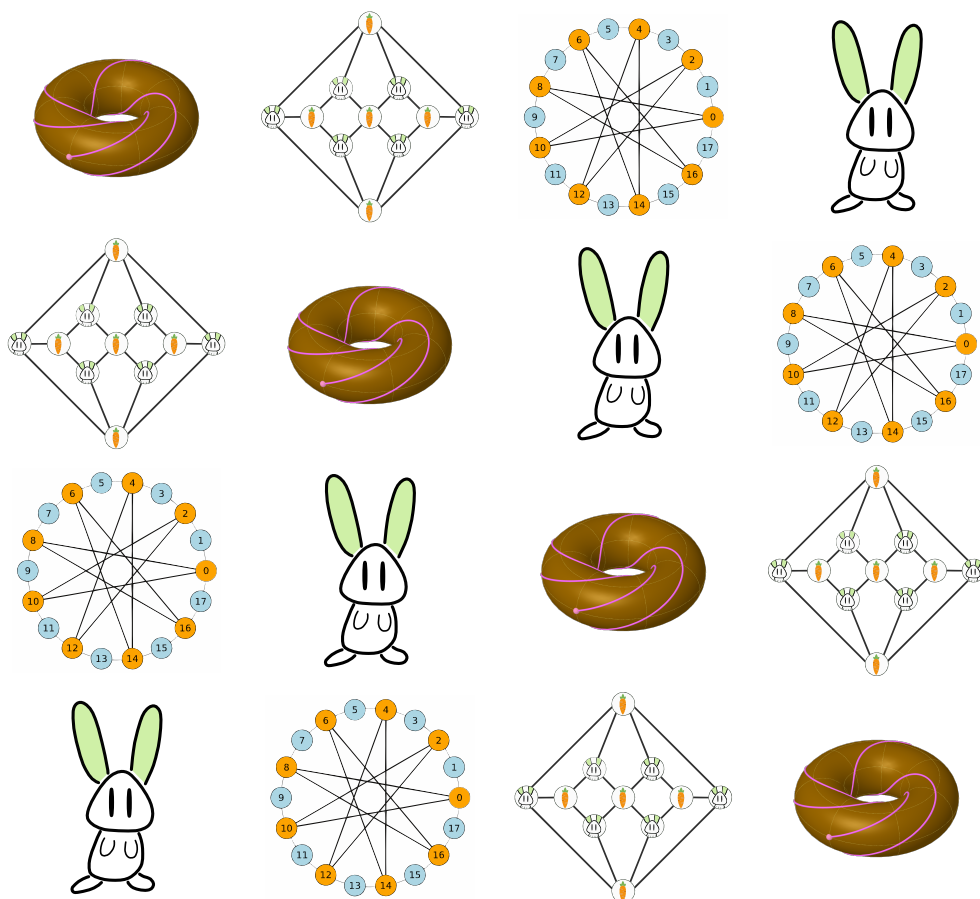


DISZKRÉT MATEMATIKA II

feladatgyűjtemény



A feladatgyűjteményt az SZTE Bolyai Intézete Algebra és Számelmélet Tanszékének volt és jelenlegi tagjai által évek alatt készített és összegyűjtött feladatokból Waldhauser Tamás állította össze. A feladatokhoz tartozó videókat

Kátai-Urbán Kamilla

Maróti Miklós

Tóth Endre

Kulin Júlia

Szilák Zsófia

Varga Kristóf

Kunos Ádám

Torma Gábor

Waldhauser Tamás

készítette.

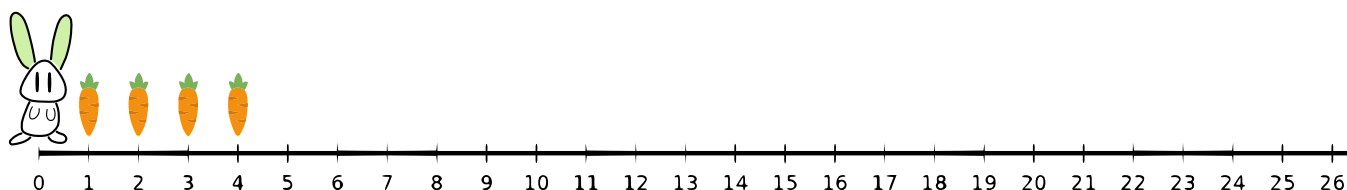
👉 Minden feladat sorszáma egy link, ami hátra, a feladat végeredményéhez vezet. Onnan ismét a feladat sorszáma kattintva lehet visszajutni a feladathoz.

📺 A kamera azt jelzi, hogy ehhez a feladathoz van videó; a link hátul, a végeredménynél található.

Tartalomjegyzék

FELADATOK

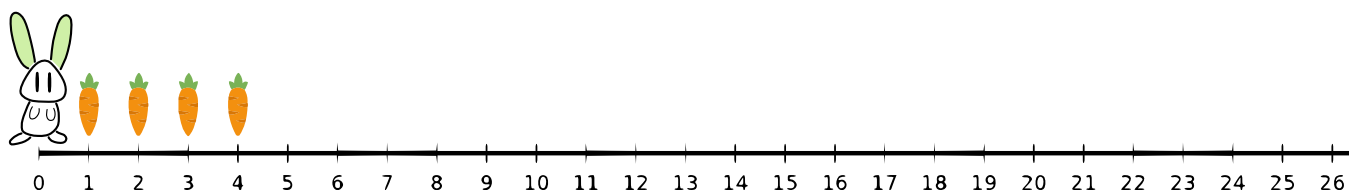
1. Számelmélet	5
1.1 Oszthatóság, legnagyobb közös osztó, euklideszi algoritmus	6
1.2 Lineáris diofantoszi egyenletek	7
1.3 A modulo m kongruenciareláció	13
1.4 Lineáris kongruenciák	15
1.5 Lineáris kongruenciarendszerek	18
1.6 Maradékosztályok	23
1.7 Redukált maradékosztályok, multiplikatív inverz, multiplikatív rend	25
1.8 Az Euler-féle φ függvény	27
1.9 Az Euler–Fermat-tétel	28



Tartalomjegyzék

VÉGEREDMÉNYEK, MEGOLDÁSOK

1. Számelmélet	31
1.1 Oszthatóság, legnagyobb közös osztó, euklideszi algoritmus	32
1.2 Lineáris diofantoszi egyenletek	32
1.3 A modulo m kongruenciareláció	34
1.4 Lineáris kongruenciák	35
1.5 Lineáris kongruenciarendszerek	36
1.6 Maradékosztályok	36
1.7 Redukált maradékosztályok, multiplikatív inverz, multiplikatív rend	37
1.8 Az Euler-féle φ függvény	38
1.9 Az Euler–Fermat-tétel	39



FELADATOK

1. Számelmélet

1.1. Oszthatóság, legnagyobb közös osztó, euklideszi algoritmus

A feladatok megoldása előtt célszerű megnézni az elméleti háttér bemutató videó(ka)t:

👉 https://youtu.be/3rAs_gBBHxU (oszthatóság, prímszámok)

👉 <https://youtu.be/mPigchEMSEk> (legnagyobb közös osztó, euklideszi algoritmus)

1.1. feladat. Határozzuk meg mindazon x egész számok halmazát, amelyekre teljesülnek az alábbi feltételek.

❑ (a) $28 \mid 36x$

❑ (d) $x \mid 112$ és $x \mid 84$

(g) $x \mid 126$ és $x \mid 54$

❑ (b) $140 \mid x$ és $84 \mid x$

(e) $105 \mid 45x$

(h) $75 \mid x$ és $60 \mid x$

❑ (c) $144 \mid 108x$

(f) $88 \mid x$ és $66 \mid x$

(i) $x \mid 132$ és $x \mid 99$

❑ **1.2. feladat.** Melyik az a legkisebb pozitív egész, amelynek pontosan 12 darab pozitív osztója van?

Kidolgozott feladat.

Határozzuk meg euklideszi algoritmussal 302 és 112 legnagyobb közös osztóját, és fejezzük ki $302u + 112v$ alakban (alkalmas u, v egész számokkal).

Megoldás. Használjuk az $a = 302$, $b = 112$ jelölést, és fejezzük ki az euklideszi algoritmus minden lépésénél a maradékot a és b segítségével:

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

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

Az alábbi linken a számítógép még bármennyiszer türelmesen elmagyarázza az euklideszi algoritmust, lépésről lépésre: http://www.math.u-szeged.hu/~twaldha/tanitas/regi/dimat2_2021tavasz/euklideszialg.html

▲ **1.3. feladat.** Határozzuk meg euklideszi algoritmussal az alábbi a, b egész számok legnagyobb közös osztóját, és fejezzük ki $\text{lko}(a, b) = au + bv$ alakban (alkalmas u, v egész számokkal), majd adjuk meg a és b legkisebb közös többszörösét is.

❑ (a) $a = 36, b = 28$

❑ (c) $a = -1253, b = -3241$

(e) $a = 368, b = 161$

❑ (b) $a = 78, b = 30$

(d) $a = 48, b = 34$

(f) $a = 539, b = 1001$

1.4. feladat. Melyek azok a z komplex számok, amelyekre $z^{100} = 1$ és $z^{76} = 1$ egyszerre teljesül?

1.2. Lineáris diofantoszi egyenletek

A feladatok megoldása előtt célszerű megnézni az elméleti háttér bemutató videó(ka)t:

👉 <https://youtu.be/0uz2jiwxJeg>

Kidolgozott feladat.

Oldjuk meg a $6x + 9y = 15$ diofantoszi egyenletet.

Megoldás. Hajtsuk végre az euklideszi algoritmust a 6 és 9 számokra:

$$\begin{aligned}9 &= 1 \cdot 6 + 3 \implies 3 = 9 - 6 \\6 &= 2 \cdot 3 + 0\end{aligned}$$

Azt kaptuk, hogy $\text{lko}(6, 9) = 3$ (ezt persze láthattuk volna ránézésre is), és az lko így fejezhető ki 6 és 9 segítségével: $3 = 9 - 6$. Mivel nekünk nem 3-at, hanem 15-öt kell megkapnunk $6x + 9y$ alakban, szorozzunk be 5-tel, és alakítsuk $6x + 9y$ alakúra a kifejezést, hogy könnyebben leolvashassuk a megoldást:

$$15 = 5 \cdot (9 - 6) = 6 \cdot (-5) + 9 \cdot 5.$$

Innen látható, hogy $x_0 = -5$, $y_0 = 5$ egy megoldása az egyenletnek (partikuláris megoldás).

Hogy a többi megoldást is megkapjuk, ábrázoljuk a $6x + 9y = 15$ egyenletű egyenest, és nézzük meg, hogy milyen rácspontokon halad át. Ehhez rendezzük y -ra az egyenletet:

$$y = \frac{15 - 6x}{9} = \frac{15}{9} - \frac{6}{9}x = \frac{5}{3} - \frac{2}{3}x.$$

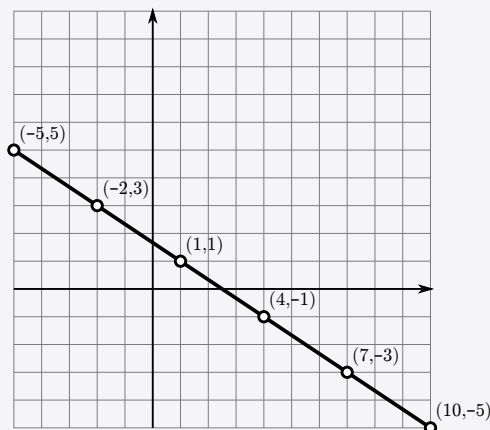
(Fontos, hogy a törteket egyszerűsítsük, amennyire csak lehet, különben a megoldások egy részét elveszítjük!) Tehát az egyenesünk meredeksége $-\frac{2}{3}$, és fent már kiszámoltuk, hogy átmegy az $(x_0, y_0) = (-5, 5)$ ponton. Ezért ebből a pontból „jobbra 3-at, lefele 2-t”, illetve „balra 3-at, fölfelé 2-t” lépésekkel megkapjuk az összes rácspontot az egyenesen, vagyis az egyenlet összes egész megoldását.

Az $(x_0, y_0) = (-5, 5)$ ponttól jobbra a t -edik rácspontot úgy kapjuk meg, hogy $3t$ egységet lépünk jobbra, és $2t$ egységet lépünk lefelé. Így az $(x_0 + 3t, y_0 - 2t)$ számpárt kapjuk, és ha itt negatív t értékeket is megengedünk, akkor megkapjuk az (x_0, y_0) ponttól balra lévő megoldásokat is. A diofantoszi egyenlet általános megoldása tehát

$$\begin{aligned}x_t &= x_0 + 3t = -5 + 3t \\y_t &= y_0 - 2t = 5 - 2t\end{aligned} \quad (t \in \mathbb{Z}).$$

Ez azt jelenti, hogy az egyenlet megoldáshalmaza az alábbi végtelen számpárhalmaz:

$$\begin{aligned}M &= \{ (x_t, y_t) : t \in \mathbb{Z} \} = \\&= \{ (-5 + 3t, 5 - 2t) : t \in \mathbb{Z} \} = \\&= \{ \dots, (-11, 9), (-8, 7), (-5, 5), (-2, 3), (1, 1), \dots \}.\end{aligned}$$



Megjegyzés. Utólag könnyű okosnak lenni: az $(1, 1)$ megoldást észrevehettük volna mindenféle számolás nélkül. Ha ezt tekintenénk kiindulópontnak (partikuláris megoldásnak), akkor az általános megoldás így festene:

$$\begin{aligned}x_t &= 1 + 3t \\y_t &= 1 - 2t\end{aligned} \quad (t \in \mathbb{Z}).$$

Ez látszólag különbözik attól, amit fent kaptunk, de valójában ekvivalens vele, mert ugyanazt a végtelen számpárhalmazt írja le, amint a t paraméter befutja az egész számok halmazát. Mindössze annyi a különbség, hogy a t paraméterek 2-vel el vannak csúszva, pl. a $(7, -3)$ megoldás fent $t = 4$ esetén jön ki, itt pedig $t = 2$ esetén (és hasonlóan az összes többi megoldásra).

Kidolgozott feladat.

Oldjuk meg a $6x - 9y = 15$ diofantoszi egyenletet.

Megoldás. Az előző feladatban kapott rendkívül bonyolult $3 = 9 - 6$ összefüggést megint 5-tel szorozzuk, de most úgy alakítjuk, hogy $6x - 9y$ alakú legyen:

$$15 = 5 \cdot (9 - 6) = 6 \cdot (-5) - 9 \cdot (-5).$$

Innen látható, hogy $x_0 = -5$, $y_0 = -5$ jó lesz partikuláris megoldásnak. (Itt nagyon kell vigyázni az előjelekre, mert könnyű elrontani! A biztonság kedvéért ellenőrizzük a megoldást: $6x_0 - 9y_0 = 6 \cdot (-5) - 9 \cdot (-5) = -30 - (-45) = -30 + 45 = 15$. ✓)

Rendezzük az egyenletet úgy, hogy le tudjuk olvasni az egyenes meredekségét:

$$y = \frac{15 - 6x}{-9} = -\frac{15}{9} + \frac{6}{9}x = -\frac{5}{3} + \frac{2}{3}x.$$

Tehát az egyenesünk meredeksége $\frac{2}{3}$, ezért a fent kiszámolt $(-5, -5)$ pontból „jobbra 3-at, fölfelé 2-t” illetve „balra 3-at, lefele 2-t” lépésekkel megkapjuk az összes rácspontot az egyenesen, vagyis az egyenlet összes egész megoldását.

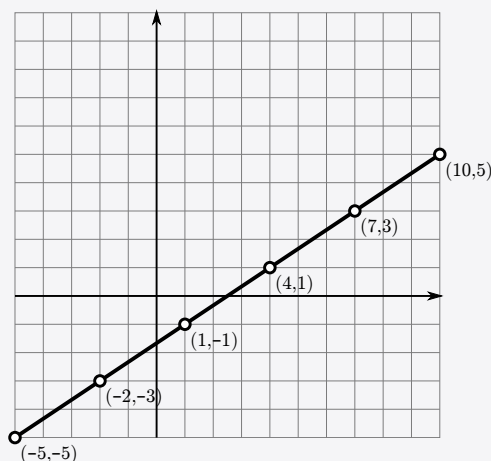
Az $(x_0, y_0) = (-5, -5)$ ponttól jobbra a t -edik rácspontot úgy kapjuk meg, hogy $3t$ egységet lépünk jobbra, és $2t$ egységet lépünk fölfelé. Így az $(x_0 + 3t, y_0 + 2t)$ számpárt kapjuk, és ha itt negatív t értékeket is megengedünk, akkor megkapjuk az (x_0, y_0) ponttól balra lévő megoldásokat is. A diofantoszi egyenlet általános megoldása tehát

$$\begin{aligned} x_t &= x_0 + 3t = -5 + 3t \\ y_t &= y_0 + 2t = -5 + 2t \end{aligned} \quad (t \in \mathbb{Z}).$$

A változatosság kedvéért most táblázatban is megadjuk a megoldáshalmazt alkotó számpárokat:

t	$\dots$	-3	-2	-1	0	1	2	3	4	$\dots$
x_t	$\dots$	-14	-11	-8	-5	-2	1	4	7	$\dots$
y_t	$\dots$	-11	-9	-7	-5	-3	-1	1	3	$\dots$

Figyeljük meg, hogy balról jobbra haladva az x értékek hármasával nőnek, az y értékek pedig kettesével.



Kidolgozott 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):

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

Tehát $\text{lko}(a, b) = 6$, 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:

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

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 rácpontokat. Helyes (és még szebb!) az $x_t = 3 + 9t$, $y_t = 8 + 25t$ ($t \in \mathbb{Z}$) általános megoldás is. (Végtelen sok rácpont van az egyenesen, és ezek bármelyikét választhatjuk partikuláris megoldásnak, ezért végtelen sokféleképpen fel lehet írni az általános megoldást.)

Kidolgozott feladat.

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

Megoldás. Az euklideszi algoritmusból azt kapjuk, hogy $\text{lko}(51, 21) = 3 = -2 \cdot 51 + 5 \cdot 21$. Beszorozunk 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

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

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.

1.5. feladat. Oldjuk meg az alábbi diofantoszi egyenleteket.

- | | | |
|------------------------|------------------------|----------------------------|
| ❑ (a) $72x + 60y = 24$ | (e) $18x + 21y = 9$ | (i) $197x + 418y = 17$ |
| ❑ (b) $21x - 15y = 12$ | (f) $21x + 36y = 12$ | (j) $2021x + 1739y = 4750$ |
| (c) $48x + 34y = 20$ | (g) $6x - 10y = 22$ | |
| (d) $78x + 30y = 12$ | (h) $237x + 571y = 13$ | |

▲ 1.6. feladat. Van-e megoldásuk az alábbi diofantoszi egyenleteknek?

(a) $12x + 20y = 18$

(c) $28x - 21y = -35$

(e) $25x - 30y = 2025$

(b) $13x - 21y = 17$

(d) $10x + 28y = -4$

(f) $21x + 36y = 2026$

▲ 1.7. feladat. A megadott képletek közül melyek írják le helyesen a diofantoszi egyenlet általános megoldását?

egyenlet	1. képlet	2. képlet	3. képlet
(a) $8x + 20y = 64$	$x = -7 + 5t, y = 6 - 2t$	$x = -7 + 5t, y = 6 + 2t$	$x = -7 - 2t, y = 6 + 5t$
(b) $9x + 6y = 66$	$x = 6 + 2t, y = 2 + 3t$	$x = 6 - 2t, y = 2 + 3t$	$x = 6 + 2t, y = 2 - 3t$
(c) $10x - 15y = 25$	$x = -2 + 2t, y = -3 + 3t$	$x = -2 - 2t, y = -3 + 3t$	$x = -2 - 3t, y = -3 - 2t$
(d) $12x - 8y = 60$	$x = 9 + 2t, y = 6 + 3t$	$x = 9 + 8t, y = 6 + 12t$	$x = 9 - 2t, y = 6 - 3t$

Kidolgozott feladat.

Soroljuk fel a $H = \{y \in \mathbb{Z} : (\exists x \in \mathbb{Z})(32x - 14y = 6) \text{ és } 10 \leq y \leq 50\}$ 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 $\text{lko}(32, 14) = 2 = -3 \cdot 32 + 7 \cdot 14$. Beszorunk 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 $10 \leq y_t \leq 50$ feltétel szerint $10 \leq -21 + 16t \leq 50$, amiből rendezés után azt kapjuk, hogy $\frac{31}{16} \leq t \leq \frac{71}{16}$. 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. Megúsíthatjuk az egyenlőtlenségek megoldását, ha elkészítjük a megoldások táblázatát:

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

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

▲ 1.8. feladat. Határozzuk meg a következő halmazok elemszámát.

❖ (a) $\{x \in \mathbb{Z} : (\exists y \in \mathbb{Z})(11x - 8y = 3) \text{ és } 10 \leq x \leq 30\}$

(d) $\{y \in \mathbb{Z} : (\exists x \in \mathbb{Z})(7x - 19y = 10) \text{ és } 15 \leq y \leq 35\}$

(b) $\{x \in \mathbb{Z} : (\exists y \in \mathbb{Z})(75x - 27y = 15) \text{ és } 30 \leq x \leq 60\}$

(e) $\{y \in \mathbb{Z} : (\exists x \in \mathbb{Z})(13x - 20y = 7) \text{ és } 20 \leq y \leq 40\}$

(c) $\{x \in \mathbb{Z} : (\exists y \in \mathbb{Z})(7x - 3y = 13) \text{ és } 10 \leq x \leq 30\}$

Kidolgozott 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:

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

Tehát $\text{lko}(a, b) = 4$, 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:

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

Keressük meg a pozitív megoldásokat:

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

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

■ **1.9. feladat.** Kukutyinban 20 és 45 petáros érmék vannak forgalomban. Hogyan lehet ezekre felváltani 245 petákat? (Az összes megoldást adjuk meg.)

■ **1.10. feladat.** Az alábbi linken elérhető játékban egy nyúl ugrál a számegyenesen a 0-ból indulva. Kétféle ugrásra képes, amelyek hossza a , illetve b egység.

http://www.math.u-szeged.hu/~twaldha/tanitas/regi/dimat2_2021tavasz/nyul-szamegyenes.html

(a) Ha $a = 36$ és $b = 28$, akkor az 1, 2, 3, 4 számoknál lévő répák közül melyeket tudja megenni?

(b) Ha $a = 36$ és $b = 28$, akkor hogyan jut el a lehető legkevesebb ugrással 12-be?

1.11. feladat. Az előző feladatbeli nyúl $a = 26$ és $b = 38$ esetén hogyan tud eljutni a lehető legkevesebb ugrással 1000-be úgy, hogy mindig csak előre (jobbra) haladhat? És ha szabad visszafelé (balra) is ugrania?

1.12. feladat. Hogyan lehet egy 21 centiméteres és egy 25 centiméteres mérőrúd segítségével kimérni 2 centimétert?

1.13. 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?

1.14. feladat. Kati néni az utolsó tanítási napon megajándékozta a 2.d osztály 30 nebulóját: mindenki választhatott, hogy csokit vagy rágót kér. A csoki 69 Ft-tal drágább, mint a rágó, ezért Kati néni örült, hogy a gyerekek több mint fele rágót kért. Így is 2094 forintja bánja az ajándékozást. Mennyibe került a rágó, illetve a csoki, és melyiket hány gyerek választotta?

■ **1.15. feladat.** Háromféle bélyeget vásároltunk. Az első alkalommal az egyes fajtákból rendre 3, 5 és 7 darabot, a második alkalommal 11, 13 és 9 darabot. A számla első alkalommal 110 Ft, a második alkalommal 250 Ft volt. Milyen címletű bélyegeket vásároltunk?

1.16. 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?

1.17. feladat. Egy 5 m hosszú kerítés szegélyének elkészítéséhez 15 cm, 20 cm és 93 cm hosszúságú lécek állnak rendelkezésünkre. Az egyes lécfajták felszegeléséhez rendre 2, 3 és 9 szög kell. Mennyire van szükségünk a lécekből, ha 50 szegünk van, és ezeket mind fel is akarjuk használni?

1.3. A modulo m kongruenciareláció

A feladatok megoldása előtt célszerű megnézni az elméleti háttérrel bemutató videó(ka)t:

👉 https://youtu.be/_-h76rgIvvg

Kidolgozott 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	...
$2^k \bmod 24$	1	2	4	8	16	8	16	8	16	8	16	...

A maradékok az első három tag után kettésével 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.

Kidolgozott 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	...
$5^k \bmod 28$	1	5	25	13	9	17	1	5	25	13	9	17	1	5	25	13	9	17	...

(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: $5^6 \equiv 1 \pmod{28}$).

1.18. feladat. Számítsuk ki az alábbi hatványok maradékát a megadott modulus szerint.

- | | | |
|-------------------------------------|---------------------------------------|-------------------------------------|
| ❖ (a) $699^{1001} \equiv? \pmod{7}$ | ❖ (d) $3423^{3423} \equiv? \pmod{20}$ | (g) $1522^{2023} \equiv? \pmod{15}$ |
| ❖ (b) $2^{102} \equiv? \pmod{7}$ | (e) $1992^{1991} \equiv? \pmod{10}$ | (h) $1841^{1814} \equiv? \pmod{18}$ |
| ❖ (c) $3^{201} \equiv? \pmod{7}$ | (f) $2616^{2021} \equiv? \pmod{13}$ | (i) $2022^{2022} \equiv? \pmod{20}$ |

▲ 1.19. feladat. Mit ad maradékul az x egész szám 7-tel osztva, ha az alábbiakat tudjuk róla?

- | | | |
|---------------------------------------|-----------------------------|----------------------------|
| (a) $x = 7k + 7 \ (k \in \mathbb{Z})$ | (d) $x \equiv 14 \pmod{7}$ | (g) $x \equiv 16 \pmod{7}$ |
| (b) $x = 7k - 1 \ (k \in \mathbb{Z})$ | (e) $x \equiv -14 \pmod{7}$ | (h) $x \equiv 20 \pmod{7}$ |
| (c) $x = 7k - 5 \ (k \in \mathbb{Z})$ | (f) $x \equiv -8 \pmod{7}$ | (i) $x \equiv 9 \pmod{7}$ |

1.20. feladat. Mennyi lehet m értéke, ha $187 \equiv 5 \pmod{m}$ és $311 \equiv 3 \pmod{m}$?

❖ **1.21. feladat.** Bizonyítsuk be (kongruenciák segítségével), hogy $7 \mid 2^{n+2} + 3^{2n+1}$ minden n természetes számra.

1.22. feladat. Bizonyítsuk be (kongruenciák segítségével), hogy $27 \mid 2^{5n+1} + 5^{n+2}$ minden n természetes számra.

1.4. Lineáris kongruenciák

A feladatok megoldása előtt célszerű megnézni az elméleti háttérrel bemutató videó(ka)t:

👉 <https://youtu.be/WVdonTsgGZU>

Kidolgozott feladat.

Oldjuk meg a $6x \equiv 15 \pmod{9}$ lineáris kongruenciát.

Megoldás. A kongruencia definíciója szerint $6x \equiv 15 \pmod{9}$ azt jelenti, hogy $9 \mid 6x - 15$. Ez pedig az oszthatóság definíciója szerint azt jelenti, hogy $6x - 15 = 9y$, alkalmas y egész számmal. Tehát a lineáris kongruenciánk ekvivalens a $6x - 9y = 15$ lineáris diofantoszi egyenlettel (de most csak x -re van szükségünk). Korábban már megoldottuk ezt az egyenletet, és azt kaptuk, hogy általános megoldása $x = -5 + 3t$, $y = -5 + 2t$ ($t \in \mathbb{Z}$). Eszerint egy x egész szám akkor és csak akkor megoldása a kongruenciának, ha előáll $x = -5 + 3t$ alakban, vagyis a megoldáshalmaz egy mindkét irányba végtelen, 3-as differenciájú számtani sorozat:

$$M = \{3t - 5 : t \in \mathbb{Z}\} = \{\dots, -14, -11, -8, -5, -2, 1, 4, 7, 10, 13, \dots\}.$$

Ez a halmaz pontosan azokból a számokból áll, amelyek 3-mal osztva 1-et adnak maradékkal (egy úgynevezett modulo 3 maradékosztály). Tehát egyetlen megoldás van modulo 3, és a megoldást tömören „kongruenciásan” így is felírhatjuk: $x \equiv 1 \pmod{3}$. (Persze azt is írhatnánk, hogy $x \equiv -5 \pmod{3}$, ha már -5 szerepelt a diofantoszi egyenlet megoldásában. Ez a két kongruencia ekvivalens egymással, hiszen $-5 \equiv 1 \pmod{3}$.)

Másik megoldás. A fenti módszerrel minden lineáris kongruencia visszavezethető lineáris diofantoszi egyenletre, de ennél gyakran rövidebb (és élvezetesebb!), ha kongruenciákkal számolunk. A $6x \equiv 15 \pmod{9}$ kongruenciát jó lenne egyszerűsíteni 6-tal, de sajnos 15 nem osztható 6-tal (márpedig a kongruenciának csak egész számokra van értelme). Vegyük azonban észre, hogy $15 \equiv 6 \pmod{9}$, és így a kongruenciánk ekvivalens a $6x \equiv 6 \pmod{9}$ kongruenciával, amit már tudunk 6-tal egyszerűsíteni. Az egyszerűsítésnél vigyázni kell, mert a modulus megváltozhat! Az általános szabály így fest:

$$ca \equiv cb \pmod{m} \iff a \equiv b \pmod{\frac{m}{\text{lko}(m,c)}}.$$

Nálunk most $c = 6$ és $m = 9$ a „szereposztás” (és $a = x$, $b = 1$), tehát az új modulus $\frac{m}{\text{lko}(m,c)} = \frac{9}{\text{lko}(9,6)} = \frac{9}{3} = 3$ lesz. Egyszerűsítés után tehát az $x \equiv 1 \pmod{3}$ megoldást kapjuk, akárcsak az előbb.

Kidolgozott 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:

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

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 $\text{luko}(m, c) = 1$. 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:

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

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

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

Kidolgozott feladat.

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

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

$$\begin{array}{ll}
 56x \equiv 48 & (\text{mod } 88) \\
 7x \equiv 6 & (\text{mod } 11) \\
 -4x \equiv 6 & (\text{mod } 11) \\
 -2x \equiv 3 & (\text{mod } 11) \\
 -2x \equiv 14 & (\text{mod } 11) \\
 x \equiv -7 & (\text{mod } 11) \\
 x \equiv 4 & (\text{mod } 11)
 \end{array}$$

(Találd ki, hogy melyik lépésben mit csináltunk! Meg tudnád oldani kevesebb lépésből?)

1.23. feladat. Oldjuk meg az alábbi lineáris kongruenciákat.

- | | | |
|---------------------------------|-------------------------------|---------------------------------|
| ❏ (a) $3x \equiv 4 \pmod{5}$ | (e) $6x \equiv 4 \pmod{8}$ | (i) $5x \equiv 24 \pmod{13}$ |
| ❏ (b) $10x \equiv 26 \pmod{28}$ | (f) $13x \equiv -3 \pmod{34}$ | (j) $27x \equiv 9 \pmod{93}$ |
| ❏ (c) $9x \equiv 15 \pmod{12}$ | (g) $30x \equiv 9 \pmod{51}$ | (k) $92x \equiv 20 \pmod{212}$ |
| ❏ (d) $29x \equiv 17 \pmod{73}$ | (h) $88x \equiv 42 \pmod{55}$ | (l) $160x \equiv 60 \pmod{230}$ |

1.24. feladat. Van-e megoldásuk az alábbi lineáris kongruenciáknak?

- | | | |
|-------------------------------|-------------------------------|-------------------------------|
| (a) $12x \equiv 19 \pmod{21}$ | (c) $24x \equiv 32 \pmod{28}$ | (e) $15x \equiv 55 \pmod{24}$ |
| (b) $18x \equiv 14 \pmod{30}$ | (d) $15x \equiv 42 \pmod{24}$ | (f) $21x \equiv 36 \pmod{30}$ |

1.25. feladat. Az alábbi linken elérhető játékban egy nyúl ugrál egy szabályos 28 oldalú sokszög csúcsain.

http://www.math.u-szeged.hu/~twaldha/tanitas/regi/dimat2_2021tavasz/nyul-sokszog.html

Mekkorákat ugorjon, hogy...

- (a) a 10. ugrással a 26-os csúcsba jusson?
- (b) a 12. ugrással a 26-os csúcsba jusson?
- (c) a 16. ugrással a 20-as csúcsba jusson? (És hogy a 16. ugrással érkezzen *először* a 20-as csúcsba?)

Kidolgozott feladat.

Melyek azok a 32-re végződő négyjegyű számok, amelyek oszthatóak 47-tel? Határozzuk meg az összes megoldást!

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 kért négyjegyű számra két lehetőség van: 2632 és 7332.

1.26. feladat. Melyik az a 4-re végződő háromjegyű szám, amely 63-mal osztva 1-et ad maradékkal?

1.27. feladat. Határozzuk meg azt a legkisebb háromjegyű természetes számot, amelynek 12-szerese 6-ot ad maradékkal 30-cal osztva.

1.5. Lineáris kongruenciarendszerek

A feladatok megoldása előtt célszerű megnézni az elméleti háttér bemutató videó(ka)t:

👉 https://youtu.be/m_J7XaKhQmE

Kidolgozott 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:

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

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. Ezt az egyenletet már [korábban megoldottuk](#) (csak ott nem y és z , hanem x és y voltak az ismeretlenek). Az egyenlet megoldása $y = 4 + 3t$, $z = 1 + 2t$ ($t \in \mathbb{Z}$). Ebből kifejezhetjük x -et: $x = 6y + 7 = 6 \cdot (4 + 3t) + 7 = 18t + 31$ (ugyanazt 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. Ezt a következő feladatban mutatjuk be.

Kidolgozott feladat.

Oldjuk meg az alábbi lineáris kongruenciarendszert.

$$\left. \begin{aligned} 8x &\equiv 6 \pmod{18} \\ 9x &\equiv 18 \pmod{42} \end{aligned} \right\}$$

Megoldás. Az első kongruencia megoldása: $x \equiv 3 \pmod{9}$, tehát x -et $x = 9y + 3$ alakban keressük. Ezt beírva a második kongruenciába azt kapjuk, hogy $81y + 27 \equiv 18 \pmod{42}$, azaz $-3y \equiv -9 \pmod{42}$. Ennek megoldása: $y \equiv 3 \pmod{14}$, tehát y -t $y = 14t + 3$ alakba írhatjuk. Visszahelyettesítve x felírásába, azt kapjuk, hogy $x = 9y + 3 = 9 \cdot (14t + 3) + 3 = 126t + 30$, azaz $x \equiv 30 \pmod{126}$.

Másik megoldás. Először oldjuk meg egyenként a kongruenciákat:

$$\left. \begin{aligned} x &\equiv 3 \pmod{9} \\ x &\equiv 2 \pmod{14} \end{aligned} \right\}$$

Ezt a kongruenciarendszert az előző feladat módszerével átírhatjuk a $9y + 3 = 14z + 2$ ($= x$) diofantoszi egyenletre, amelynek megoldása $y = 3 + 14t$, $z = 2 + 9t$ ($t \in \mathbb{Z}$). Ezután x -et megkaphatjuk akár y -ből akár z -ből; most a változatosság kedvéért használjuk z -t: $x = 14z + 2 = 14 \cdot (2 + 9t) + 2 = 126t + 30$, azaz $x \equiv 30 \pmod{126}$.

Kidolgozott feladat.

Oldjuk meg az alábbi lineáris kongruenciarendszert.

$$\left. \begin{array}{l} x \equiv 3 \pmod{4} \\ x \equiv 5 \pmod{6} \\ x \equiv 2 \pmod{7} \end{array} \right\}$$

Megoldás. Megoldjuk az első két kongruenciából álló részrendszert (kongruenciás számolással vagy diofantoszi egyenletre való átírással):

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

Ezt a kongruenciát „összerakjuk” az eredeti rendszer harmadik kongruenciájával, és megoldjuk ezt a rendszert is:

$$\left. \begin{array}{l} x \equiv 11 \pmod{12} \\ x \equiv 2 \pmod{7} \end{array} \right\} \iff x \equiv 23 \pmod{84}$$

Tehát a megoldás: $x \equiv 23 \pmod{84}$.

Kidolgozott 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. Megoldjuk az első kongruenciát, 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: $x = 12z + 11 = 12 \cdot (7t + 1) + 11 = 84t + 23$. Tehát a végeredmény: $x \equiv 23 \pmod{84}$.

Másik 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:

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

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

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

1.28. feladat. Oldjuk meg az alábbi lineáris kongruenciarendszereket.

❏ (a) $\left. \begin{aligned} x &\equiv 1 \pmod{14} \\ x &\equiv 7 \pmod{10} \end{aligned} \right\}$

(e) $\left. \begin{aligned} 3x &\equiv 15 \pmod{24} \\ 4x &\equiv 11 \pmod{21} \end{aligned} \right\}$

(i) $\left. \begin{aligned} 2x &\equiv 1 \pmod{5} \\ 5x &\equiv -1 \pmod{6} \\ 4x &\equiv 11 \pmod{9} \end{aligned} \right\}$

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

(f) $\left. \begin{aligned} x &\equiv 5 \pmod{6} \\ x &\equiv 3 \pmod{10} \\ x &\equiv 8 \pmod{45} \end{aligned} \right\}$

(j) $\left. \begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{7} \end{aligned} \right\}$

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

(g) $\left. \begin{aligned} 3x &\equiv 1 \pmod{5} \\ 5x &\equiv 3 \pmod{7} \\ 13x &\equiv 4 \pmod{9} \end{aligned} \right\}$

(k) $\left. \begin{aligned} 5x &\equiv 1 \pmod{6} \\ 7x &\equiv 9 \pmod{10} \end{aligned} \right\}$

(d) $\left. \begin{aligned} x &\equiv 3 \pmod{2} \\ x &\equiv 6 \pmod{5} \end{aligned} \right\}$

(h) $\left. \begin{aligned} x &\equiv 7 \pmod{8} \\ x &\equiv 6 \pmod{7} \end{aligned} \right\}$

(l) $\left. \begin{aligned} 2x &\equiv 18 \pmod{10} \\ 10x &\equiv 40 \pmod{12} \\ 15x &\equiv 9 \pmod{21} \end{aligned} \right\}$

Kidolgozott 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:

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

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.

■ **1.29. 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. Mászor 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?

1.30. feladat. Bizonyos megfigyelések szerint a varjak mindig azonos létszámú rajokban vándorolnak. Ha 11 varjúraj oly módon száll le egy fára, hogy a fa minden ágára 4 varjú kerül, akkor végül egy varjú egyedül marad. Ha 12 varjúraj száll le egy fa ágaira hetes csoportokban, akkor szintén egy varjú egyedül lesz egy ágon. Míg ha 13 varjúraj kilences csoportokban száll le egy fa ágaira, akkor az utolsó ágon 7 varjú lesz. Hány varjú van egy rajban, ha tudjuk, hogy ez a szám nem több, mint 100?

1.31. feladat. Ha 7 zacskó gümecukrot osztok el 10 gyerek között, akkor a végén 9 szem gümecukor marad meg. Ha 10 zacskót osztok el 14 gyerek között, akkor meg 6 marad. Hány darab gümecukor van egy-egy zacskóban, ha minden zacskóban ugyanannyi, mégpedig 50-nél több, de 150-nél kevesebb darab van?

1.32. feladat. Egy tizenhéttagú kalózcsapat egy zsák aranypént lopott. Amikor megpróbálták egyenlően elosztani, azt tapasztalták, hogy három aranypént kimaradt. A kimaradt aranyak fölötti vitában egy kalózt megöltek. Ezután újraosztották egyenlő arányban a zsákmányt, s most tíz arany maradt ki. Az e fölötti vitában egy újabb kalózt öltek meg, s ezután már el tudták osztani a lopott aranyat úgy, hogy mindenki ugyanannyit kapott. Legkevesebb hány aranypént zsákmányoltak?

1.33. 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 a kosárban. Legalább hány tojás lehet a kosárban?

1.34. feladat. Oldjuk meg a kínai maradéktétel segítségével az alábbi paraméteres kongruenciarendszereket.

$$\begin{array}{lll} \blacksquare \text{ (a)} & \left. \begin{array}{l} x \equiv c_1 \pmod{11} \\ x \equiv c_2 \pmod{6} \end{array} \right\} & \text{(b)} \quad \left. \begin{array}{l} x \equiv c_1 \pmod{10} \\ x \equiv c_2 \pmod{7} \end{array} \right\} & \text{(c)} \quad \left. \begin{array}{l} x \equiv c_1 \pmod{3} \\ x \equiv c_2 \pmod{4} \\ x \equiv c_2 \pmod{5} \end{array} \right\} \end{array}$$

1.6. Maradékosztályok

A feladatok megoldása előtt célszerű megnézni az elméleti háttér bemutató videó(ka)t:

👉 https://youtu.be/1t_OUyU8-Xk (maradékosztályok és maradékrendszerek)

👉 <https://youtu.be/08GhI3fdAbI> (számolás maradékosztályokkal)

■ **1.35. feladat.** Teljes maradékrendszert alkotnak-e az alábbi számok a megadott modulus szerint?

(a) 1000, 2000, 3000, 4000, 5000, 6000, 7000 modulo 7

(b) 2, 8, 14, ..., 302 modulo 51

(c) 3, 18, 33, ..., 678 modulo 46

1.36. feladat. Teljes maradékrendszert alkotnak-e az alábbi számok a megadott modulus szerint?

(a) 10, -1, 25, -13, 28, 38, 12 modulo 7

(c) 11, 21, 31, ..., 911 modulo 91

(b) 11, 22, 33, ..., 154 modulo 14

(d) 4, 9, 14, ..., 239 modulo 49

▲ **1.37. feladat.** Végezzük el $\mathbb{Z}_m$ -ben a számításokat. A végeredmény $\bar{0}, \bar{1}, \dots, \overline{m-1}$ valamelyike legyen.

■ (a) $\bar{8} + \bar{10}, \bar{8} - \bar{10}, \bar{8} \cdot \bar{10} \in \mathbb{Z}_{15}$

(d) $\bar{17} + \bar{15}, \bar{9} - \bar{15}, \bar{6} \cdot \bar{7} \in \mathbb{Z}_{21}$

■ (b) $\bar{10} + \bar{15}, \bar{10} - \bar{15}, \bar{10} \cdot \bar{15} \in \mathbb{Z}_{18}$

(e) $\bar{23} + \bar{25}, \bar{0} - \bar{21}, \bar{9} \cdot \bar{12} \in \mathbb{Z}_{33}$

(c) $\bar{10} + \bar{15}, \bar{10} - \bar{15}, \bar{10} \cdot \bar{15} \in \mathbb{Z}_{21}$

Kidolgozott feladat.

Oldjuk meg $\mathbb{Z}_{84}$ -ben az alábbi egyenleteket. (Az összes megoldást keressük meg és a megoldásokat $\bar{a}$ alakban adjuk meg, ahol $a \in \{0, 1, \dots, 83\}$.)

(a) $\bar{16} \cdot \bar{x} = \bar{12}$

(b) $\bar{16} \cdot \bar{x} = \bar{10}$

Megoldás.

(a) Az egyenlet a $16x \equiv 12 \pmod{84}$ kongruenciára vezet, aminek a megoldása $x \equiv 6 \pmod{21}$. Soroljuk fel az x értékeket, és nézzük meg, hogy milyen maradékokat adnak 84-gyel osztva:

x	...	-36	-15	6	27	48	69	90	111	...
$x \bmod 84$	...	48	69	6	27	48	69	6	27	...

Látjuk, hogy a kongruencia megoldásai négyféle maradékot tudnak adni 84-gyel osztva, ezért az egyenletnek $\mathbb{Z}_{84}$ -ben négy megoldás van: $\bar{6}, \bar{27}, \bar{48}, \bar{69}$.

Megjegyzés. Nem véletlen, hogy négy megoldást kaptunk, hiszen a kongruencia megoldása során a modulus a negyedére csökkent. Általában is hasonló a helyzet: az $ax \equiv b \pmod{m}$ kongruencia megoldásai egyetlen modulo $\frac{m}{\text{lko}(a,m)}$ maradékosztályt alkotnak (ha van megoldás egyáltalán), és ez a halmaz $\text{lko}(a,m)$ darab modulo m maradékosztályra „hasad”.

(b) Az egyenlet a $16x \equiv 10 \pmod{84}$ kongruenciára vezet, ennek pedig nincs megoldása, mert $\text{lko}(16, 84) = 4 \nmid 10$.

▲ 1.38. feladat. Oldjuk meg $\mathbb{Z}_m$ -ben az alábbi egyenleteket (az összes megoldást keressük meg!)

❏ (a) $\overline{10} \cdot \bar{x} = \bar{8}$ $\mathbb{Z}_{15}$ -ben

(f) $\bar{9} \cdot \bar{x} = \overline{15}$ $\mathbb{Z}_{12}$ -ben

(k) $\overline{10} \cdot \bar{x} = \overline{26}$ $\mathbb{Z}_{28}$ -ben

❏ (b) $\bar{9} \cdot \bar{x} = \bar{6}$ $\mathbb{Z}_{15}$ -ben

(g) $\bar{5} \cdot \bar{x} = \overline{11}$ $\mathbb{Z}_{13}$ -ban

(l) $\overline{25} \cdot \bar{x} = \overline{35}$ $\mathbb{Z}_{90}$ -ben

❏ (c) $\bar{7} \cdot \bar{x} = \bar{6}$ $\mathbb{Z}_{15}$ -ben

(h) $\overline{28} \cdot \bar{x} = \overline{23}$ $\mathbb{Z}_{40}$ -ben

(m) $\overline{30} \cdot \bar{x} = \bar{9}$ $\mathbb{Z}_{51}$ -ben

❏ (d) $\bar{6} \cdot \bar{x} = \bar{4}$ $\mathbb{Z}_8$ -ban

(i) $\overline{28} \cdot \bar{x} = \overline{24}$ $\mathbb{Z}_{40}$ -ben

❏ (e) $\overline{88} \cdot \bar{x} = \overline{42}$ $\mathbb{Z}_{55}$ -ben

(j) $\bar{3} \cdot \bar{x} = \bar{4}$ $\mathbb{Z}_5$ -ben

1.7. Redukált maradékosztályok, multiplikatív inverz, multiplikatív rend

A feladatok megoldása előtt célszerű megnézni az elméleti háttér bemutató videó(ka)t:

👉 <https://youtu.be/na257Lu75CU>

Kidolgozott feladat.

Számítsuk ki $\mathbb{Z}_{21}$ -ben az alábbi elemeket. (A végeredményt mindig $\bar{a}$ alakban adjuk meg, ahol $a \in \{0, 1, \dots, 20\}$.)

(a) $\bar{5}^{-2} = ?$

(b) $\bar{6}^{-5} = ?$

(c) $\bar{6}! = ?$

Megoldás.

- (a) Az $\bar{5}^{-2}$ hatványt kétféleképpen is ki tudjuk számolni: $\bar{5}^{-2} = (\bar{5}^{-1})^2 = \overline{-4}^2 = \overline{16}$ (itt az $\bar{5}^{-1}$ hatványt, vagyis $\bar{5}$ multiplikatív inverzét, az $5x \equiv 1 \pmod{21}$ lineáris kongruencia megoldásával kaptuk), vagy pedig $\bar{5}^{-2} = (\bar{5}^2)^{-1} = \bar{4}^{-1} = \overline{16}$ (itt a $\bar{4}^{-1}$ hatványt a $4x \equiv 1 \pmod{21}$ lineáris kongruencia megoldásával kaptuk).
- (b) A $\bar{6}^{-5}$ hatvány nem értelmezett, mert 6 nem relatív prím 21-hez, ezért nincs modulo 21 multiplikatív inverze.
- (c) A $\bar{6}!$ maradékosztályt megkaphatjuk úgy, hogy a $6! = 720$ számot maradékosan osztjuk 21-gyel, de kisebb lépésekben haladva nem kell ilyen nagy számmal dolgoznunk: $\bar{6}! = \bar{2} \cdot \bar{3} \cdot \bar{4} \cdot \bar{5} \cdot \bar{6} = \bar{24} \cdot \bar{30} = \bar{3} \cdot \bar{9} = \bar{27} = \bar{6}$.

▲ 1.39. feladat. Határozzuk meg a megadott multiplikatív inverzeket.

❏ (a) $\overline{88}^{-1} \in \mathbb{Z}_{55}$

(c) $\bar{5}^{-1} \in \mathbb{Z}_{14}$

(e) $\bar{3}^{-1} \in \mathbb{Z}_5$

❏ (b) $\bar{5}^{-1} \in \mathbb{Z}_{13}$

(d) $\bar{9}^{-1} \in \mathbb{Z}_{12}$

(f) $\overline{29}^{-1} \in \mathbb{Z}_{73}$

1.40. feladat. Soroljuk fel $\mathbb{Z}_m^*$ elemeit, és állítsuk az elemeket párba az inverzükkel.

❏ (a) $m = 15$

(c) $m = 7$

(e) $m = 10$

❏ (b) $m = 9$

(d) $m = 8$

(f) $m = 11$

Kidolgozott feladat.

Határozzuk meg $\mathbb{Z}_{18}^*$ -ban a megadott elemek multiplikatív rendjét és hatványait. (A hatványokat mindig $\bar{a}$ alakban adjuk meg, ahol $a \in \{0, 1, \dots, 17\}$.)

(a) $o(\bar{5}) = ?$, $\bar{5}^{100} = ?$

(b) $o(\bar{8}) = ?$, $\bar{8}^{100} = ?$

Megoldás.

(a) Kezdjük el hatványozni az $\bar{5} \in \mathbb{Z}_{18}$ elemet:

k	$\dots$	0	1	2	3	4	5	6	7	8	$\dots$
$\bar{5}^k$	$\dots$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{-1}$	$\bar{-5}$	$\bar{-7}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\dots$

A hatodik hatványra jött ki először $\bar{1}$, ezért $o(\bar{5}) = 6$, és így $\bar{5}$ hatványozásakor a kitevőt modulo 6 kell figyelembe venni. Ezért 100-at maradékosan osztjuk 6-tal: azt kapjuk, hogy $100 \equiv 4 \pmod{6}$. Tehát $\bar{5}^{100} = \bar{5}^4 = \bar{-5} = \bar{13}$ (a táblázatból kiolvasható).

(b) Mivel 8 nem relatív prím 18-hoz, azaz $\bar{8} \notin \mathbb{Z}_{18}^*$, az $o(\bar{8})$ multiplikatív rend nem értelmezett (bármeddig hatványozzuk is a $\bar{8} \in \mathbb{Z}_{18}$ elemet, soha nem fog kijönni $\bar{1}$). Ennek ellenére $\bar{8}^{100}$ értelmezett, és kiszámításához segít, ha megfigyeljük $\bar{8}$ hatványainak sorozatában a szabályszerűséget:

k	0	1	2	3	4	5	6	7	8	$\dots$
$\bar{8}^k$	$\bar{1}$	$\bar{8}$	$\bar{10}$	$\bar{8}$	$\bar{10}$	$\bar{8}$	$\bar{10}$	$\bar{8}$	$\bar{10}$	$\dots$

Innen látható, hogy $\bar{8}$ pozitív egész kitevős hatványainál csak a kitevő paritása számít, tehát $\bar{8}^{100} = \bar{10}$.

1.41. feladat. Határozzuk meg a megadott maradékosztály multiplikatív rendjét és számítsuk ki a hatványait.

❖ (a) $\mathbb{Z}_7^*$ -ban $o(\bar{2}) = ?$, $\bar{2}^{102} = ?$, $\bar{2}^{2021} = ?$

(f) $\mathbb{Z}_{25}^*$ -ban $o(\bar{21}) = ?$, $\bar{21}^{153} = ?$, $\bar{21}^{2024} = ?$

❖ (b) $\mathbb{Z}_{10}^*$ -ban $o(\bar{3}) = ?$, $\bar{3}^{402} = ?$, $\bar{3}^{2021} = ?$

(g) $\mathbb{Z}_{18}^*$ -ban $o(\bar{5}) = ?$, $\bar{5}^{908} = ?$, $\bar{5}^{-1} = ?$

(c) $\mathbb{Z}_{11}^*$ -ban $o(\bar{4}) = ?$, $\bar{4}^{200} = ?$, $\bar{4}^{2023} = ?$

(h) $\mathbb{Z}_{25}^*$ -ban $o(\bar{6}) = ?$, $\bar{6}^{912} = ?$, $\bar{6}^{-67} = ?$

(d) $\mathbb{Z}_{15}^*$ -ban $o(\bar{13}) = ?$, $\bar{13}^{-102} = ?$, $\bar{13}^{2023} = ?$

(i) $\mathbb{Z}_{40}^*$ -ban $o(\bar{2}) = ?$, $\bar{2}^{102} = ?$, $\bar{2}^{-11} = ?$

(e) $\mathbb{Z}_{10}^*$ -ban $o(\bar{2}) = ?$, $\bar{2}^{402} = ?$, $\bar{2}^{2024} = ?$

(j) $\mathbb{Z}_{20}^*$ -ban $o(\bar{6}) = ?$, $\bar{6}^6 = ?$, $\bar{6}^{2026} = ?$

1.8. Az Euler-féle φ függvény

A feladatok megoldása előtt célszerű megnézni az elméleti háttér bemutató videó(ka)t:

👉 <https://youtu.be/tu130aZJnyc>

Kidolgozott feladat.

Számítsuk ki $\varphi(7!)$ értékét.

Megoldás. Készítsük el $7!$ prímszámhatványozós felbontását: $7! = 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$. Az Euler-féle φ függvény képletét használva azt kapjuk, hogy

$$\begin{aligned}\varphi(7!) &= \varphi(2^4 \cdot 3^2 \cdot 5 \cdot 7) = \varphi(2^4) \cdot \varphi(3^2) \cdot \varphi(5) \cdot \varphi(7) = \\ &= (2^4 - 2^3) \cdot (3^2 - 3^1) \cdot (5 - 1) \cdot (7 - 1) = 8 \cdot 6 \cdot 4 \cdot 6 = 1152.\end{aligned}$$

1.42. feladat. Számítsuk ki az Euler-féle φ függvény alábbi értékeit.

- | | | |
|---------------------------|-----------------------|------------------------|
| ❏ (a) $\varphi(1000) = ?$ | (d) $\varphi(60) = ?$ | (g) $\varphi(30) = ?$ |
| ❏ (b) $\varphi(360) = ?$ | (e) $\varphi(88) = ?$ | (h) $\varphi(75) = ?$ |
| ❏ (c) $\varphi(2021) = ?$ | (f) $\varphi(20) = ?$ | (i) $\varphi(128) = ?$ |

1.43. feladat. Oldjuk meg az egyenletet a természetes számok halmazán.

- | | | |
|----------------------|---------------------------|----------------------------------|
| (a) $\varphi(x) = 4$ | (d) $2\varphi(x) = x$ | (g) $\varphi(x^2) = 2x$ |
| (b) $\varphi(x) = 5$ | (e) $\varphi(x) = x - 8$ | (h) $\varphi(x^2) = x\varphi(x)$ |
| (c) $\varphi(x) = 6$ | (f) $\varphi(x) = x - 10$ | |

1.9. Az Euler–Fermat-tétel

A feladatok megoldása előtt célszerű megnézni az elméleti háttérrel bemutató videó(ka)t:

👉 <https://youtu.be/21jdmZsFfG0> (az Euler–Fermat-tétel)

👉 <https://youtu.be/Qld3r2pkbs8> (az Euler–Fermat-tétel bizonyítása)

Kidolgozott feladat.

Mennyit ad 98^{272} maradékul 27-tel osztva? (A végeredmény egy 0 és 26 közötti szám legyen.)

Megoldás.

- Először csökkentsük a hatvány alapját: $98 \equiv 17 \pmod{27}$, ezért $98^{272} \equiv 17^{272} \pmod{27}$.
- Az Euler–Fermat-tételt fogjuk használni, ezért ellenőrizzük, hogy teljesül a tétel feltétele, azaz a hatvány alapja és a modulus relatív prím: $\text{luko}(17, 27) = 1$.
- Szükségünk lesz a modulus φ -értékére: $\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 18$.
- Az Euler–Fermat-tétel szerint $17^{18} \equiv 1 \pmod{27}$; ezt a következőképpen használjuk a hatvány kiszámítására:

$$17^{272} \equiv 17^{15 \cdot 18 + 2} \equiv (17^{18})^{15} \cdot 17^2 \equiv 1^{15} \cdot 17^2 \equiv 17^2 \equiv 289 \equiv 19 \pmod{27}.$$

(A kitevőben az történt, hogy 272-t elosztottuk maradékosan $\varphi(27) = 18$ -cal. Kiderült, hogy a hányados nem is fontos, mert az úgyis csak az 1-es kitevőjében szerepel. A végeredményhez csak arra volt szükség, hogy 272 kettőt ad maradékul 18-cal osztva.)

Tehát 98^{272} tizenkilencet ad maradékul 27-tel osztva.

Megjegyzés. Figyeljük meg, hogy a hatvány alapját modulo 27 kellett figyelembe venni, a kitevő viszont nem modulo 27, hanem modulo $\varphi(27)$ számít. Ez általában is így van: ha $\text{luko}(a, m) = 1$ és $k \equiv \ell \pmod{m}$, akkor, az Euler–Fermat-tételnek köszönhetően, $a^k \equiv a^\ell \pmod{m}$.

Kidolgozott feladat.

Mennyit ad 873^{2002} maradékul 28-cal osztva? (A végeredmény egy 0 és 27 közötti szám legyen.)

Megoldás. Az előző feladat gondolatmenetének lépéseit követjük:

- alap redukálása: $873 \equiv 5 \pmod{28}$;
- feltétel ellenőrzése: $\text{luko}(5, 28) = 1$;
- a modulus φ -értékének kiszámítása: $\varphi(28) = \varphi(2^2 \cdot 7) = \varphi(2^2) \cdot \varphi(7) = 2 \cdot 6 = 12$;
- kitevő redukálása: $2002 \equiv 10 \pmod{12}$.

Az Euler–Fermat-tételt használva a fentiek alapján ezt kapjuk: $873^{2002} \equiv 5^{10} \pmod{28}$. 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 873^{2002} kilencet ad maradékul 28-cal osztva.

Másik megoldás. Jobban járnánk, ha a 4. pontban 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. Ezt a feladatot [korábban már megoldottuk](#). Ott azt figyeltük meg, hogy 5 hatványainak modulo 28 maradékai hatosával ismétlődnek, azaz $o(5) = 6$ teljesül az $\bar{5} \in \mathbb{Z}_{28}$ maradékosztályra. 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.

1.44. feladat. Határozzuk meg a hatvány maradékát a megadott modulus szerint.

- | | | |
|--------------------------------------|--------------------------------------|------------------------------------|
| ❏ (a) $63^{42} \equiv ? \pmod{50}$ | (e) $19^{81} \equiv ? \pmod{75}$ | (i) $557^{517} \equiv ? \pmod{53}$ |
| ❏ (b) $123^{765} \equiv ? \pmod{11}$ | (f) $42^{62} \equiv ? \pmod{25}$ | (j) $15^{159} \equiv ? \pmod{34}$ |
| (c) $111^{50} \equiv ? \pmod{52}$ | (g) $6^{418} \equiv ? \pmod{29}$ | (k) $20^{449} \equiv ? \pmod{31}$ |
| (d) $3^{65} \equiv ? \pmod{128}$ | (h) $4447^{2018} \equiv ? \pmod{44}$ | (l) $3^{298} \equiv ? \pmod{25}$ |

Kidolgozott feladat.

Mi az utolsó két számjegye a 2003^{2004} számnak?

Megoldás. Az utolsó két számjegyet a modulo 100 maradék adja meg. A szokásos előkészítő lépéseket tesszük az Euler–Fermat-tétel felhasználása előtt:

- $2003 \equiv 3 \pmod{100}$;
- $\text{luko}(3, 100) = 1$;
- $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2) \cdot \varphi(5^2) = 2 \cdot 20 = 40$;
- $2004 \equiv 4 \pmod{40}$.

Most jöhet az Euler–Fermat-tétel: $2003^{2004} \equiv 3^4 \equiv 81 \pmod{100}$. Tehát 2003^{2004} utolsó két számjegye 8 és 1.

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

1.46. feladat. Milyen nap lesz $\underbrace{11 \dots 11}_{99}$ nap múlva?

1.47. feladat. Határozzuk meg a hatványok maradékát a megadott modulus szerint. (Az emeletes hatványokat $a^{(b^c)}$ zárójelezéssel értelmezzük.)

- | | |
|--|--|
| ❏ (a) $13^{321^{50}} \equiv ? \pmod{87}$ | (c) $80^{111^{50}} \equiv ? \pmod{53}$ |
| (b) $91^{441^{222}} \equiv ? \pmod{88}$ | (d) $95^{81^{99}} \equiv ? \pmod{46}$ |

1.48. feladat. Milyen nap lesz $711^{185^{937}}$ nap múlva?

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

VÉGEREDMÉNYEK, MEGOLDÁSOK

1. Számelmélet

1.1. Oszthatóság, legnagyobb közös osztó, euklideszi algoritmus

1.1. feladat.

- (a) 7 többszörösei: $\{7k : k \in \mathbb{Z}\}$
- (b) 420 többszörösei: $\{420k : k \in \mathbb{Z}\}$
- (c) 4 többszörösei: $\{4k : k \in \mathbb{Z}\}$
- (d) 28 osztói: $\{\pm 1, \pm 2, \pm 4, \pm 7, \pm 14, \pm 28\}$
- (e) 7 többszörösei: $\{7k : k \in \mathbb{Z}\}$
- (f) 264 többszörösei: $\{264k : k \in \mathbb{Z}\}$
- (g) 18 osztói: $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$
- (h) 300 többszörösei: $\{300k : k \in \mathbb{Z}\}$
- (i) 33 osztói: $\{\pm 1, \pm 3, \pm 11, \pm 33\}$

👉 megoldás: <https://youtu.be/mPigchEMSEk>

👉 megoldás: <https://youtu.be/t4nG7hH4Tj0>

👉 megoldás: <https://youtu.be/LwNf6SZVsRY>

👉 megoldás: <https://youtu.be/uXRxFfHRidE>

1.2. feladat. 60

👉 megoldás: <https://youtu.be/1QozYexyCbE>

1.3. feladat.

- (a) $\text{lko}(a, b) = 4 = -3a + 4b$, $\text{lkkt}(a, b) = 252$
- (b) $\text{lko}(a, b) = 6 = 2a - 5b$, $\text{lkkt}(a, b) = 390$
- (c) $\text{lko}(a, b) = 7 = -194a + 75b$, $\text{lkkt}(a, b) = 580139$
- (d) $\text{lko}(a, b) = 2 = 5a - 7b$, $\text{lkkt}(a, b) = 816$
- (e) $\text{lko}(a, b) = 23 = -3a + 7b$, $\text{lkkt}(a, b) = 2576$
- (f) $\text{lko}(a, b) = 77 = 2a - b$, $\text{lkkt}(a, b) = 7007$

👉 megoldás: <https://youtu.be/mPigchEMSEk>

👉 megoldás: <https://youtu.be/O9dvXVao1s4>

👉 megoldás: https://youtu.be/yhc3rs_xcEU

1.4. feladat. A negyedik egységgyökök, azaz $z = 1, -1, i, -i$.

1.2. Lineáris diofantoszi egyenletek

1.5. feladat.

- (a) $x = 2 + 5t$, $y = -2 - 6t$ ($t \in \mathbb{Z}$)
- (b) $x = 2 - 5t$, $y = 2 - 7t$ ($t \in \mathbb{Z}$)
- (c) $x = -1 + 17t$, $y = 2 - 24t$ ($t \in \mathbb{Z}$)
- (d) $x = -1 + 5t$, $y = 3 - 13t$ ($t \in \mathbb{Z}$)
- (e) $x = -3 + 7t$, $y = 3 - 6t$ ($t \in \mathbb{Z}$)
- (f) $x = 4 + 12t$, $y = -2 - 7t$ ($t \in \mathbb{Z}$)
- (g) $x = 22 + 5t$, $y = 11 + 3t$ ($t \in \mathbb{Z}$)
- (h) $x = -689 + 571t$, $y = 286 - 237t$ ($t \in \mathbb{Z}$)
- (i) $x = 1479 + 418t$, $y = -697 - 197t$ ($t \in \mathbb{Z}$)
- (j) nincs megoldása

👉 megoldás: <https://youtu.be/jUS-e1yxCR4>

👉 megoldás: <https://youtu.be/DAdW4f14Z4Y>

1.6. feladat.

- (a) nincs megoldása
- (b) van megoldása
- (c) van megoldása
- (d) van megoldása
- (e) van megoldása
- (f) nincs megoldása

1.7. feladat.

- (a) Csak az 1. képlet helyes.
- (b) A 2. és a 3. képlet helyes, az 1. képlet nem.
- (c) Csak a 3. képlet helyes.
- (d) Az 1. és a 3. képlet helyes, a 2. képlet nem.

1.8. feladat.

- (a) $2 = |\{17, 25\}|$
- (b) $3 = |\{38, 47, 56\}|$
- (c) $7 = |\{10, 13, 16, 19, 22, 25, 28\}|$
- (d) $3 = |\{19, 26, 33\}|$
- (e) $2 = |\{25, 38\}|$

👉 megoldás: <https://youtu.be/dhQjZvZYFC8>

1.9. feladat. $10 \cdot 20 + 1 \cdot 45$ és $1 \cdot 20 + 5 \cdot 45$

👉 megoldás: <https://youtu.be/pHs93VAV56g>

1.10. feladat.

- (a) Csak a 4-nél lévőt tudja megszerezni.
- (b) $(-2) \cdot a + 3 \cdot b = 12$ (5 ugrás)

👉 megoldás: <https://youtu.be/Ouz2jiwxJeg>

👉 megoldás: <https://youtu.be/Ouz2jiwxJeg>

1.11. feladat. Az első esetben $18 \cdot a + 14 \cdot b = 1000$ (32 ugrás), a második esetben $(-1) \cdot a + 27 \cdot b = 1000$ (28 ugrás).

1.12. feladat. Végtelen sok megoldás van, íme a két legegyszerűbb: $12 \cdot 21 - 10 \cdot 25 = 2$ és $11 \cdot 25 - 13 \cdot 21 = 2$.

1.13. feladat. Gombóc Artúr 17 éves (és az ötödik napon fogyott el a csokoládé). Az alábbi linken a számítógép lépésenként végigvezet a feladat megoldásán:

http://www.math.u-szeged.hu/~twaldha/tanitas/regi/dimat2_2021tavasz/gombocartur.html

1.14. feladat. A rágó 56 forintba került, és 24 gyerek választotta, a csoki 125 forintba került, és 6 gyerek választotta.

1.15. feladat. 6, 10, 6

👉 megoldás: <https://youtu.be/XoX3vjwV9MI>

1.16. feladat. 7, 5, 10

1.17. feladat. 1, 1, 5

1.3. A modulo m kongruenciareláció

1.18. feladat.

- (a) 6
- (b) 1
- (c) 6
- (d) 7
- (e) 8
- (f) 9
- (g) 13
- (h) 7
- (i) 4

👉 megoldás: https://youtu.be/_-h76rgIvgg

👉 megoldás: https://youtu.be/_-h76rgIvgg

👉 megoldás: https://youtu.be/_-h76rgIvgg

👉 megoldás: https://youtu.be/RCqlfd5_iek

1.19. feladat.

- (a) 0
- (b) 6
- (c) 2
- (d) 0
- (e) 0
- (f) 6
- (g) 2
- (h) 6
- (i) 2

1.20. feladat. 2, 7, 14

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

👉 megoldás: https://youtu.be/_-h76rgIvgg

1.22. feladat. $2^{5n+1} + 5^{n+2} = 2 \cdot 32^n + 25 \cdot 5^n \equiv 2 \cdot 5^n + 25 \cdot 5^n = 27 \cdot 5^n \equiv 0 \pmod{27}$

1.4. Lineáris kongruenciák

1.23. feladat.

- (a) $x \equiv 3 \pmod{5}$
- (b) $x \equiv 11 \pmod{14}$
- (c) $x \equiv 3 \pmod{4}$
- (d) $x \equiv 61 \pmod{73}$
- (e) $x \equiv 2 \pmod{4}$
- (f) $x \equiv 5 \pmod{34}$
- (g) $x \equiv 2 \pmod{17}$
- (h) nincs megoldása
- (i) $x \equiv 10 \pmod{13}$
- (j) $x \equiv 21 \pmod{31}$
- (k) $x \equiv 44 \pmod{53}$
- (l) $x \equiv 9 \pmod{23}$

👉 megoldás: <https://youtu.be/WVdonTsgGZU>

👉 megoldás: <https://youtu.be/WVdonTsgGZU>

👉 megoldás: <https://youtu.be/aqndyWxassg>

👉 megoldás: https://youtu.be/OKK5Qwo_oYM

1.24. feladat.

- (a) nincs megoldása
- (b) nincs megoldása
- (c) van megoldása
- (d) van megoldása
- (e) nincs megoldása
- (f) van megoldása

1.25. feladat.

- (a) 11, 25
- (b) ez lehetetlen
- (c) 3, 10, 17, 24 (először: 3, 17)

1.26. feladat. 694

1.27. feladat. 103

1.5. Lineáris kongruenciarendszerek

1.28. feladat.

- (a) $x \equiv 57 \pmod{70}$
- (b) $x \equiv 43 \pmod{90}$
- (c) $x \equiv 214 \pmod{315}$
- (d) $x \equiv 1 \pmod{10}$
- (e) $x \equiv 29 \pmod{168}$
- (f) $x \equiv 53 \pmod{90}$
- (g) $x \equiv 37 \pmod{315}$
- (h) $x \equiv -1 \pmod{56}$
- (i) nincs megoldása
- (j) $x \equiv 18 \pmod{35}$
- (k) $x \equiv 17 \pmod{30}$
- (l) $x \equiv 184 \pmod{210}$

👉 megoldás: https://youtu.be/m_J7XaKhQmE

👉 megoldás: <https://youtu.be/Mt1eWRo3mV8>

👉 megoldás: <https://youtu.be/ENqm2oqMmR>

1.29. feladat. 47

👉 megoldás: <https://youtu.be/VW7nCtXrgjY>

1.30. feladat. 31

1.31. feladat. 107

1.32. feladat. 3930

1.33. feladat. 119

1.34. feladat.

- (a) $x \equiv 12c_1 + 55c_2 \pmod{66}$
- (b) $x \equiv 21c_1 + 50c_2 \pmod{70}$
- (c) $x \equiv 40c_1 + 45c_2 + 36c_3 \pmod{60}$

👉 megoldás: https://youtu.be/m_J7XaKhQmE

1.6. Maradékosztályok

1.35. feladat.

- (a) igen
- (b) nem
- (c) igen

👉 megoldás: https://youtu.be/1t_OUyU8-Xk

👉 megoldás: <https://youtu.be/kLsPdMoDZrY>

👉 megoldás: <https://youtu.be/kLsPdMoDZrY>

1.36. feladat.

- (a) nem
- (b) igen
- (c) igen
- (d) nem

1.37. feladat.

- (a) $\overline{3}$, $\overline{13}$, $\overline{5}$
- (b) $\overline{7}$, $\overline{13}$, $\overline{6}$
- (c) $\overline{4}$, $\overline{16}$, $\overline{3}$
- (d) $\overline{11}$, $\overline{15}$, $\overline{0}$
- (e) $\overline{15}$, $\overline{12}$, $\overline{9}$

👉 megoldás: <https://youtu.be/08GhI3fdAbI>

👉 megoldás: <https://youtu.be/yTB6jZGYpng>

1.38. feladat.

- (a) nincs megoldása
- (b) $\overline{x} = \overline{4}$, $\overline{9}$, $\overline{14}$
- (c) $\overline{x} = \overline{3}$
- (d) $\overline{x} = \overline{2}$, $\overline{6}$
- (e) nincs megoldása
- (f) $\overline{x} = \overline{3}$, $\overline{7}$, $\overline{11}$
- (g) $\overline{x} = \overline{10}$
- (h) nincs megoldása
- (i) $\overline{x} = \overline{8}$, $\overline{18}$, $\overline{28}$, $\overline{38}$
- (j) $\overline{x} = \overline{3}$
- (k) $\overline{x} = \overline{11}$, $\overline{25}$
- (l) $\overline{x} = \overline{5}$, $\overline{23}$, $\overline{41}$, $\overline{59}$, $\overline{77}$
- (m) $\overline{x} = \overline{2}$, $\overline{19}$, $\overline{36}$

👉 megoldás: <https://youtu.be/08GhI3fdAbI>

👉 megoldás: <https://youtu.be/08GhI3fdAbI>

👉 megoldás: <https://youtu.be/na257Lu75CU>

👉 megoldás: <https://youtu.be/eseKJbPJbcs>

👉 megoldás: <https://youtu.be/eseKJbPJbcs>

1.7. Redukált maradékosztályok, multiplikatív inverz, multiplikatív rend

1.39. feladat.

- (a) $\overline{88}^{-1} \in \mathbb{Z}_{55}$ nem értelmezett
- (b) $\overline{5}^{-1} = \overline{8} \in \mathbb{Z}_{13}$
- (c) $\overline{5}^{-1} = \overline{3} \in \mathbb{Z}_{14}$
- (d) $\overline{9}^{-1} \in \mathbb{Z}_{12}$ nem értelmezett
- (e) $\overline{3}^{-1} = \overline{2} \in \mathbb{Z}_5$
- (f) $\overline{29}^{-1} = \overline{68} \in \mathbb{Z}_{73}$

👉 megoldás: <https://youtu.be/yjj70WqAuK0>

👉 megoldás: <https://youtu.be/yjj70WqAuK0>

1.40. feladat. Az inverz párok tagjai szorosan egymás mellé vannak írva; amelyik elemnek nincs „párja” az saját magának az inverze.

(a) $\mathbb{Z}_{15}^* = \{\bar{1}; \bar{2}, \bar{8}; \bar{4}; \bar{7}, \bar{13}; \bar{11}; \bar{14}\}$

👉 megoldás: <https://youtu.be/na257Lu75CU>

(b) $\mathbb{Z}_9^* = \{\bar{1}; \bar{2}, \bar{5}; \bar{4}, \bar{7}; \bar{8}\}$

👉 megoldás: <https://youtu.be/t0CkN8RJv0g>

(c) $\mathbb{Z}_7^* = \{\bar{1}; \bar{2}, \bar{4}; \bar{3}, \bar{5}; \bar{6}\}$

(d) $\mathbb{Z}_8^* = \{\bar{1}; \bar{3}; \bar{5}; \bar{7}\}$

(e) $\mathbb{Z}_{10}^* = \{\bar{1}; \bar{3}, \bar{7}; \bar{9}\}$

(f) $\mathbb{Z}_{11}^* = \{\bar{1}; \bar{2}, \bar{6}; \bar{3}, \bar{4}; \bar{5}, \bar{9}; \bar{7}, \bar{8}; \bar{10}\}$

1.41. feladat.

(a) $\mathbb{Z}_7^*$ -ban $o(\bar{2}) = 3$, $\bar{2}^{102} = \bar{1}$, $\bar{2}^{2021} = \bar{4}$

👉 megoldás: <https://youtu.be/na257Lu75CU>

(b) $\mathbb{Z}_{10}^*$ -ban $o(\bar{3}) = 4$, $\bar{3}^{402} = \bar{9}$, $\bar{3}^{2021} = \bar{3}$

👉 megoldás: <https://youtu.be/2RxZ-dqYC3k>

(c) $\mathbb{Z}_{11}^*$ -ban $o(\bar{4}) = 5$, $\bar{4}^{200} = \bar{1}$, $\bar{4}^{2023} = \bar{9}$

(d) $\mathbb{Z}_{15}^*$ -ban $o(\bar{13}) = 4$, $\bar{13}^{-102} = \bar{4}$, $\bar{13}^{2023} = \bar{7}$

(e) $\bar{2} \notin \mathbb{Z}_{10}^*$, így $o(\bar{2})$ nem ért., $\bar{2}^{402} = \bar{4}$, $\bar{2}^{2024} = \bar{6}$

(f) $\mathbb{Z}_{25}^*$ -ban $o(\bar{21}) = 5$, $\bar{21}^{153} = \bar{11}$, $\bar{21}^{2024} = \bar{6}$

(g) $\mathbb{Z}_{18}^*$ -ban $o(\bar{5}) = 6$, $\bar{5}^{908} = \bar{7}$, $\bar{5}^{-1} = \bar{11}$

(h) $\mathbb{Z}_{25}^*$ -ban $o(\bar{6}) = 5$, $\bar{6}^{912} = \bar{11}$, $\bar{6}^{-67} = \bar{16}$

(i) $\bar{2} \notin \mathbb{Z}_{40}^*$, így $o(\bar{2})$ nem ért., $\bar{2}^{102} = \bar{24}$, $\bar{2}^{-11}$ nem ért.

(j) $\bar{6} \notin \mathbb{Z}_{20}^*$, így $o(\bar{6})$ nem ért., $\bar{6}^6 = \bar{16}$, $\bar{6}^{2026} = \bar{16}$

1.8. Az Euler-féle φ függvény

1.42. feladat.

(a) $\varphi(1000) = 400$

👉 megoldás: <https://youtu.be/tul30aZJnyc>

(b) $\varphi(360) = 96$

👉 megoldás: <https://youtu.be/tul30aZJnyc>

(c) $\varphi(2021) = 1932$

👉 megoldás: <https://youtu.be/tul30aZJnyc>

(d) $\varphi(60) = 16$

(e) $\varphi(88) = 40$

(f) $\varphi(20) = 8$

(g) $\varphi(30) = 8$

(h) $\varphi(75) = 40$

(i) $\varphi(128) = 64$

1.43. feladat.

- (a) $x = 5, 8, 10, 12$
- (b) nincs megoldása
- (c) $x = 7, 9, 14, 18$
- (d) $x = 2^k$ ($k \in \mathbb{N}$)
- (e) $x = 12, 14, 16$
- (f) nincs megoldása
- (g) $x = 3, 4, 6$
- (h) minden $x \in \mathbb{N}$ esetén teljesül

1.9. Az Euler–Fermat-tétel

1.44. feladat.

- (a) $63^{42} \equiv 13^2 \equiv 19 \pmod{50}$
- (b) $123^{765} \equiv 2^5 \equiv 10 \pmod{11}$
- (c) $111^{50} \equiv 7^2 \equiv 49 \pmod{52}$
- (d) $3^{65} \equiv 3^1 \equiv 3 \pmod{128}$
- (e) $19^{81} \equiv 19^1 \equiv 19 \pmod{75}$
- (f) $42^{62} \equiv 17^2 \equiv 14 \pmod{25}$
- (g) $6^{418} \equiv 6^{-2} \equiv 25 \pmod{29}$
- (h) $4447^{2018} \equiv 3^{-2} \equiv 5 \pmod{44}$
- (i) $557^{517} \equiv 27^{-3} \equiv 8 \pmod{53}$
- (j) $15^{159} \equiv 15^{-1} \equiv 25 \pmod{34}$
- (k) $20^{449} \equiv 20^{-1} \equiv 14 \pmod{31}$
- (l) $3^{298} \equiv 3^{-2} \equiv 14 \pmod{25}$

👉 megoldás: <https://youtu.be/wfuSez0gA80>

👉 megoldás: <https://youtu.be/21jdmZsFfG0>

👉 megoldás: <https://youtu.be/KVMvp9UBUno>

👉 megoldás: <https://youtu.be/21jdmZsFfG0>

1.45. feladat. $1997^{1998} \equiv (-3)^{-2} \equiv 89 \pmod{100} \implies$ az utolsó két jegy 8 és 9

1.46. feladat. $\underbrace{11 \dots 11}_{99} \equiv 9^{-1} \cdot \underbrace{99 \dots 99}_{99} \equiv 4 \cdot (10^{99} - 1) \equiv 4 \cdot (3^3 - 1) \equiv 4 \cdot 26 \equiv 4 \cdot 5 \equiv -1 \pmod{7} \implies$ ugyanolyan nap lesz, mint amilyen tegnap volt

1.47. feladat.

- (a) $13^{321^{50}} \equiv 13^{41^2} \equiv 13^1 \equiv 13 \pmod{87}$
- (b) $91^{441^{222}} \equiv 3^{1^{222}} \equiv 3 \pmod{88}$
- (c) $91^{441^{222}} \equiv 3^{1^{222}} \equiv 3 \pmod{88}$
- (d) $80^{111^{50}} \equiv 27^{7^2} \equiv 27^{-3} \equiv 8 \pmod{53}$
- (e) $95^{81^{99}} \equiv 3^{15^{-1}} \equiv 3^3 \equiv 27 \pmod{46}$

👉 megoldás: https://youtu.be/Xoo_3zgZhsY

1.48. feladat. $711^{185^{937}} \equiv 4^{(-1)^1} \equiv 4^{-1} \equiv 2 \pmod{7} \implies$ ugyanolyan nap lesz, mint holnapután

1.49. feladat. $googolplex = 10^{10^{100}} \equiv 10^4 \equiv (-5)^2 \equiv 4 \pmod{21}$