Számelmélet

Legnagyobb közös osztó, Euklideszi algoritmus. Lineáris diofantoszi egyenletek. Számelméleti kongruenciák, kongruenciarendszerek. Euler-féle φ-függvény.

1. Oszthatóság

1. Definíció. Legyen $a, b \in \mathbb{Z}$. Az a **osztó**ja b-nek, ha létezik olyan $c \in \mathbb{Z}$ egész szám, melyre $ac = b$. Jelölése: $a \mid b$.

2. Példa. $3 \mid 12, \quad -2 \mid 6, \quad 1 \mid -132, \quad 7 \mid 0, \quad 0 \mid 0.$

3. *Megjegyzés.* Az oszthatóság nem egyezik meg az osztás fogalmával, mint látható a 0 osztható 0-val, de ettől még a nullával való osztás értelmetlen marad.

4. Tétel. *Tekintsük az $\mathbb{N}_0$ halmazon értelmezett oszthatósági relációt, vagyis az x és y nemnegatív számok pontosan akkor állnak relációban, ha $x \mid y$. Legyen $a, b, c, d \in \mathbb{N}_0$ tetszőleges.*

1. *Az oszthatósági reláció az $\mathbb{N}_0$ halmazon részbenrendezés, azaz reflexív, antiszimmetrikus és tranzitív.*
2. *Ha $a \mid b$ és $a \mid c$, akkor $a \mid bc$, $a \mid b + c$ és $a \mid b - c$.*
3. *Ha $ac \mid bc$ és $c \neq 0$, akkor $a \mid b$.*

5. *Megjegyzés.* Az előbbi tétel azt állítja, hogy $(\mathbb{N}_0; |)$ részbenrendezett halmaz. Ennek a részbenrendezett halmaznak a legnagyobb eleme a 0, mert minden nemnegatív egész szám osztója a 0-nak; illetve 1 a legkisebb elem, mert minden nemnegatív egész szám osztható 1-gyel. Ezen fogalmak a Diszkrét matematika I. kurzuson már előkerültek.

1.1. Prímszámok

6. Definíció. A $d \in \mathbb{Z}$ számot az $a, b \in \mathbb{Z}$ számok **legnagyobb közös osztó**jának nevezzük, ha $d \mid a$ és $d \mid b$, valamint bármely $\tilde{d} \in \mathbb{Z}$ esetén, ha $\tilde{d} \mid a$ és $\tilde{d} \mid b$, akkor $\tilde{d} \mid d$. Az a és b számok legnagyobb közös osztóját $\mathrm{lnko}(a, b)$-vel jelöljük.

7. Definíció. A $t \in \mathbb{Z}$ számot az $a, b \in \mathbb{Z}$ számok **legkisebb közös többszörös**ének nevezzük, ha $a \mid t$ és $b \mid t$, valamint bármely $\tilde{t} \in \mathbb{Z}$ esetén, ha $a \mid \tilde{t}$ és $b \mid \tilde{t}$, akkor $t \mid \tilde{t}$. Az a és b számok legkisebb közös többszörösét $\mathrm{lkkt}(a, b)$-vel jelöljük.

A prímszámok definíciója különbözni fog attól, amit középiskolában tanítanak. Felsőbb matematikában be kell vezetni az irreducibilis elemek fogalmát, mely különbözhet a prím elemek fogalmától.

8. Definíció. A $p \in \mathbb{N}_0$ számot **irreducibilis**nek nevezzük, ha $\mathbb{N}_0$-ban két osztója van: 1 és p.

9. Definíció. A $p \in \mathbb{N}_0$ számot **prím**számnak nevezzük, ha $p \mid ab$ esetén $p \mid a$ vagy $p \mid b$.

10. *Megjegyzés.* A nemnegatív számok halmazában az irreducibilis számok ugyanazok, mint a prímszámok, ezért fordulhat elő, hogy a prímszámokat szokták definiálni az osztók számával. Azonban a két fogalom nem fog mindig egybeesni, ezért szükség van a definíciók elkülönítésére. Például a páros számok körében a 6 irreducibilis, mert nem tudjuk előállítani két páros szám szorzataként, viszont nem prím, mert $6 \mid 18 \cdot 30$, hiszen $540 = 6 \cdot 90$, de $6 \nmid 18$ és $6 \nmid 30$ a páros számok körében.

Sok prímszámmal kapcsolatos kérdést sikerült már megválaszolni, azonban sok még csak sejtésként van jelen a matematikában. Ha valaki először találkozik prímszámokkal, akkor felmerülhet az a kérdése is, hogy egyáltalán hány darab prímszám van? A választ már Euler is tudta a kérdésre, és egy elég elegáns bizonyítást adott rá. A bizonyítás annyira rövid és ötletes, hogy itt is feltüntetjük.

11. Tétel (Euler tétele)**.** *Végtelen sok prímszám van.*

Bizonyítás. Tegyük fel, hogy véges sok prímszám van, ezek $p_1, p_2, \ldots, p_k$. Képezzük az $n = p_1 p_2 \ldots p_k + 1$ számot. Az n szám p_i-kkel vett osztási maradéka mindig 1, így n nem osztható egyik p_i-vel sem. Tehát n prím, vagy létezik egy p_i-ktől különböző prímosztója. Mindkét esetben ellentmondásra jutottunk, ugyanis találtunk egy p_i-ktől különböző prímet, viszont az elején feltettük, hogy $p_1, p_2, \ldots, p_k$ az összes prímszám. □

1.2. Maradékos osztás

12. Tétel. *Az egész számok körében mindig elvégezhető a maradékos osztás. Azaz bármely $a \in \mathbb{Z}$ és $b \in \mathbb{Z} \setminus \{0\}$ esetén létezik olyan $q, r \in \mathbb{Z}$, hogy $a = b \cdot q + r$, ahol $0 \leq r < |b|$. (A q-t nevezzük hányadosnak, míg az r-et maradéknak.)*

A következő tétel egy olyan algoritmust ad, mellyel gyorsan és könnyen kiszámítható két szám legnagyobb közös osztója.

13. Tétel (Euklideszi algoritmus)**.** *Legyen $a, b \in \mathbb{N}$, és tekintsük az alábbi maradékos osztásokat (mindig q_i jelenti a hányadost, r_i pedig a maradékot):*

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1 q_2 + r_2, \\ r_1 &= r_2 q_3 + r_3, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Ekkor r_n, azaz az utolsó nemnulla maradék lesz az a és b számok legnagyobb közös osztója.

14. *Megjegyzés.* Az euklideszi algoritmus során mindig az előző osztóból lesz az osztandó, illetve az előző maradék lesz az osztó.

15. *Megjegyzés.* Mivel $b > r_1 > r_2 > \dots$ véges lépésben végig ér (a maradék nemnegativitása miatt), eljutunk addig, míg az utolsó maradék 0 lesz. Ekkor állunk meg.

16. *Megjegyzés.* Az euklideszi algoritmus hatékony kiszámítási módját adja két szám legnagyobb közös osztójának meghatározásához, mely könnyen programozható.

17. Példa. Határozzuk meg 246 és a 132 legnagyobb közös osztóját.

$$\begin{aligned} 246 &= 132 \cdot 1 + 114 \\ 132 &= 114 \cdot 1 + 18 \\ 114 &= 18 \cdot 6 + 6 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

Mivel az utolsó nemnulla maradék 6, így $\operatorname{lnko}(246, 132) = 6$.

Az euklideszi algoritmus segítségével bizonyíthatóak a legnagyobb közös osztó alábbi tulajdonságai.

18. Tétel (A legnagyobb közös osztó tulajdonságai)**.**

1. *Bármely két egész számnak van legnagyobb közös osztója.*
2. *Ha $a, b \in \mathbb{Z}$, akkor van olyan $u, v \in \mathbb{Z}$, hogy* $\operatorname{lnko}(a, b) = ua + vb$.
3. *Ha $a, b, c \in \mathbb{Z}$, akkor* $\operatorname{lnko}(ca, cb) = |c| \operatorname{lnko}(a, b)$, *azaz a legnagyobb közös osztó képzésekor a közös tényező kiemelhető.*
4. *Ha $a, b \in \mathbb{Z}$ és legalább az egyik nem nulla, akkor*

$$\operatorname{lnko}\left(\frac{a}{\operatorname{lnko}(a, b)}, \frac{b}{\operatorname{lnko}(a, b)}\right) = 1.$$

Két szám legkisebb közös többszörösét is hatékonyan tudjuk számolni, ugyanis a meghatározása visszavezethető a legnagyobb közös osztó meghatározására, ahogy azt a következő tétel állítja.

19. Tétel. *Az egész számok között bármely két számnak van legkisebb közös többszöröse. Ha $a, b \in \mathbb{Z}$, akkor érvényes az* $\operatorname{lnko}(a, b) \cdot \operatorname{lkkt}(a, b) = |ab|$ *összefüggés.*

20. Példa. Határozzuk meg 246 és a 132 legkisebb közös többszörösét. A 17. Példa alapján tudjuk, hogy $\operatorname{lnko}(246, 132) = 6$. Így $\operatorname{lkkt}(246, 132) = \frac{246 \cdot 132}{6} = 5412$.

Felmerülhet a kérdés, hogy miért nem a középiskolában tanult módszerrel határozzuk meg a legnagyobb közös osztót, mely szerint a számok prímtényezős felbontását használjuk. A következő részben ez fog kiderülni, a rövid összefoglaló után.

1.3. Számelmélet alaptétele

21. Tétel (A számelmélet alaptétele)**.** *Minden pozitív egész szám felbontható prímszámok szorzatára. Ez a felbontás a tényezők sorrendjétől eltekintve egyértelmű.*

22. *Megjegyzés.* Az n szám prímtényezős felbontását $n = \sum_{i=1}^{k} p_i^{\alpha_i}$ alakban fogjuk felírni, ahol a p_i-k az n szám különböző prímosztói, az α_i kitevők pedig pozitív egész számok.

23. Tétel. *Legyen* $m = \prod_{i=1}^{k} p_i^{\alpha_i}$ *és* $n = \prod_{i=1}^{k} p_i^{\beta_i}$*, ahol* $p_1, \ldots, p_k$ *páronként különböző prímek, az* α_i *és* β_i *kitevők pedig nemnegatív egészek (fontos, hogy a kitevők nullák is lehetnek, ha az egyik szám prímosztói között nem szerepel a másik szám egyik prímosztója, de azért* 0 *kitevővel szereltetjük). Ekkor*

- $m \mid n \iff (\forall i \in \{1, \ldots, k\})(\alpha_i \leq \beta_i)$,
- $\mathrm{lnko}(m, n) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$,
- $\mathrm{lkkt}(m, n) = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$.

24. Példa. Határozzuk meg az $168 = 2^3 \cdot 3 \cdot 7$ és a $630 = 2 \cdot 3^2 \cdot 5 \cdot 7$ legnagyobb közös osztóját és legkisebb közös többszörösét.

$$\mathrm{lnko}(168, 630) = 2 \cdot 3 \cdot 7 = 42 \qquad \mathrm{lkkt}(168, 630) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$$

Mint látható, ha ismerjük két szám prímtényezős felbontását, akkor nagyon gyorsan meg tudjuk mondani a legnagyobb közös osztójukat. Azonban a problémát az jelenti, hogy hogyan határozzuk meg a számok prímtényezős felbontását. A jelenleg ismert algoritmusok erre a célra teljesen használhatatlanok egy több száz számjegyű szám esetén, és ezen múlik az adataink online biztonsága. Ezzel szemben az euklideszi algoritmus két több száz számjegyű számra is rendkívül gyorsan lefut.

2. Lineáris diofantoszi egyenletek

Gyakran előfordul, hogy egy egyenletnek csak az egész értékű megoldásai érdekelnek minket, főleg, ha az egyenlet valamilyen gyakorlati probléma modellezéséből keletkezett. Az ilyen egyenletek egyik legegyszerűbb formájával ismerkedünk meg ebben a fejezetben.

25. Definíció. Lineáris diofantoszi egyenleten egy

$$ax + by = c$$

egyenletet értünk, ahol $a, b, c \in \mathbb{Z}$, és az x, y ismeretleneket is az egész számok körében keressük.

26. Tétel. *A fenti diofantoszi egyenlet pontosan akkor oldható meg, ha* $\text{lnko}(a,b) \mid c$. *Ha az egyenlet megoldható és* (x_0, y_0) *egy ismert megoldása, akkor az egyenlet általános megoldása*

$$x = x_0 + \frac{b}{\text{lnko}(a,b)} \cdot t, \qquad y = y_0 - \frac{a}{\text{lnko}(a,b)} \cdot t \qquad (t \in \mathbb{Z}).$$

27. Példa. Adjuk meg a $12x + 18y = 186$ diofantoszi egyenlet általános megoldását.

I. Ellenőrizzük, hogy létezik-e megoldása, azaz ki kell számítani a 12 és 18 legnagyobb közös osztóját. Ezt az euklideszi algoritmussal célszerű megtenni, mert később az egész algoritmus számításait fel fogjuk használni. (Természetesen látszik, hogy $\text{lnko}(12,18) = 6$, de tegyük fel, hogy ezt nem tudjuk ránézésre meghatározni.) Tehát az euklideszi algoritmust végrehajtva:

$$\begin{aligned} 18 &= 12 \cdot 1 + 6, \\ 12 &= 6 \cdot 2 + 0. \end{aligned}$$

Mivel az utolsó nem nulla maradék 6, így $\text{lnko}(12,18) = 6$, és ezt osztja a 186-ot, tehát van megoldás.

II. Megkeressük az egyenlet egy partikuláris megoldását, azaz a tételben szereplő (x_0, y_0) számpárt. Erre használjuk az euklideszi algoritmus menetét $6 = 18 \cdot 1 - 12 \cdot 1$. Mivel a 6 osztja a 186-ot, így megszorozzuk az egyenlet mindkét oldalát azzal a számmal, hogy bal oldalon 186-ot kapjunk:

$$\begin{aligned} 6 &= 18 \cdot 1 - 12 \cdot 1, \\ (186 =) 6 \cdot 31 &= 18 \cdot 31 - 12 \cdot 31. \\ 186 &= 12 \cdot (-31) + 18 \cdot 31 \end{aligned}$$

Megkaptuk az egyenlet egy partikuláris megoldását: $(x_0, y_0) = (-31, 31)$.

III. A tételbeli képlet segítségével megkapjuk az általános megoldást:

$$x = -31 + 3t \quad \text{és} \quad y = 31 - 2t,$$

ahol $t \in \mathbb{Z}$ tetszőleges egész szám.

28. Példa. Adjuk meg a $97x + 35y = 13$ diofantoszi egyenlet általános megoldását.

I. Meghatározzuk a 97 és 35 legnagyobb közös osztóját.

$$\begin{aligned} 97 &= 35 \cdot 2 + 27, \\ 35 &= 27 \cdot 1 + 8, \\ 27 &= 8 \cdot 3 + 3, \\ 8 &= 3 \cdot 2 + 2, \\ 3 &= 2 \cdot 1 + 1, \\ 2 &= 1 \cdot 2 + 0, \end{aligned}$$

Mivel az utolsó nem nulla maradék 1, így $\text{lnko}(97,35) = 1$, és ezt osztja a 13-at, tehát van megoldás.

II. Megkeressük az egyenlet egy partikuláris megoldását, azaz a tételben szereplő egy (x_0, y_0) számpárt. Erre használjuk az euklideszi algoritmus végrehajtása során kapott adatokat. Kifejezzük a maradékokat, és egyesével visszahelyettesítjük azokat, a legnagyobb közös osztót kiadó egyenletbe.

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - (8 - 3 \cdot 2) \cdot 1 = 8 \cdot (-1) + 3 \cdot 3 \\ &= 8 \cdot (-1) + 3 \cdot 3 = 8 \cdot (-1) + (27 - 8 \cdot 3) \cdot 3 = 8 \cdot (-10) + 27 \cdot 3 \\ &= 8 \cdot (-10) + 27 \cdot 3 = (35 - 27) \cdot (-10) + 27 \cdot 3 = 35 \cdot (-10) + 27 \cdot 13 \\ &= 35 \cdot (-10) + 27 \cdot 13 = 35 \cdot (-10) + (97 - 35 \cdot 2) \cdot 13 = 35 \cdot (-36) + 97 \cdot 13 \end{aligned}$$

Tehát azt kaptuk, hogy $35 \cdot (-36) + 97 \cdot 13 = 1$. Nekünk az egyenlet jobb oldalán 13-nak kellene lennie, így mindkét oldalt megszorozzuk 13-mal, így azt kapjuk, hogy $35 \cdot (-36) \cdot 13 + 97 \cdot 13 \cdot 13 = 13$, azaz $35 \cdot (-468) + 97 \cdot 169 = 13$. Megkaptuk az egyenlet egy partikuláris megoldását: $(x_0, y_0) = (169, -468)$.

III. A tételbeli képlet segítségével megkapjuk az általános megoldást:

$$x = 169 + 35t \quad \text{és} \quad y = -468 - 97t,$$

ahol $t \in \mathbb{Z}$ tetszőleges egész szám.

3. Számelméleti kongruencia

29. Definíció. Legyen $a, b, m \in \mathbb{Z}$. Azt mondjuk, hogy „a **kongruens** b-vel modulo m”, ha $m \mid a - b$. Jelölésben: $a \equiv b \pmod{m}$.

30. *Megjegyzés.* Az $a \equiv b \pmod{m}$ kifejezés gyakorlatilag azt jelenti, hogy a és b ugyanazt a maradékot adják m-mel osztva.

31. Példa. $6 \equiv 4 \pmod{2}$, $22 \equiv -2 \pmod{8}$, $23 \equiv 8 \pmod{5}$.

32. Tétel. *Legyen $m \in \mathbb{N}_0$ egy rögzített modulus. Ekkor a*

$$\varrho = \{(a, b) \in \mathbb{Z}^2 : a \equiv b \pmod{m}\} \subseteq \mathbb{Z}^2$$

reláció ekvivalenciareláció a $\mathbb{Z}$ halmazon. (Tehát reflexív, szimmetrikus és tranzitív.)

33. Tétel. *Rögzített m modulus és tetszőleges a_1, b_1, a_2, b_2 egész számok esetén ha $a_1 \equiv a_2 \pmod{m}$ és $b_1 \equiv b_2 \pmod{m}$, akkor*

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m} \quad \text{és} \quad a_1 b_1 \equiv a_2 b_2 \pmod{m}.$$

34. Tétel. *Ha $ac \equiv bc \pmod{m}$ és $\text{lnko}(m, c) = 1$, akkor $a \equiv b \pmod{m}$.*

Az előző tétel élesíthető.

35. Tétel. *Ha* $ac \equiv bc \pmod{m}$, *akkor* $a \equiv b \pmod{\frac{m}{\text{lnko}(m,c)}}$.

36. Tétel (Kis Fermat-tétel)**.** *Ha* p *prímszám, és* $a \in \mathbb{Z}$ ***nem osztható*** p*-vel, akkor*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Az előző tételt a fontossága miatt a későbbiekben általánosítani fogjuk, de ahhoz új fogalmak bevezetésére van szükség.

4. Lineáris kongruencia

37. Definíció. Egy $ax \equiv b \pmod{m}$ alakú kongruenciát **lineáris kongruenciá**nak nevezünk, ha $a, b \in \mathbb{Z}$ és $m \in \mathbb{N}$ adott, és $x \in \mathbb{Z}$ ismeretlen.

Egy $ax \equiv b \pmod{m}$ alakú lineáris kongruencia megoldásának kérdése tulajdonképpen ekvivalens az $ax - my = b$ diofantoszi egyenlet megoldásainak kérdésével, természetesen az x-re vonatkozóan. Így a diofantoszi egyenletre vonatkozó tételek átfogalmazhatók lineáris kongruenciákra.

38. Tétel. *Az* $ax \equiv b \pmod{m}$ *kongruencia pontosan akkor oldható meg, ha* $\text{lnko}(a, m)$ *osztója* b*-nek. Ha van megoldása, akkor egy* x_0 *partikuláris megoldás ismeretében az általános megoldás* $x \equiv x_0 \pmod{\frac{m}{\text{lnko}(a,m)}}$.

39. Példa. Oldjuk meg a $21x \equiv 14 \pmod{35}$ lineáris kongruenciát.

Első megoldás. A feladat ekvivalens azzal, hogy oldjuk meg a $21x - 35y = 14$ diofantoszi egyenletet. Mivel $\text{lnko}(21, 35) = 7 \mid 14$, így az egyenlet megoldható. Az egyenlet általános megoldása (ami megkapható a 27. és 28. Példákban látott módon) $x = 4 + 5t$, $y = 2 + 3t$, ahol $t \in \mathbb{Z}$ tetszőleges egész szám. Nekünk csak az x ismeretlen értékére van szükségünk, így a kongruencia általános megoldása $x \equiv 4 \pmod{5}$.

Második megoldás. (Kátai-Urbán Kamilla megoldása.) Ha a lineáris kongruencia megoldható, akkor a kongruencia jobb oldalát addig növeljük (vagy csökkentjük) a modulus értékével, amíg osztható nem lesz az x együtthatójával: $21x \equiv 14 \equiv 14 + 2 \cdot 35 \pmod{35}$, azaz $21x \equiv 84 \pmod{35}$. A 35. Tétel alapján, ha 21-gyel osztunk, a következőt kapjuk: $x \equiv 4 \pmod{\frac{35}{\text{lnko}(35,21)}}$, tehát a lineáris kongruencia megoldása $x \equiv 4 \pmod{5}$.

40. Definíció. Lineáris kongruenciarendszernek nevezzük a

$$\begin{aligned} c_1 x &\equiv d_1 \pmod{n_1} \\ &\vdots \\ c_k x &\equiv d_k \pmod{n_k} \end{aligned} \tag{1}$$

alakú kongruenciarendszert, ha $2 \leq k \in \mathbb{N}$, $n_1, \ldots, n_k \in \mathbb{N}$, $c_1, \ldots, c_k, d_1, \ldots, d_k \in \mathbb{Z}$ adott számok, és az $x \in \mathbb{Z}$ ismeretlen.

41. *Megjegyzés.* A fenti (1) kongruenciarendszer megoldhatóságának szükséges feltétele, hogy a kongruenciák külön-külön megoldhatóak legyenek. Ha megoldhatóak, akkor a kongruenciarendszer

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{2}$$

alakúra hozható.

A kongruenciarendszerek megoldásának menete, hogy felírjuk a kongruenciarendszer (2) alakját, majd kettesével oldjuk meg a kongruenciákat, ahogy azt a következő tétel mutatja.

42. Tétel. *Az*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

kongruenciarendszer pontosan akkor oldható meg, ha $\text{lnko}(m_1, m_2) \mid a_1 - a_2$. *Amennyiben megoldható és* x_0 *egy rögzített megoldása, akkor a fenti kongruenciarendszer ekvivalens az alábbi kongruenciával:*

$$x \equiv x_0 \pmod{\text{lkkt}(m_1, m_2)},$$

és ezért az általános megoldása

$$x = x_0 + t \cdot \text{lkkt}(m_1, m_2), \qquad (t \in \mathbb{Z}).$$

43. Példa. (Kátai-Urbán Kamilla feladata és megoldásai.) Oldjuk meg a következő kongruenciarendszert:

$$\begin{aligned} 5x &\equiv 3 \pmod{6} \\ 4x &\equiv 6 \pmod{18}. \end{aligned}$$

Először külön-külön megoldjuk a lineáris kongruenciákat a 39. Példában látott módon, így kapjuk az

$$\begin{aligned} x &\equiv 3 \pmod{6} \\ x &\equiv 6 \pmod{9} \end{aligned}$$

kongruenciarendszert.

Első megoldás. Ha mindkét kongruencia jobb oldalából kivonjuk a megfelelő modulus értékét, mindkét esetben -3-at kapunk, így megkaptuk a kongruenciarendszer egy megoldását ($x_0 = -3$). A 42. Tétel alapján az általános megoldás: $x \equiv -3 \pmod{\text{lkkt}(6,9)}$, azaz $x \equiv 15 \pmod{18}$.

Másik megoldás. Az első kongruenciából kifejezve az x-et kapjuk, hogy $x = 6k + 3$, ahol $k \in \mathbb{Z}$. Ezt behelyettesítjük a második kongruenciába: $6k+3 \equiv 6 \pmod{9}$, majd megoldjuk a lineáris kongruenciát k-ra a 39. Példában látott módon. Így kapjuk, hogy $k \equiv 2 \pmod{3}$, ami azt jelenti, hogy $k = 3l + 2$, ahol $l \in \mathbb{Z}$, ezt visszahelyettesítve: $x = 6k + 3 = 6(3l + 2) + 3 = 18l + 15$. Tehát a kongruenciarendszer megoldása: $x \equiv 15 \pmod{18}$.

A következő tétel összefoglalja, hogy mikor oldható meg egy lineáris kongruenciarendszer. Ez a tétel egyébként a fentiek egyenes következménye.

44. Tétel. *A* (2) *kongruenciarendszer pontosan akkor oldható meg, ha bármely kételemű részrendszere megoldható, azaz bármely* $1 \leq i < j \leq k$ *esetén* $\text{lnko}(m_i, m_j) \mid a_i - a_j$

45. Tétel (Kínai maradéktétel)**.** *Ha a* (2) *kongruenciarendszerben az* $m_1, \ldots, m_k$ *modulusok páronként relatív prímek, akkor a* (2) *kongruenciarendszer mindig megoldható, és ha* x_0 *egy partikuláris megoldása, akkor a rendszer általános megoldása*

$$x = x_0 + t \cdot m_1 \ldots m_k.$$

5. Euler-féle φ-függvény

46. Definíció. Ha $n \in \mathbb{N}$, akkor $\varphi(n) = |\{x \in \mathbb{N} : x \leq n \text{ és } \text{lnko}(x, n) = 1\}|$. Tehát $\varphi(n)$ jelöli az n számnál nem nagyobb, hozzá relatív prím pozitív egész számok darabszámát. Ezt a függvényt **Euler-féle φ-függvény**nek nevezzük.

47. Példa. Például $\varphi(1) = 1$, $\varphi(6) = 2$ és ha p prím, akkor $\varphi(p) = p - 1$.

48. Tétel. *Ha az* $n \in \mathbb{N}$ *szám prímtényezős alakja*

$$n = \prod_{i=1}^{t} p_i^{k_i},$$

akkor

$$\varphi(n) = \prod_{i=1}^{t} \left(p_i^{k_i} - p_i^{k_i - 1}\right) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right).$$

49. Tétel. *Ha* $m, n \in \mathbb{N}$ *relatív prímek, akkor* $\varphi(mn) = \varphi(m)\varphi(n)$.

50. Példa. $\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\varphi(5^2) = (2^2 - 2^1)(5^2 - 5^1) = 2 \cdot 20 = 40$.

51. Tétel (Euler tétele)**.** *Ha* $m \in \mathbb{N}$ *és* $a \in \mathbb{Z}$ *relatív prímek, akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

52. Példa. Mi az utolsó két számjegye (a tízes számrendszerben) a

$$7^{160002}$$

számnak? Az igazi kérdés itt az, hogy mivel kongruens a 7^{160002} szám modulo 100? Tudjuk, hogy $\varphi(100) = 40$ (lásd az előző példában), illetve Euler tétele szerint $7^{40} \equiv 1 \pmod{100}$. Ebből következik, hogy

$$7^{160002} = 7^{4000 \cdot 40 + 2} = \left(7^{40}\right)^{4000} \cdot 7^2 \equiv 1^{4000} \cdot 49 \equiv 49 \pmod{100}.$$

(A kongruenciák végig modulo 100 értendők.)

2. feladatsor – Számelmélet

2.1. Feladat. Határozzuk meg euklideszi algoritmussal az alábbi a, b egész számok legnagyobb közös osztóját, és adjuk meg legkisebb közös többszörösüket.

(a) $a = 78$, $b = 30$;
(b) $a = 368$, $b = 161$;
(c) $a = 539$, $b = 1001$;
(d) $a = -1253$, $b = -3241$;
(e) $a = -1183$, $b = 1573$.

2.2. Feladat. Oldjuk meg az alábbi diofantoszi egyenleteket.

(a) $72x + 60y = 24$; (b) $78x + 30y = 12$; (c) $18x + 21y = 9$;
(d) $21x + 36y = 12$; (e) $21x - 15y = 12$; (f) $6x - 10y = 22$
(g) $237x + 571y = 13$; (h) $197x + 418y = 17$.

2.3. Feladat. Határozzuk meg a következő halmazok elemszámát.

(a) $\{x \in \mathbb{Z} : (\exists y \in \mathbb{Z})(11x - 8y = 3) \text{ és } 10 \leq x \leq 30\}$;
(b) $\{x \in \mathbb{Z} : (\exists y \in \mathbb{Z})(7x - 3y = 13) \text{ és } 10 \leq x \leq 30\}$;
(c) $\{y \in \mathbb{Z} : (\exists x \in \mathbb{Z})(7x - 19y = 10) \text{ és } 15 \leq y \leq 35)\}$;
(d) $\{y \in \mathbb{Z} : (\exists x \in \mathbb{Z})(13x - 20y = 7) \text{ és } 20 \leq y \leq 40)\}$.

2.4. Feladat. Kukutyinban 20 és 45 petákos érmék vannak forgalomban. Hogyan lehet ezekre felváltani 245 petákot. (Az összes megoldást adjuk meg.)

2.5. 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?

2.6. 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?

2.7. 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?

2.8. Feladat. Melyik az a legkisebb pozitív egész, amelynek pontosan 12 darab pozitív osztója van?

2.9. Feladat. Oldjuk meg az alábbi kongruenciákat.

(a) $6x \equiv 4 \pmod 8$; (b) $13x \equiv -3 \pmod{34}$; (c) $88x \equiv 42 \pmod{55}$;
(d) $5x \equiv 24 \pmod{13}$; (e) $9x \equiv 15 \pmod{12}$; (f) $29x \equiv 17 \pmod{73}$.

2.10. Feladat. Melyik az a 4-re végződő háromjegyű szám, amely 63-mal osztva 1-et ad maradékul?

2.11. Feladat. Határozza meg azt a legkisebb háromjegyű természetes számot, amelynek 12-szerese 6-ot ad maradékul 30-cal osztva.

2.12. Feladat.

(a) $\begin{aligned} x &\equiv 7 \pmod 8, \\ x &\equiv 6 \pmod 7; \end{aligned}$

(b) $\begin{aligned} x &\equiv 3 \pmod 5, \\ x &\equiv 4 \pmod 7; \end{aligned}$

(c) $\begin{aligned} x &\equiv 3 \pmod 2, \\ x &\equiv 6 \pmod 5; \end{aligned}$

(d) $\begin{aligned} 3x &\equiv 15 \pmod{24}, \\ 4x &\equiv 11 \pmod{21}; \end{aligned}$

(e) $\begin{aligned} 5x &\equiv 1 \pmod 6, \\ 7x &\equiv 9 \pmod{10}; \end{aligned}$

(f) $\begin{aligned} x &\equiv 3 \pmod 5, \\ x &\equiv 1 \pmod 6, \\ x &\equiv 7 \pmod 9; \end{aligned}$

(g) $\begin{aligned} 2x &\equiv 18 \pmod{10}, \\ 10x &\equiv 40 \pmod{12}, \\ 15x &\equiv 9 \pmod{21}; \end{aligned}$

(h) $\begin{aligned} 10x &\equiv 16 \pmod 9, \\ 6x &\equiv 3 \pmod{21}, \\ 3x &\equiv 2 \pmod 5; \end{aligned}$

(i) $\begin{aligned} 3x &\equiv 1 \pmod 5, \\ 5x &\equiv 3 \pmod 7, \\ 13x &\equiv 4 \pmod 9; \end{aligned}$

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

2.13. Feladat. Egy labdarúgó mérkőzésre azonos számú férőhellyel rendelkező buszokkal érkeznek a szurkolók, akiket biztonsági okokból kisebb csoportokban engednek be a stadionba. Ha a szurkolók 4 busszal érkeznek, és 5 fős csoportokban engedik be őket, akkor az utolsó csoportban csak 3 szurkoló marad. Ha 13 busszal érkeznek, és 8-as csoportokban nyernek bebocsátást, akkor szintén 3 szurkoló lesz az utoljára beengedett csoportban. Míg ha 16 busszal érkeznek szurkolók, és egyszerre 9-et léptetnek be, akkor végül 5 szurkoló marad. Hány személyesek a buszok, ha tudjuk, hogy egy buszba legfeljebb 100-an férnek, és a buszok minden esetben tele voltak?

2.14. 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?

2.15. Feladat. A mai napon (2013. január 18-án) péntek van. Milyen nap lesz 7770016^{6664} nap múlva?

2.16. Feladat. Számoljuk ki az Euler-féle φ függvény következő értékeit.

(a) $\varphi(20)$; (b) $\varphi(75)$; (c) $\varphi(88)$; (d) $\varphi(128)$; (e) $\varphi(360)$.

2.17. Feladat. Oldjuk meg a következő egyenleteket a természetes számok halmazán.

(a) $2\varphi(x) = x$; (b) $3\varphi(x) = x$; (c) $\varphi(x) = x - 8$;
(d) $\varphi(x) = x - 10$; (e) $\varphi(x^2) = 2x$; (f) $\varphi(x^2) = x\varphi(x)$.

2.18. Feladat. Határozzuk meg, hogy az a szám milyen maradékot ad n-nel osztva.

(a) $a = 3^{65},\ n = 128$; (b) $a = 19^{81},\ n = 75$; (c) $a = 63^{42},\ n = 50$;
(d) $a = 42^{62},\ n = 25$; (e) $a = 13^{321^{50}},\ n = 87$; (f) $a = 91^{441^{222}},\ n = 88$.

2.19. Feladat. A mai napon (2013. január 21-én) hétfő van. Milyen nap lesz $712^{185^{937}}$ nap múlva?

2.20. Feladat. Bizonyítsuk be, hogy ha n páratlan természetes szám, akkor

$$n \mid 2^{(n-1)!} - 1.$$

2. feladatsor – Számelmélet
MEGOLDÁSOK

2.1. Feladat. .

(a) 6, 390;
(b) 23, 2576;
(c) 77, 7007;
(d) 7, $1253 \cdot 463 = 580139$;
(e) 13, $91 \cdot 1573 = 143143$.

2.2. Feladat. .

(a) $x = 2 + 5t,\ y = -2 - 6t\ (t \in \mathbb{Z})$;
(b) $x = -1 + 5t,\ y = 3 - 13t\ (t \in \mathbb{Z})$;
(c) $x = -3 + 7t,\ y = 3 - 6t\ (t \in \mathbb{Z})$;
(d) $x = 4 + 12t,\ y = -2 - 7t\ (t \in \mathbb{Z})$;
(e) $x = 2 - 5t,\ y = 2 - 7t\ (t \in \mathbb{Z})$;
(f) $x = 22 + 5t,\ y = 11 + 3t\ (t \in \mathbb{Z})$;
(g) $x = -689 + 571t,\ y = 286 + 237t\ (t \in \mathbb{Z})$;
(h) $x = 1479 + 481t,\ y = -679 - 197t\ (t \in \mathbb{Z})$.

2.3. Feladat.

(a) 2; (b) 7; (c) 3; (d) 2.

2.4. Feladat. 10, 1, valamint 1, 5.

2.5. Feladat. 6, 10, 6.

2.6. Feladat. 7, 5, 10.

2.7. Feladat. 1, 1, 5.

2.8. Feladat. 60.

2.9. Feladat. .

(a) $x \equiv 2 \pmod 8$, $x \equiv 6 \pmod 8$;
(b) $x \equiv 5 \pmod{34}$;
(c) nincs megoldás;
(d) $x \equiv 10 \pmod{13}$;
(e) $x \equiv 3 \pmod{12}$, $x \equiv 7 \pmod{12}$, $x \equiv 11 \pmod{12}$;
(f) $x \equiv 61 \pmod{73}$.

2.10. Feladat. 694.

2.11. Feladat. 103.

2.12. Feladat. .

(a) $x \equiv -1 \pmod{56}$;
(b) $x \equiv 18 \pmod{35}$;
(c) $x \equiv 1 \pmod{10}$;
(d) $x \equiv 29 \pmod{168}$;
(e) $x \equiv 17 \pmod{30}$;
(f) $x \equiv 43 \pmod{90}$;

(g) $x \equiv 184 \pmod{210}$;
(h) $x \equiv 214 \pmod{315}$;
(i) $x \equiv 37 \pmod{315}$;
(j) nincs megoldás.

2.13. Feladat. 47.

2.14. Feladat. 31.

2.15. Feladat. vasárnap

2.16. Feladat.

(a) 8; (b) 40; (c) 40; (d) 64; (e) 96.

2.17. Feladat. .

(a) $x = 2^l (l \in \mathbb{N})$;
(b) $x = 2^l 3^k (k, l \in \mathbb{N})$;
(c) $x \in \{12, 14, 16\}$;
(d) nincs megoldás;
(e) $x \in \{3, 6, 4\}$;
(f) tetszőleges $x \in \mathbb{N}$.

2.18. Feladat.

(a) 3; (b) 19; (c) 19; (d) 14; (e) 13; (f) 3.

2.19. Feladat. csütörtök

2.20. Feladat. H.F.