ \implies 2 &=& 10 - 2\cdot 4 \end{array} \quad \begin{array}{rcl} & & \\ &=& b - (a - 2b) \\ &=& (a - 2b) - 2(-a + 3b) \\ &=& (-a + 3b) - 3(3a - 8b) \\ &=& (3a - 8b) - 2(-10a + 27b) \end{array} \quad \begin{array}{rcl} &=& a - 2b \\ &=& -a + 3b \\ &=& 3a - 8b \\ &=& -10a + 27b \\ &=& 23a - 62b \end{array}$$

Tehát $\text{lnko}(a, b) = 2$, és ez így fejezhető ki a és b segítségével: $2 = 23a - 62b$, azaz $x = 23, y = -62$.

---

14. feladat. Legyen $a = 9\ldots9$ az 500 darab kilencesből álló szám, és legyen $b = 9999999999999$ a tizenhárom darab kilencesből álló szám. Mit ad a maradékul b-vel osztva?

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

16. feladat. Hogyan lehet egy 62 cm és egy 23 cm hosszúságú mérőrúddal kimérni 1 centimétert?

17. feladat. Az alábbi játékban 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!
`http://www.math.u-szeged.hu/~twaldha/tanitas/szamelmot_2023tavasz/nyul-sokszog.html`

18. feladat. Legyenek a és b pozitív egészek, tfh. $a > b$ és az a-ra és b-re végrehajtott euklideszi algoritmus pontosan n lépésből áll (az n-edik lépés az, ahol nulla a maradék). Bizonyítsa be, hogy ekkor $a \geq F_{n+1}$ és $b \geq F_n$. Itt $\{F_n\}_{n=0}^{\infty}$ a Fibonacci sorozat: $F_0 = 1$, $F_1 = 1$, $F_2 = 2$, $F_3 = 3$, $F_4 = 5$, $F_5 = 8, \ldots$.

---

19. feladat. Milyen n természetes számok esetén lehet egyszerűsíteni a $\dfrac{3n+2}{4n+1}$ törtet?

20. feladat. Határozza meg az összes olyan a és b természetes számokat, melyekre $\text{lnko}(a, b) = 26$ és $\text{lkkt}(a, b) = 2288$.

21. feladat. Határozza meg az összes olyan a és b természetes számokat, melyekre $\text{lnko}(a, b) = 17$ és $a^2 - b^2 = 2023$.

22. feladat. Határozza meg az összes olyan p természetes számot, melyre p, $p + 4$ és $p + 14$ is prímszám. Mi a helyzet, ha negatív prímszámokat (pontosabban prím elemeket) is megengedünk?

---

23. feladat. Oldjuk meg a $150x - 54y = 18$ diofantoszi egyenletet.

Megoldás. Hajtsuk végre az euklideszi algoritmust a 150 és 54 számokra, és használjuk az $a = 150$ és $b = -54$ jelölést (kicsit kellemetlen, hogy b negatív, de ezzel a jelöléssel lesz az egyenletünk a tanult $ax + by = c$ alakú, és így könnyebb lesz felírni az általános megoldást):

$$\begin{array}{rcl} 150 &=& 2\cdot 54 + 42 \\ 54 &=& 1\cdot 42 + 12 \\ 42 &=& 3\cdot 12 + \ 6 \\ 12 &=& 2\cdot\ 6 + \ 0 \end{array} \quad \begin{array}{rcl} \implies 42 &=& 150 - 2\cdot 54 \\ \implies 12 &=& 54 - 42 \\ \implies 6 &=& 42 - 3\cdot 12 \end{array} \quad \begin{array}{rcl} & & \\ &=& -b - (a + 2b) \\ &=& (a + 2b) - 3(-a - 3b) \end{array} \quad \begin{array}{rcl} &=& a + 2b \\ &=& -a - 3b \\ &=& 4a + 11b \end{array}$$

Tehát $\text{lnko}(a, b) = 6$, és ez így fejezhető ki a és b „lineáris kombinációjaként”: $6 = 4a+11b$. Szorozzunk 3-mal, hogy megkapjuk 18-at is $ax + by$ alakban:

$$18 = 3 \cdot (4a + 11b) = 12a + 33b.$$

Innen látható, hogy $x_0 = 12$, $y_0 = 33$ egy megoldása az egyenletnek. (Célszerű visszahelyettesítéssel ellenőrizni!)

Írjuk fel az általános megoldás képletét:

$$\begin{aligned} x_t &= x_0 + \frac{b}{\operatorname{lnko}(a,b)} \cdot t = x_0 + \frac{-54}{6} \cdot t = 12 - 9t \\ y_t &= y_0 - \frac{a}{\operatorname{lnko}(a,b)} \cdot t = y_0 - \frac{150}{6} \cdot t = 33 - 25t \end{aligned} \qquad (t \in \mathbb{Z}).$$

Vigyázat: az általános megoldásra tanult képletben a t paramétert tartalmazó tagok egyike előtt $+$, másika előtt $-$ szerepel, de mivel $a = 150$ és $b = -54$ ellentétes előjelűek, végül egyforma előjelűek lettek a tagok. Ezt könnyű eltéveszteni, ezért célszerű ábrázolni, vagy legalább elképzelni az egyenest (pozitív a meredeksége, ezért x és y együtt csökken, együtt növekszik) vagy pedig visszahelyettesíteni az egyenletbe (a t paramétert tartalmazó tagoknak mindenképp ki kell ejteniük egymást).

Megjegyzés. Az $x_t = 12 + 9t$, $y_t = 33 + 25t$ ($t \in \mathbb{Z}$) általános megoldás is jó (és szebb is!), ez csak annyiban különbözik a fentitől, hogy nem jobbról balra, hanem balról jobbra indexezzük az egyenesen lévő rácspontokat. Helyes (és még szebb!) az $x_t = 3 + 9t$, $y_t = 8 + 25t$ ($t \in \mathbb{Z}$) általános megoldás is. (Végtelen sok rácspont van az egyenesen, és ezek bármelyikét választhatjuk partikuláris megoldásnak, ezért végtelen sokféleképpen fel lehet írni az általános megoldást.)

---

24. feladat. Oldjuk meg az $51x - 21y = 6$ diofantoszi egyenletet.

Megoldás. Az euklideszi algoritmusból azt kapjuk, hogy $\operatorname{lnko}(51, 21) = 3 = -2 \cdot 51 + 5 \cdot 21$. Beszorzunk 2-vel, és a jobb oldalt úgy alakítjuk, hogy $51x - 21y$ alakú legyen: $6 = 51 \cdot (-4) - 21 \cdot (-10)$. Ebből leolvasható egy megoldás: $x_0 = -4$, $y_0 = -10$. Az általános megoldás tehát

$$x_t = -4 + 7t,\ y_t = -10 + 17t \quad (t \in \mathbb{Z}).$$

Természetesen jó megoldás az is, hogy $x_t = -4 - 7t$, $y_t = -10 - 17t$ ($t \in \mathbb{Z}$) és $x_t = 3 + 7t$, $y_t = 7 + 17t$ ($t \in \mathbb{Z}$) is helyes.

---

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

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

Tehát $\operatorname{lnko}(21, 57) = 3$, 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 $20 \le x \le 90$. Nézzük meg, hogy a t paraméter mely értékeire teljesül ez a két egyenlőtlenség:

$$\begin{aligned} x_t \ge 20 &\iff t \ge \frac{100}{19} = 5,2\ldots \iff t \ge 6, \\ x_t \le 90 &\iff t \le \frac{170}{19} = 8,9\ldots \iff t \le 8. \end{aligned}$$

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

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

Megjegyzés. 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	$\cdots$

---

26. feladat. Soroljuk fel a $H = \{y \in \mathbb{Z} \mid \exists x \in \mathbb{Z}\colon 32x - 14y = 6 \text{ és } 10 \le y \le 50\}$ halmaz elemeit.

Megoldás. Először írjuk fel a $32x - 14y = 6$ diofantoszi egyenlet általános megoldását, aztán majd kiválogatjuk a 10 és 50 közé eső y értékeket. Az euklideszi algoritmusból azt kapjuk, hogy $\operatorname{lnko}(32, 14) = 2 = -3 \cdot 32 + 7 \cdot 14$. Beszorzunk 3-mal, és a jobb oldalt úgy alakítjuk, hogy $32x - 14y$ alakú legyen: $6 = 32 \cdot (-9) - 14 \cdot (-21)$. Ebből leolvasható egy megoldás: $x_0 = -9$, $y_0 = -21$. Az általános megoldás tehát

$$x_t = -9 + 7t,\ y_t = -21 + 16t \quad (t \in \mathbb{Z}).$$

A $10 \le y_t \le 50$ feltétel szerint $10 \le -21 + 16t \le 50$, amiből rendezés után azt kapjuk, hogy $\frac{31}{16} \le t \le \frac{71}{16}$. Mivel t egész szám, csak a $t = 2, 3, 4$ értékek jönnek szóba, így $H = \{y_2, y_3, y_4\} = \{11, 27, 43\}$.

Megjegyzés. Megúszhatjuk az egyenlőtlenségek megoldását, ha elkészítjük a megoldások táblázatát:

t	$\cdots$	-1	0	1	2	3	4	5	6	$\cdots$
x_t	$\cdots$	-16	-9	-2	5	12	19	26	33	$\cdots$
y_t	$\cdots$	-37	-21	-5	11	27	43	59	75	$\cdots$

Innen is kiolvasható, hogy a 10 és 50 közé eső y értékek: 11, 27, 43.

---

27. feladat. Vettem izéket és bigyókat, összesen 400 forintért. Az izének 36 forintba, a bigyónak pedig 28 forintba kerül darabja. Hány izét és hány bigyót vettem? Az összes lehetséges megoldást keressük meg!

Megoldás. Az izék számát x-szel, a bigyók számát y-nal jelölve a $36x + 28y = 400$ egyenletet írhatjuk fel, melynek a pozitív egész megoldásait keressük. Hajtsuk végre az euklideszi algoritmust az $a = 36$ és $b = 28$ számokra:

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

Tehát $\operatorname{lnko}(a, b) = 4$, 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:

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

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, vagyis a pozitív megoldások a következők:

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

Tehát két megoldás van: vagy 1 izét és 13 bigyót vettem, vagy pedig 8 izét és 4 bigyót.

Megjegyzés. 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	$\cdots$

---

28. feladat. Gombóc Artúrt születésnapja alkalmából Föld körüli útra fizették be a barátai, és az útra ellátták 15 láda csokoládéval. Minden ládában pont annyi csoki volt, ahány éves Gombóc Artúr. Naponta 54 csokoládét evett meg, így még egy hétig sem tartott ki az ellátmány, és az utolsó napra már csak 39 csoki maradt (mármint az utolsó olyan napra, amelyikre még jutott egyáltalán csoki). Hány éves Gombóc Artúr?

Megoldás. Az alábbi linken a számítógép lépésenként végigvezet a feladat megoldásán:
`http://www.math.u-szeged.hu/~twaldha/tanitas/regi/dimat2_2021tavasz/gombocartur.html`

---

29. feladat. Bizonyítsa be, hogy ha az n pozitív egész szám nem négyzetszám, akkor $\sqrt{n}$ irracionális.

30. feladat. Bizonyítsa be, hogy ha $n = a^2 = b^3$, ahol a és b természetes számok, akkor n egy természetes szám hatodik hatványa.

31. feladat. Az alábbi játékban egy nyúl ugrál a számegyenesen a 0-ból indulva. Kétféle ugrásra képes, amelyek hossza 26, illetve 38 egység.
`http://www.math.u-szeged.hu/~twaldha/tanitas/szamelmot_2023tavasz/nyul-szamegyenes.html`

Hogyan tud eljutni a lehető legkevesebb ugrással 1000-be úgy, hogy
(a) mindig csak előre (jobbra) haladhat?
(b) szabad visszafelé (balra) is ugrania?

32. 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?

---

33. feladat. Mit ad maradékul 24-gyel osztva 242^{2023}?

Megoldás. A hatvány alapját csökkenthetjük, ha megfigyeljük, hogy $242 \equiv 2 \pmod{24}$, és ebből következik, hogy $242^{2023} \equiv 2^{2023} \pmod{24}$. Még 2^{2023} is túl nagy szám ahhoz, hogy kedvünk legyen kiszámolni, de írjuk fel 2 első néhány hatványának modulo 24 maradékát, hátha észreveszünk valami szabályszerűséget:

k	0	1	2	3	4	5	6	7	8	9	10	$\cdots$
$2^k \bmod 24$	1	2	4	8	16	8	16	8	16	8	16	$\cdots$

A maradékok az első három tag után kettesével ismétlődnek: ha $k \geq 3$ páratlan szám, akkor $2^k \equiv 8 \pmod{24}$, ha pedig $k \geq 3$ páros szám, akkor $2^k \equiv 16 \pmod{24}$. Mivel 2023 páratlan (és persze $2023 \geq 3$), azt kapjuk, hogy

$$242^{2023} \equiv 2^{2023} \equiv 8 \pmod{24}.$$

Megjegyzés. A táblázat kitöltése során mindig a legutoljára kiszámolt érték dupláját, pontosabban annak a modulo 24

maradékát kell venni (hiszen $2^{k+1} = 2 \cdot 2^k$). Például a kilences oszlopban nem kell kiszámolni, hogy $2^9 = 512$, és hogy ez 8-at ad maradékul 24-gyel osztva; elég csak az előző számot (a nyolcas oszlopbeli 16-ost) megszorozni kettővel: $16 \cdot 2 = 32 \equiv 8 \pmod{24}$. Ebből a számolási módból látszik, hogy az empirikusan megfigyelt szabályszerűség valóban minden $k \geq 3$ esetén teljesül. Ezt persze be is lehetne (sőt, illene!) bizonyítani, például teljes indukcióval, de ettől most eltekintünk. Azt is be lehet(ne) bizonyítani, hogy akármilyen számot hatványozunk, és akármilyen modulus szerint vesszük a maradékokat, a sorozat egy véges „bevezető szakasz" után mindig periodikussá válik.

---

34. feladat. Mit ad maradékul 28-cal osztva 873^{2002}?

Megoldás. Az előző feladathoz hasonlóan, először a hatvány alapját csökkentjük: $873 \equiv 5 \pmod{28}$, ezért $873^{2002} \equiv 5^{2002} \pmod{28}$. Készítsük el 5 hatványai modulo 28 maradékainak táblázatát, és reménykedjünk...

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	$\cdots$
$5^k \bmod 28$	1	5	25	13	9	17	1	5	25	13	9	17	1	5	25	13	9	17	$\cdots$

(Egy trükk: érdemes a legkisebb nemnegatív maradék helyett a legkisebb abszolút értékű maradékkal számolni. Például $5^2 \equiv 25 \equiv -3 \pmod{28}$, ezért $5^3 \equiv 5 \cdot (-3) \equiv -15 \equiv 13 \pmod{28}$. Így az egész számolást meg lehet úszni kétjegyű számokkal.) A maradékok már a legelejétől kezdve hatosával ismétlődnek. Ezért 5^k modulo 28 maradéka csak attól függ, hogy a k kitevő mit ad maradékul 6-tal osztva:

$$\begin{aligned}
k \equiv 0 \pmod 6 &\implies 5^k \equiv 1 \pmod{28} \\
k \equiv 1 \pmod 6 &\implies 5^k \equiv 5 \pmod{28} \\
k \equiv 2 \pmod 6 &\implies 5^k \equiv 25 \pmod{28} \\
k \equiv 3 \pmod 6 &\implies 5^k \equiv 13 \pmod{28} \\
k \equiv 4 \pmod 6 &\implies 5^k \equiv 9 \pmod{28} \\
k \equiv 5 \pmod 6 &\implies 5^k \equiv 17 \pmod{28}
\end{aligned}$$

Nekünk a $k = 2002$ esetre van szükségünk: $2002 \equiv 4 \pmod 6$, ezért $5^{2002} \equiv 9 \pmod{28}$.

Megjegyzés. Ha a hatvány alapja és a modulus relatív prím (mint a mi példánkban: $\text{lnko}(5, 28) = 1$), akkor a sorozat mindig már a legelejétől kezdve periodikus lesz (nincs olyan „bevezető szakasz", mint az előző feladatban), és mindig akkor kezdődik a következő periódus, amikor 1-et kapunk maradékul (a mi példánkban: $5^6 \equiv 1 \pmod{28}$).

---

35. feladat. Bizonyítsuk be, *kongruenciát használva*, hogy $2^{n+2} + 3^{2n+1}$ osztható 7-tel minden n nemnegatív egész szám esetén.

Megoldás. A hatványozás azonosságait és a kongruencia tulajdonságait használva így számolhatunk:

$$2^{n+2} + 3^{2n+1} = 4 \cdot 2^n + 3 \cdot 9^n \boxed{\equiv} 4 \cdot 2^n + 3 \cdot 2^n = 7 \cdot 2^n \equiv 0 \pmod 7.$$

Az egyetlen „trükk" a bekeretezett lépésben történt: azt használtuk ki, hogy $9 \equiv 2 \pmod 7$.

---

36. feladat. Oldjuk meg a $114x \equiv 6 \pmod{52}$ lineáris kongruenciát.

Megoldás. A kongruencia tanult tulajdonságait használva, ekvivalens átalakításokkal jutunk el a megoldáshoz. Erre sok lehetőség van, íme egy levezetés:

$$\begin{aligned}
114x &\equiv 6 \pmod{52} && \text{egyszerűsítünk 6-tal: } \operatorname{lnko}(52,6)=2\\
19x &\equiv 1 \pmod{26} && 19 \equiv 45 \pmod{26} \text{ és } 1 \equiv -25 \pmod{26}\\
45x &\equiv -25 \pmod{26} && \text{egyszerűsítünk 5-tel: } \operatorname{lnko}(26,5)=1\\
9x &\equiv -5 \pmod{26} && -5 \equiv 21 \pmod{26}\\
9x &\equiv 21 \pmod{26} && \text{egyszerűsítünk 3-mal: } \operatorname{lnko}(26,3)=1\\
3x &\equiv 7 \pmod{26} && 7 \equiv 33 \pmod{26}\\
3x &\equiv 33 \pmod{26} && \text{egyszerűsítünk 3-mal: } \operatorname{lnko}(26,3)=1\\
x &\equiv 11 \pmod{26} && \text{kész!}
\end{aligned}$$

Másik megoldás. Ha c relatív prím az m modulushoz, akkor a c-vel való egyszerűsítés ekvivalens átalakítás (nem változik a modulus), mint például a fenti levezetésben az 5-tel és 3-mal való egyszerűsítésnél. Ezt „visszafelé” végrehajtva: a kongruencia mindkét oldalát c-vel szorozni ekvivalens átalakítás, feltéve, hogy $\operatorname{lnko}(m,c)=1$. Ez a beszorzás első pillantásra nem tűnik jó ötletnek, mert (abszolút értékben) nagyobb számok jelennek meg, de ha ezeknek a nagyobb számoknak a modulo m maradéka kicsi, akkor jól járhatunk a beszorzással. Mutatunk egy levezetést, amiben kétszer is használjuk ezt a trükköt:

$$\begin{aligned}
114x &\equiv 6 \pmod{52} && \text{egyszerűsítünk 6-tal: } \operatorname{lnko}(52,6)=2\\
19x &\equiv 1 \pmod{26} && 19 \equiv -7 \pmod{26}\\
-7x &\equiv 1 \pmod{26} && \text{beszorzunk 3-mal: } \operatorname{lnko}(26,3)=1\\
-21x &\equiv 3 \pmod{26} && -21 \equiv 5 \pmod{26}\\
5x &\equiv 3 \pmod{26} && \text{beszorzunk 5-tel: } \operatorname{lnko}(26,5)=1\\
25x &\equiv 15 \pmod{26} && 25 \equiv -1 \pmod{26}\\
-x &\equiv 15 \pmod{26} && \text{egyszerűsítünk vagy beszorzunk } (-1)\text{-gyel: } \operatorname{lnko}(26,-1)=1\\
x &\equiv -15 \pmod{26} && \text{kész!}
\end{aligned}$$

Ez a megoldás ugyanaz, mint az előbbi, hiszen $-15 \equiv 11 \pmod{26}$.

Harmadik megoldás. A kongruenciát áírjuk a $114x - 52y = 6$ diofantoszi egyenletre, amelynek megoldásából $x = 11 + 26t$ adódik, ami azt jelenti, hogy $x \equiv 11 \pmod{26}$.

---

37. feladat. Oldjuk meg az $56x \equiv 48 \pmod{88}$ lineáris kongruenciát.

Megoldás. A kongruencia tanult tulajdonságait használva, ekvivalens átalakításokkal jutunk el a megoldáshoz:

$$\begin{aligned}
56x &\equiv 48 \pmod{88}\\
7x &\equiv 6 \pmod{11}\\
-4x &\equiv 6 \pmod{11}\\
-2x &\equiv 3 \pmod{11}\\
-2x &\equiv 14 \pmod{11}\\
x &\equiv -7 \pmod{11}\\
x &\equiv 4 \pmod{11}
\end{aligned}$$

(Melyik lépésben mit csináltunk? Meg lehetne oldani kevesebb lépésből?)

---

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

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

41. feladat. Oldja meg az $52x \equiv 8 \pmod{124}$ kongruenciát. Adja meg az összes 0 és 123 közötti megoldást!

42. feladat. Keresse meg az összes olyan négyjegyű számot, amely osztható 66-tal, és tízes számrendszerben 18-ra végződik. (Próbálgatni nem ér!)

---

43. feladat. Oldjuk meg az alábbi lineáris kongruenciarendszert:

$$\left.\begin{aligned} x &\equiv 7 \pmod{6} \\ x &\equiv 22 \pmod{9} \end{aligned}\right\}$$

Megoldás. Fogalmazzuk át mindkét kongruenciát oszthatóságra, majd „milyen alakú szám x" típusú állításra:

$$\begin{aligned} x \equiv 7 \pmod{6} &\iff 6 \mid x-7 \iff \exists y \in \mathbb{Z}\colon x = 6y+7; \\ x \equiv 22 \pmod{9} &\iff 9 \mid x-22 \iff \exists z \in \mathbb{Z}\colon x = 9z+22. \end{aligned}$$

Az x-re kapott két kifejezést egyenlővé téve a $6y+7 = 9z+22$ diofantoszi egyenletet kapjuk, amit rendezés után a $6y-9z = 15$ alakba írhatunk. Az egyenlet megoldása $y = 4+3t$, $z = 1+2t$ ($t \in \mathbb{Z}$). (Lásd a jegyzetben a 2.5. Példát, csak ott nem y és z, hanem x és y voltak az ismeretlenek.) Ebből kifejezhetjük x-et: $x = 6y+7 = 6\cdot(4+3t)+7 = 18t+31$ (ugyanezt megkaphattuk volna z-ből is). Tehát a kongruenciarendszer megoldásai az $x = 18t+31$ ($t \in \mathbb{Z}$) alakú számok, vagyis x akkor és csak akkor megoldás, ha $x \equiv 31 \pmod{18}$. Mivel $31 \equiv 13 \pmod{18}$, a megoldást így is felírhatjuk $x \equiv 13 \pmod{18}$.

Megjegyzés. A diofantoszi egyenletre való visszavezetés helyett kongruenciás számolással is meg lehet oldani ilyen kongruenciarendszereket, és ez általában kevesebb számolással jár. Ezt a módszert a következő két feladatban mutatjuk be.

---

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

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

(A számolást lehetett volna ügyesebben is csinálni: a zárójel felbontása előtt leoszthattunk volna 4-gyel, és utána már 12-t és 11-et redukálhattuk volna modulo 7. Így nem kellett volna kiszámolni olyan szörnyű dolgokat, mint $16\cdot 12 = 192$.) 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:

$$\left.\begin{aligned} x &\equiv 4 \pmod{5} \\ x-1 &\equiv 0 \pmod{7} \\ x-2 &\equiv 0 \pmod{9} \end{aligned}\right\} \quad \text{azaz} \quad \left.\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 2 \pmod{9} \end{aligned}\right\}$$

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. Oldjuk meg az alábbi paraméteres lineáris kongruenciarendszert.

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

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.)

---

50. feladat. Oldja meg az alábbi lineáris kongruenciarendszert.

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

51. feladat. Az alábbi játékban két nyúl, egy lány és egy fiú ugrál a számegyenesen, és szeretnének randevúzni.
`http://www.math.u-szeged.hu/~twaldha/tanitas/szamelmot_2023tavasz/nyulak-szamegyenes.html`
A lány a 0-ról indul, és 72-esével ugrál, a fiú a 42-esről indul, és 42-esével ugrál. Így könnyen tudnának találkozni (pl. a 0-ban), de még a kapcsolatuk elején járnak (és különben is: nyuszik), ezért nem akarnak rögtön egymás karjába omolni, tehát nem ugorhatnak ugyanarra a számra. Milyen közel kerülhetnek így egymáshoz, és hova kell elugrálniuk, hogy ezt a minimális távolságot elérjék?

52. 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?

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

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

---

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. 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.)

57. 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.

58. feladat. Oldja meg $\mathbb{Z}_{30}$-ban a $\overline{25}x = \overline{15}$ egyenletet. (Az összes megoldást meg kell keresni, és próbálgatni nem ér!)

59. 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!

---

60. feladat. Mit ad 96! maradékul 101-gyel osztva?

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

(a) Az $1001, 2001, 3001, \ldots, 22001$ számok teljes maradékrendszert alkotnak modulo 22.

(b) Az $\overline{5} \in \mathbb{Z}_{26}$ és $\overline{8} \in \mathbb{Z}_{62}$ halmazok diszjunktak.

(c) A $\mathbb{Z}_{625}^*$ halmaznak 500 eleme van.

62. feladat. Oldja meg a $\varphi(n) = 4$ egyenletet a természetes számok halmazán. (Négy megoldás van, és ezek megtalálásán kívül a feladatnak lényeges része megindokolni, hogy ezeken kívül miért nincs több megoldás.)

63. feladat. Milyen n természetes számok esetén lesz $\varphi(n)$ páratlan? (A megoldást természetesen indokolni kell.)

---

64. feladat. Határozzuk meg 7 rendjét modulo 20. Mit ad maradékul 20-szal osztva 7^{2023}?

Megoldás. Kezdjük el hatványozni 7-et, és nézzük meg, mikor kapunk először 1-et modulo 20:

k	1	2	3	4
$7^k \bmod 20$	7	9	3	1

A negyedik lépésben jött ki először 1, ezért $o_{20}(7) = 4$. Emiatt 7 modulo 20 hatványozásakor a kitevő csak modulo 4 „számít". Mivel $2023 \equiv 3 \pmod 4$, ezért $7^{2023} \equiv 7^3 \equiv 3 \pmod{20}$.

---

65. feladat. Határozzuk meg 5 rendjét modulo 28. Mit ad maradékul 28-cal osztva 5^{2002}?

Megoldás. Kezdjük el hatványozni 5-öt, és nézzük meg, mikor kapunk először 1-et modulo 28:

k	1	2	3	4	5	6
$5^k \bmod 28$	5	25	13	9	17	1

A hatodik lépésben jött ki először 1, ezért $o_{28}(5) = 6$. Emiatt 5 modulo 28 hatványozásakor a kitevő csak modulo 6 „számít". Mivel $2002 \equiv 4 \pmod 6$, ezért $5^{2002} \equiv 5^4 \equiv 9 \pmod{28}$.

Megjegyzés. Ez a feladat lényegében ugyanaz, mint a 34. feladat, csak ott még nem ismertük a rend fogalmát.

---

66. feladat. Mennyit ad 5^{2002} maradékul 28-cal osztva?

Megoldás.

1. Az Euler–Fermat-tételt fogjuk használni, ezért ellenőrizzük, hogy teljesül a tétel feltétele, azaz a hatvány alapja és a modulus relatív prím: $\text{lnko}(5, 28) = 1$. ✓
2. Szükségünk lesz a modulus φ-értékére: $\varphi(28) = \varphi(2^2 \cdot 7) = \varphi(2^2) \cdot \varphi(7) = 2 \cdot 6 = 12$.
3. A kitevőt modulo $\varphi(28)$ lehet redukálni: $2002 \equiv 10 \pmod{12}$.

Az Euler–Fermat-tételt használva a fentiek alapján ezt kapjuk: $5^{2002} \equiv 5^{10} \pmod{28}$. Ugyan 5^{10} elég nagy szám, de a modulo 28 maradékát kis ügyeskedéssel könnyen kiszámíthatjuk számológép nélkül is:

$$5^{10} \equiv (5^2)^5 \equiv 25^5 \equiv (-3)^5 \equiv (-3)^3 \cdot (-3)^2 = (-27) \cdot 9 \equiv 1 \cdot 9 \equiv 9 \pmod{28}.$$

Tehát 5^{2002} kilencet ad maradékul 28-cal osztva.

Másik megoldás. Jobban járnánk, ha a 3. pontban a legkisebb nemnegatív maradék helyett inkább a legkisebb abszolút értékű maradékot vennénk: $2002 \equiv -2 \pmod{12}$; így 5^{10} helyett az $5^{-2} \equiv 25^{-1}$ hatványt kell kiszámítanunk modulo 28. Tehát 25 multiplikatív inverzét keressük modulo 28. Ehhez a $25x \equiv 1 \pmod{28}$ lineáris kongruenciát kell megoldanunk. A megoldás: $x \equiv 9 \pmod{28}$.

Megjegyzés. A 34 és a 65. feladatban is kiszámoltuk 5^{2002} maradékát 28-cal osztva. Ott azt figyeltük meg, hogy 5 hatványainak modulo 28 maradékai hatosával ismétlődnek, és így a 2002-es kitevőt 4-re tudtuk redukálni. Az Euler–Fermat-tétel ennél valamivel gyengébb állítást, 12-es periodicitást adott, viszont itt nem kellett próbálgatással megfigyelnünk a hatványok alakulását, „kapásból" tudtuk a 2002-es kitevőt 10-re (illetve (-2)-re) redukálni.

---

67. feladat. Mennyit ad 98^{272} maradékul 27-tel osztva?

Megoldás.

0. Először csökkentsük a hatvány alapját: $98 \equiv 17 \pmod{27}$, ezért $98^{272} \equiv 17^{272} \pmod{27}$.
1. Az Euler–Fermat-tételt fogjuk használni, ezért ellenőrizzük, hogy teljesül a tétel feltétele, azaz a hatvány alapja és a modulus relatív prím: $\text{lnko}(17, 27) = 1$. ✓
2. Szükségünk lesz a modulus φ-értékére: $\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 18$.
3. A kitevőt modulo $\varphi(18)$ lehet redukálni: $272 \equiv 2 \pmod{18}$.

Az Euler–Fermat-tételt használva a fentiek alapján ezt kapjuk: $98^{272} \equiv 17^2 \equiv 289 \equiv 19 \pmod{27}$. Tehát 98^{272} tizenkilencet ad maradékul 27-tel osztva.

---

68. 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 $\overline{111}^{50} = \overline{49}$.

---

69. 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.

---

70. feladat. Határozza meg 10 rendjét modulo 7. (Ehhez készítsen táblázatot a 10-hatványok modulo 7 maradékaiból.) Ezután írásbeli osztással számítsa ki 1/7 tizedes tört alakját. Milyen kapcsolat van a két számolás között?

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

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

73. feladat. Mit ad maradékul *googolplex* 21-gyel osztva? (Csak óvatosan!)

74. feladat. Mutassa meg, hogy ha $a \perp 100$, akkor $a^{20} \equiv 1 \pmod{100}$.

75. feladat. Bizonyítsa be, hogy ha egy szám nem osztható se 2-vel se 5-tel, akkor van olyan többszöröse, ami csupa kilencesből áll.

---

76. feladat. Készítsünk indextáblázatot a $p = 13$ modulushoz a $g = 2$ primitív gyökkel, majd oldja meg az indextáblázat segítségével az $x^9 \equiv 8 \pmod{13}$ kongruenciát.

Megoldás. Számítsuk ki 2 hatványainak modulo 13 maradékait:

i	0	1	2	3	4	5	6	7	8	9	10	11
2^i	1	2	4	8	3	6	12	11	9	5	10	7

Ha megcseréljük a két sort, és a fölső számok szerint rendezzük az oszlopokat, akkor megkapjuk az indextáblázatot:

a	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_g\, a$	0	1	4	2	9	5	11	3	8	10	7	6

Ha x nem relatív prím 13-hoz, akkor biztosan nem megoldása a kongruenciának (miért?), ezért a megoldást kereshetjük $x \equiv 2^i \pmod{11}$ alakban. Ekvivalens átalakításokkal így juthatunk el a megoldáshoz:

$$\begin{aligned}
x^9 \equiv 8 \pmod{13} &\iff 2^{9i} \equiv 2^3 && \pmod{13}\\
&\iff 9i \equiv 3 && \pmod{12}\\
&\iff i \equiv -1 && \pmod{4}\\
&\iff i \equiv 3, 7, 11 && \pmod{12}\\
&\iff 2^i \equiv 8, 11, 7 && \pmod{13}\\
&\iff x \equiv 8, 11, 7 && \pmod{13}
\end{aligned}$$

---

77. 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 $3^2 \cdot 2^6 = 576$.

---

78. 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.

---

79. 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: $n = 20, 26, 41$.

---

80. 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 $\alpha_2 = 2$.

Minden lehetséges módon kombinálni kell a kapott p_1, α_1 és p_2, α_2 értékeket. Vigyázni kell arra, hogy p_1 és p_2 ne legyen egyenlő! Ezért csak egy lehetőség van: $p_1 = 2, \alpha_1 = 1$ és $p_2 = 5, \alpha_2 = 2$, tehát $n = 2^1 \cdot 5^2 = 50$.

---

81. feladat. Készítsen indextáblázatot a $p = 17$ modulushoz a $g = 3$ primitív gyökkel, majd oldja meg az indextáblázat segítségével az $x^{10} \equiv 13 \pmod{17}$ kongruenciát.

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

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