LÁNG CSABÁNÉ

SZÁMELMÉLET

Példák és feladatok

ELTE IK Budapest
2010-10-24
2. javított kiadás

Felsőoktatási tankönyv

Lektorálták:
Kátai Imre
Bui Minh Phong
Burcsi Péter
Farkas Gábor
Fülöp Ágnes
Germán László
Kovács Attila
Kovácsvölgyi István

ISBN 963 463 791 4

Tartalomjegyzék

1. Bevezetés

Akiknek ez a könyv készült

Elsősorban az ELTE Informatikai Kar informatikus, programtervező matematikus, programozó és informatika tanár szakos hallgatói számára készült ez a példatár.

Ajánlom azonban másoknak is, akik a számelmélet alapjaiban jártasságot szeretnének szerezni. Ezt megkönnyítheti az, hogy valamennyi példa részletesen ki van dolgozva.

A könyv szerkezete

A 2. fejezet alfejezeteinek elején azok a tudnivalók – definíciók, tételek – szerepelnek röviden összefoglalva, amelyekre a példák megoldása közben szükség lehet. A számelmélet alapjainak részletes felépítése megtalálható többek között a szerző *Bevezető fejezetek a matematikába I.* című könyvében, illetve az *Ajánlott irodalomban* felsorolt könyvek egy részében.

A teljes anyag lényegében két részre tagolódik. Az *Elméleti összefoglalók, példák* fejezetben minden egyes példa után következik a részletes megoldás. Úgy gondolom, hogy e fejezet anyagát végigkövetve kialakulhat egy átfogó kép a számelmélet alapvető fogalmairól. Ha valaki ezeket az ismereteit mélyíteni kívánja, akkor a *Feladatok* fejezet példáihoz nyúlhat. Ezeknek a megoldásai a *Megoldás* fejezetben találhatók.

Technikai tudnivalók

A képletek számozása az elméleti összefoglalókban római számokkal történik, a különböző fejezetekben egymástól függetlenül. A példák és feladatok képletei arab sorszámot kaptak, minden példában és feladatban újra kezdődik a sorszámozás.

Jelölések, felhasznált egyéb fogalmak

$\mathbb{N}$ a természetes számok (pozitív egész számok) halmaza, $\mathbb{N} = \{1, 2, 3...\}$.
$\mathbb{Z}$ az egész számok halmaza.
$\mathbb{Q}$ a racionális számok halmaza.
$\mathbb{R}$ a valós számok halmaza.

Valamely $\alpha \in \mathbb{R}$ szám *egész része*, $[\alpha]$ az az egyértelműen meghatározott egész szám, amelyre $[\alpha] \leq \alpha < [\alpha] + 1$, *tört része* az $\{\alpha\} = \alpha - [\alpha]$ érték. Nyilván $0 \leq \{\alpha\} < 1$.

Valamely $a \in \mathbb{R}$ szám *abszolút értékét* $|a|$ jelöli. $|a| = a$, ha $a \geq 0$, egyébként $|a| = -a$.

Binomiális tétel.

Legyen n természetes szám, x, y pedig egész számok. Ekkor

$$(x+y)^n = \binom{n}{0} y^n + \binom{n}{1} xy^{n-1} + \ldots + \binom{n}{k} x^k y^{n-k} + \ldots + \binom{n}{n} x^n.$$

Fibonacci-számok.

A következő szabállyal megadott sorozat elemeit *Fibonacci-számoknak* nevezzük.

$$F_1 = 1; \quad F_2 = 1; \quad F_n = F_{n-1} + F_{n-2}$$

Az első néhány szám: $1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ \ldots$

A Fibonacci-sorozat n-edik tagja:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) \quad n = 1, 2, 3, \ldots$$

Köszönetnyilvánítás

A példák részben más könyvekből, példatárakból, mások által összeállított feladatsorokból származnak. Azok a források, amelyekről tudomásom van, szerepelnek az *Ajánlott irodalom* fejezetben. A feladatok más része pedig ebben a példatárban jelenik meg először.

Köszönöm a lektorok segítségét, akik aprólékos munkával igyekeztek kiszűrni a hibákat. Tanácsaikat igyekeztem messzemenően figyelembe venni.

A könyvben található hibákra, hiányosságokra vonatkozó észrevételeket köszönettel fogadom.

Budapest, 2005. július

Láng Csabáné
zslang@compalg.inf.elte.hu
ELTE Informatikai Kar Komputer Algebra Tanszék
1117 Budapest, Pázmány Péter sétány I/C.

2. Elméleti összefoglalók, példák

2.1. Oszthatóság

Legyenek a, b egész számok. Azt mondjuk, hogy a *osztója* b-nek, ha létezik olyan c egész szám, melyre $a \cdot c = b$ teljesül. Ezt $a|b$-vel jelöljük. Ha ilyen c szám nincs, akkor a *nem osztója* b-nek ($a \nmid b$).

Például $2|10$, mert $2 \cdot 5 = 10$, de $4 \nmid 6$.

Ez a definíció többet mond annál, mint hogy $\frac{b}{a}$ egész szám, hiszen az $a = 0$ esetet is megengedi.

Az oszthatóság néhány alapvető tulajdonsága

1. $a|0$ minden $a \in \mathbb{Z}$ esetén; ha $0|b$, akkor $b = 0$; $a|a$ minden $a \in \mathbb{Z}$ esetén.
2. Ha $a|b$ és $b|c$, akkor $a|c$.
3. $1|a$ és $-1|a$ minden $a \in \mathbb{Z}$-re.
4. Ha $a|b$ és $b|a$, akkor $|a| = |b|$.
5. *Lineáris kombinációs tulajdonság.* Ha $a|b$ és $a|c$, akkor $a|bx + cy$ minden $x, y \in \mathbb{Z}$ esetén.
6. $a|b$ akkor és csak akkor teljesül, ha $|a|\big||b|$.
7. Ha $a|b$ és $c|d$, akkor $ac|bd$.

Egy egész számot *egységnek* nevezünk, ha minden egész számnak osztója. Azok a számok az egységek, amelyek az 1-nek osztói. $\mathbb{Z}$ egységei a $+1$ és a -1.

Ha $a|b$ és $b \neq 0$, akkor $|a| \leq |b|$. Egy nem nulla b egész számnak véges sok osztója van. A $-|b|,\ -1,\ 1,\ |b|$ mindig osztói b-nek. Ezek *triviális osztók.*

Valamely a egész szám ***többszöröse*** a k egész, ha $a|k$. Az a, b egészek ***közös osztója*** a d egész, ha $d|a$ és $d|b$, ***közös többszörösük*** a k egész, ha $a|k$ és $b|k$.

A legnagyobb közös osztó számára kézenfekvő definíció a következő: a közös osztók közül a legnagyobb.

Ezzel a meghatározással az a gond, hogy nem oszthatósági, hanem rendezési tulajdonságával adja meg a legnagyobb közös osztót, s ebből nem látszik, hogy milyen oszthatósági kapcsolatban van a többi közös osztóval. Másrészt, előfordulnak olyan számkörök, amelyekben értelmezhető az oszthatóság, de olyan teljes rendezés nem adható rajtuk, amely a műveletekkel összhangban lenne, s így ezt a definíciót ott nem alkalmazhatnánk. Ezért a következő, más struktúrákra is kiterjeszthető meghatározást adjuk. (Belátható, hogy ez a meghatározás az egész számok körében lényegében egybeesik az előzővel.)

Az a, b egész számok *legnagyobb közös osztója* a d egész, ha
1. d közös osztó, és
2. d minden közös osztónak többszöröse.

0 és 0 legnagyobb közös osztója 0. Például 24 és 36 legnagyobb közös osztója a 12 és a -12 is. Ez a két szám azonban egymás egységszerese, más szóval egymás *asszociáltja.* Az asszociáltak kölcsönösen osztói egymásnak.

Bármely két számnak van legnagyobb közös osztója, amire biztosíték az *euklideszi algoritmus* (lásd a 2.4. fejezetet.) A legnagyobb közös osztó asszociáltság erejéig egyértelmű, ami azt jelenti, hogy ha a és b legnagyobb közös osztója d, akkor $-d$ is legnagyobb közös osztójuk, más szám pedig nem legnagyobb közös osztója ennek a két számnak.

(a, b)-vel, illetve $\mathrm{lnko}(a, b)$-vel a legnagyobb közös osztók nem negatív reprezentánsát jelöljük. Tehát például $(0,0) = 0$, $(24,36) = 12$, $(-24,36) = 12$ és $(-24,-36) = 12$.

Az $a_1,\ a_2,\ \ldots,\ a_n \in \mathbb{Z}$ számok *legnagyobb közös osztója* $d \in \mathbb{Z}$, ha d közös osztó és minden közös osztónak többszöröse. Ilyen d létezik és asszociáltság erejéig egyértelmű, s a nem negatív értékűt jelöljük $(a_1, a_2, \ldots, a_n)$-nel. Mivel két szám közös osztóinak halmaza megegyezik legnagyobb közös osztójuk osztóinak halmazával, ezért:

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n) = \ldots = ((((a_1, a_2), a_3), \ldots, a_{n-1}), a_n)$$

Ebből az átalakításból nemcsak az olvasható le, hogy minden esetben van az $a_1,\ a_2,\ \ldots,\ a_n$ számoknak legnagyobb közös osztója, hanem módszert is kapunk a megkeresésére. Először ugyanis megkeressük két szám legnagyobb közös osztóját, ehhez hozzávéve egy következőt újra megkeressük a legnagyobb közös osztót, és így tovább.

Az $a_1,\ a_2,\ \ldots,\ a_n$ egész számok *relatív prímek,* ha $(a_1,\ a_2,\ \ldots,\ a_n) = 1$. Az $a_1,\ a_2,\ \ldots,\ a_n$ egész számok *páronként relatív prímek*, ha $(a_i, a_j) = 1$ minden $i \neq j$ esetén. Ha n szám páronként relatív prím, akkor nyilván relatív prím is. Fordítva azonban nem feltétlenül igaz. Tekintsük a $6, 10, 15$ számokat. Jóllehet relatív prímek, páronként nem relatív prímek.

A k egész szám az $a_1,\ a_2,\ \ldots,\ a_n$ egész számok *közös többszöröse*, ha $a_i|k$ minden $i = 1,\ 2,\ \ldots,\ n$ esetén. A k egész szám az $a_1,\ a_2,\ \ldots,\ a_n$ egész számok *legkisebb közös többszöröse*, ha

1. k mindegyik számnak többszöröse, és
2. k a számok mindegyik többszörösének osztója.

Példa. 12 és 18 legkisebb közös többszöröse 36 és -36.

Ha a számok egyike 0, akkor a legkisebb közös többszörösük is az. Két szám legkisebb közös többszöröse asszociáltság erejéig egyértelmű. a és b legkisebb közös többszörösei közül a nem negatívat $[a, b]$-vel, illetve $\mathrm{lkkt}(a, b)$-vel jelöljük. Tetszőleges két egész számnak van asszociáltság erejéig egyértelműen meghatározott legkisebb közös többszöröse.

Az f 0-tól és ± 1-től különböző egész számot *felbonthatatlannak* nevezzük, ha $f = ab\ \ (a, b \in \mathbb{Z})$ esetén a vagy b egység. Egy felbonthatatlan szám osztói csak a ± 1, illetve $\pm f$ lehetnek. Ilyen számok például a $\pm 2, \pm 3, \pm 5$ stb. Törzsszámoknak is nevezik őket ama tulajdonságukra utalva, hogy a többi szám ezekből a számokból lényegében egyértelműen felépíthető. A lényegében egyértelmű jelző azt jelenti, hogy a tényezők sorrendjétől, illetve egységszorzótól eltekintve egyértelmű. Nézzük például a 12 szám néhány előállítását:

$$12 = 2 \cdot 2 \cdot 3 = (-2)3 \cdot (-2) = (-3)(-2)2 = \ldots$$

E számoknak egy másik lényeges tulajdonsága, az úgynevezett prímtulajdonság is szerepet játszik abban, hogy minden egész szám lényegében egyértelműen felépíthető belőlük. A p 0-tól és ± 1-től különböző egész szám *prímszám,* ha $p|ab\ \ (a, b \in \mathbb{Z})$ esetén $p|a$ vagy $p|b$ teljesül.

Példa. $19, 23$ felbonthatatlan számok, és egyúttal prímszámok is. 6 nem prímszám, mert van olyan eset, hogy 6 osztója egy szorzatnak, de egyik tényezőnek sem osztója. Például $6|6 = 2 \cdot 3$ de $6 \nmid 2$ és $6 \nmid 3$.

Az egész számok körében ez a két tulajdonság, a felbonthatatlanság és a prímtulajdonság egybeesik. Ez azonban nem minden számkörben van így. Például a páros számok halmazában is értelmezhető az oszthatóság, itt vannak felbonthatatlanok, prímek azonban nincsenek, sőt egység sincs. A páros számokról nem mondhatjuk el, hogy egyértelműen felbonthatók lennének felbonthatatlanok szorzatára.

A számelmélet alaptétele (Az egyértelmű felbontás tétele)

Bármely nullától és ± 1-től különböző egész szám felbontható véges sok felbonthatatlan egész szorzatára, és ez a felbontás lényegében egyértelmű. •

A szorzatra bontásnál egytényezős szorzat is szóba jöhet. A lényegében egyértelmű felbontáson azt értjük, hogy egy n egész szám bármely két felbonthatatlanok szorzatára való felbontását tekintve a tényezők kölcsönösen egyértelműen összepárosíthatók úgy, hogy az egymásnak megfelelő tényezők egymás egységszeresei legyenek.

Az egyértelmű felbontás tétele alapján a természetes számok következő előállítása egyértelmű.

Az $n \neq 1$ természetes szám *kanonikus alakja*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

ahol $p_1, p_2, \dots, p_k$ különböző pozitív prímek, és mindegyik $\alpha_i > 0$ egész szám.

Az n szám *módosított kanonikus alakjához* jutunk, ha a fenti előállításban az $\alpha_i = 0$ esetet is megengedjük (ez utóbbi alak nem egyértelmű).

Példa. A 140 szám kanonikus alakja $140 = 2^2 \cdot 5 \cdot 7$, módosított kanonikus alakja többek között a $140 = 2^2 \cdot 5 \cdot 7 \cdot 13^0$.

Az $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ kanonikus alakkal rendelkező természetes számnak a d természetes szám akkor és csak akkor osztója, ha $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, ahol $0 \le \beta_i \le \alpha_i \quad (i = 1, \dots, k)$.

A legnagyobb közös osztó és a legkisebb közös többszörös meghatározása

Két természetes szám legnagyobb közös osztója és legkisebb közös többszöröse meghatározható a számok kanonikus alakjának segítségével. Legyen

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \quad \alpha_i \ge 0 \quad (i = 1, \dots, r)$$

és

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \quad \beta_j \ge 0 \quad (i = 1, \dots, r)$$

az a és b természetes számok módosított kanonikus alakja. Ekkor

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \dots p_r^{\min(\alpha_r, \beta_r)},$$

valamint

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_r^{\max(\alpha_r, \beta_r)}.$$

Legyen például $a = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7$ és $b = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^0$. Ekkor $(a,b) = 2^2$, $[a,b] = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7$.

Ez az eljárás azonban nem hatékony, különösen nagy számok esetén. Mindmáig a legjobban használható algoritmus a több mint 2000 éves euklideszi algoritmus. (Lásd a 2.4. fejezetet.)

Ha az euklideszi algoritmussal meghatározzuk a legnagyobb közös osztót, akkor az

$$\text{lnko}(a,b) \cdot \text{lkkt}(a,b) = a \cdot b$$

összefüggés alapján a legkisebb közös többszörös könnyen kiszámítható.

Még néhány oszthatósággal kapcsolatos összefüggés

8. $a, b \in \mathbb{Z},\ c \in \mathbb{N}$ esetén $(ac, bc) = (a,b)c$.
9. Ha $a, b, c \in \mathbb{Z},\ \ a|bc$ és $(a,b) = 1$, akkor $a|c$.
10. Ha $a, b, c \in \mathbb{N},\ a|c,\ b|c$ és $(a,b) = 1$, akkor $ab|c$.
11. Legyen $a, b \in \mathbb{N},\ (a,b) = 1$. Ekkor ab tetszőleges d osztója egyértelműen állítható elő a következő alakban: $d = a_1 b_1$, ahol $a_1|a$ és $b_1|b$. Fordítva, ha $a_2|a$ és $b_2|b$, akkor $a_2 b_2|ab$.
12. $a|c, b|c \Leftrightarrow [a,b]|c$.
13. $a - b|a^n - b^n$, mert $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$.
14. $a + b|a^{2n} - b^{2n}$, mert $a^{2n} - b^{2n} = (a^n)^2 - (b^n)^2$.
15. $(a+b)|a^{2k+1} + b^{2k+1}$, mert
$a^{2k+1} + b^{2k+1} = (a+b)(a^{2k} - a^{2k-1}b + \ldots - ab^{2k-1} + b^{2k})$.

Példák

2.1-1. Állapítsuk meg, milyen maradékot adnak a természetes számok négyzetei 3-mal és 5-tel osztva.
Megoldás.

n	n^2	a maradék
$n = 3k$	$n^2 = 9k^2$	0
$n = 3k \pm 1$	$n^2 = 9k^2 \pm 6k + 1$	1

n	n^2	a maradék
$n = 5k$	$n^2 = 25k^2$	0
$n = 5k \pm 1$	$n^2 = 25k^2 \pm 10k + 1$	1
$n = 5k \pm 2$	$n^2 = 25k^2 \pm 20k + 4$	-1

Ha négyzetszámot 3-mal osztunk, 0 vagy 1 a maradék. Ha négyzetszámot 5-tel osztunk, 0, 1 vagy -1 a maradék. ■

2.1-2. Igaz-e, hogy minden 3-nál nagyobb p prímnek van 6-tal osztható szomszédja?
Megoldás.

Igaz. Mivel $2 \nmid p$ és $3 \nmid p$, ezért egyrészt $2|p-1$ és $2|p+1$, másrészt $3|p-1$ vagy $3|p+1$. $p-1$ és $p+1$ közül az egyiknek 2 és 3 is osztója, így osztója a 6 is. ■

2.1-3. Bizonyítsuk be, hogy $n^5 - 5n^3 + 4n$ osztható 120-szal. (n tetszőleges egész szám.)
Megoldás.

Nézzük a következő átalakításokat: $120 = 2^3 \cdot 3 \cdot 5$,

$$n^5-5n^3+4n = n(n^4-4n^2-n^2+4) = n(n^2(n^2-4)-(n^2-4)) = n(n^2-4)(n^2-1) =$$
$$= n(n-2)(n+2)(n-1)(n+1) = (n-2)(n-1)n(n+1)(n+2)$$

Öt egymás utáni szám között biztosan van egy 3-mal és egy 5-tel osztható, valamint van közöttük két páros, melyek egyike 4-gyel is osztható. Mivel 3, 5 és 8 páronként relatív prímek, a szorzat osztható 3, 5 és 8 szorzatával, vagyis 120-szal. ■

2.1-4. Bizonyítsuk be, hogy $665|3^{6n} - 2^{6n}$.
Megoldás.

1. *megoldás:*

$$3^{6n} - 2^{6n} = (3^6)^n - (2^6)^n$$
$$3^6 - 2^6 = 729 - 64 = 665$$
$$665|(3^6)^n - (2^6)^n,$$

mert

$$a-b|a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}).$$

2. *megoldás:*

$$3^{6n} - 2^{6n} = (3^3)^{2n} - (2^3)^{2n} = 27^{2n} - 8^{2n}$$

$$27+8 = 35|27^{2n}-8^{2n},$$

mert

$$a+b|a^{2n}-b^{2n} = (a^n)^2-(b^n)^2,$$

és

$$27-8 = 19|27^{2n}-8^{2n},$$

mert

$$a-b|a^k-b^k = (a-b)(a^{k-1}+a^{k-2}b+\ldots+b^{k-1}).$$

35 és 19 relatív prímek, így a szorzatuk, 665 is osztója a kifejezésnek.

3. *megoldás:* Teljes indukcióval bizonyítunk. $n=1$ esetén 665 osztója a kifejezésnek, mert $3^6-2^6=665$. Legyen $n\geq 1$, és tegyük fel, hogy n-re igaz az állítás. Belátjuk, hogy ekkor $n+1$-re is igaz.

$$3^{6(n+1)}-2^{6(n+1)}=3^6\cdot 3^{6n}-2^6\cdot 2^{6n}=729\cdot 3^{6n}-64\cdot 2^{6n}=$$

$$=64(3^{6n}-2^{6n})+665\cdot 3^{6n}$$

$64(3^{6n}-2^{6n})$-nek osztója 665 az indukciós feltevés szerint, $665\cdot 3^{6n}$-nek szintén osztója, így a teljes kifejezés osztható 665-tel. ∎

2.1-5. Bizonyítsuk be, hogy öt egymást követő egész szám négyzetének az összege nem négyzetszám.
Megoldás.

$$(n-2)^2+(n-1)^2+n^2+(n+1)^2+(n+2)^2=5n^2+10=5(n^2+2) \quad (1)$$

n^2 5-tel való osztási maradéka 0, 1, -1 lehet (lásd az 1. példát), emiatt n^2+2 5-tel való osztási maradéka 2, 3, illetve 1 lehet, tehát n^2+2 nem osztható 5-tel. Az (1) kifejezésben 5 páratlan kitevőjű hatványa fordul elő, s így nem négyzetszám. ∎

2.1-6. Bizonyítsuk be, hogy $a^{2^n+1}-a$ tízes számrendszerben felírva mindig 0-ra végződik, ha $n\geq 2$.

Megoldás.

Legyen $A = a^{2^n+1} - a$. Azt kell megmutatnunk, hogy 2 és 5 osztói A-nak, amiből már következik, hogy (mivel 2 és 5 relatív prímek) a szorzatuk, 10 is osztója A-nak. Alakítsuk ezt a kifejezést, miközben felhasználjuk azt, hogy $a^{2^n} = (a^{2^{n-1}})^2$, valamint $a^{2^{n-1}} = (a^{2^{n-2}})^2$.

$$a^{2^n+1} - a = a(a^{2^n} - 1) = \tag{1}$$

$$= a(a^{2^{n-1}} - 1) \cdot (a^{2^{n-1}} + 1) = a((a^{2^{n-2}})^2 - 1) \cdot ((a^{2^{n-2}})^2 + 1) \tag{2}$$

Az (1) alakból látszik, hogy $2|A$, hiszen vagy a vagy a másik tényező páros. $5|A$ is teljesül az alábbiak miatt. Vagy $5|a$, vagy pedig $5 \nmid a$, s ekkor $(a^{2^{n-2}})^2$ osztási maradéka 1 vagy -1 lehet, tehát (2) egyik tényezője osztható 5-tel. ∎

2.1-7. Bizonyítsuk be, hogy ha egy (tízes számrendszerben felírt) ötjegyű szám osztható 41-gyel, akkor a számjegyek ciklikus permutálásával nyert ötjegyű szám is osztható 41-gyel.

Megoldás.

Jelöljük az ötjegyű számot A-val.

$$A = a_0 + 10a_1 + 100a_2 + 1000a_3 + 10\,000a_4$$

Az A-ból ciklikus permutálással nyert szám

$$A1 = a_4 + 10a_0 + 100a_1 + 1000a_2 + 10\,000a_3.$$

Ebből látható, hogy

$$A1 = 10A - 100\,000a_4 + a_4 = 10A - 99\,999a_4. \tag{1}$$

Tudjuk, hogy A osztható 41-gyel, $99\,999 = 41 \cdot 2439$, s így (1) mindkét tagja osztható 41-gyel, tehát $A1$ is osztható vele. ∎

2.1-8. Bizonyítsuk be, hogy 30 osztója az $mn(m^4 - n^4)$ számnak, bármilyen m, n egész szám esetén.

Megoldás.

$$mn(m^4 - n^4) = mn(m^2 - n^2)(m^2 + n^2), \tag{1}$$

valamint $30 = 2 \cdot 3 \cdot 5$. Ha belátjuk, hogy $2, 3, 5$ osztói (1)-nek, akkor 30 is osztója, mert $2, 3, 5$ páronként relatív prímek.

$$2|mn \text{ vagy } 2|m^2 - n^2,$$

mert ha $2 \nmid m \cdot n$, m és n páratlan, de akkor m^2 és n^2 is az, így $2|m^2 - n^2$.

$$3|mn \text{ vagy } 3|m^2 - n^2,$$

mert ha $3 \nmid m \cdot n$, m és n nem osztható 3-mal, de akkor m^2 és n^2 1-et ad maradékul, tehát $3|m^2 - n^2$.

$$5|mn \text{ vagy } 5|m^2 - n^2 \text{ vagy } 5|m^2 + n^2$$

Ha ugyanis $5 \nmid mn$, akkor m^2 és n^2 5-tel osztva 1-et vagy -1-et ad maradékul. Ha mindkettő 1-et ad, akkor $5|m^2-n^2$, ha mindkettő -1-et ad, akkor ugyanez a helyzet. Ha pedig az egyik 1-et ad, a másik -1-et ad maradékul, akkor $5|m^2 + n^2$. (Lásd az 1. példát.)

■

2.1-9. Bizonyítsuk be, hogy ha a tetszőleges egész szám, akkor az

$$\frac{a^3 + 2a}{a^4 + 3a^2 + 1}$$

tört nem egyszerűsíthető.
Megoldás.

$$\frac{a^3 + 2a}{a^4 + 3a^2 + 1} = \frac{a(a^2 + 2)}{a^2(a^2 + 2) + a^2 + 1}$$

Ha valamilyen p prím osztója a számlálónak, akkor vagy a-nak, vagy a^2+2-nek osztója. Vizsgáljuk meg azt az esetet, amikor p osztója a-nak. Ekkor a nevező első és második tagjának is osztója, s így osztója a harmadik tagnak, 1-nek. Ez azonban ellentmondás, tehát a semelyik prímosztójával (ha egyáltalán van) nem egyszerűsíthető a tört.

Nézzük most azt az esetet, amikor valamilyen p prím osztója $a^2 + 2$-nek. A nevező első tagjában szerepel $a^2 + 2$, így a további résznek, $a^2 + 1$-nek is osztója kell legyen p. Ebből az következik, hogy a két rész különbségének, $(a^2 + 2) - (a^2 + 1) = 1$-nek osztója p, ami nem lehetséges. ■

2.2. Osztók száma, a τ függvény

Egy n természetes szám *pozitív osztóinak száma* $\tau(n)$.

1. Ha $n = 1$, akkor $\tau(n) = 1$.
2. Ha $n > 1$ és az n szám kanonikus alakja $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$, akkor

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \dots (\alpha_k + 1). \tag{I}$$

A τ függvény multiplikatív, vagyis

$$\tau(a \cdot b) = \tau(a) \cdot \tau(b) \quad (a, b) = 1 \text{ esetén.}$$

A τ függvénynek ezt a tulajdonságát a példák megoldása során időnként fel fogjuk használni.

Példák

2.2-1. Hány pozitív osztója van 490-nek?

Megoldás. $490 = 2 \cdot 5 \cdot 7^2, \quad \tau(490) = 2 \cdot 2 \cdot 3 = 12$ ■

2.2-2. A $15^3 \cdot 12^6 \cdot 23^2 \cdot 14$ számnak

a. hány 21-hez relatív prím pozitív osztója van?

b. hány 21-gyel nem osztható pozitív osztója van?

Megoldás. Számítsuk ki a szám kanonikus alakját.

$$15^3 \cdot 12^6 \cdot 23^2 \cdot 14 = 2^{13} \cdot 3^9 \cdot 5^3 \cdot 7 \cdot 23^2$$

a. A számnak annyi 21-hez relatív prím pozitív osztója van, ahány osztója van a $2^{13} \cdot 5^3 \cdot 23^2$-nek, tehát $14 \cdot 4 \cdot 3 = 168$.

b. 1. *megoldás.*

A 3-mal nem osztható osztók száma megegyezik $2^{13} \cdot 5^3 \cdot 7 \cdot 23^2$ osztóinak a számával.

$$\tau_1 = \tau(2^{13} \cdot 5^3 \cdot 7 \cdot 23^2) = 14 \cdot 4 \cdot 2 \cdot 3 = 2 \cdot 168$$

A 7-tel nem osztható osztók száma megegyezik $2^{13} \cdot 3^9 \cdot 5^3 \cdot 23^2$ osztóinak a számával.

$$\tau_2 = \tau(2^{13} \cdot 3^9 \cdot 5^3 \cdot 23^2) = 14 \cdot 10 \cdot 4 \cdot 3 = 10 \cdot 168$$

A 3-mal és 7-tel nem osztható osztók száma $\tau_3 = 168$. A keresett szám:

$$\tau_1 + \tau_2 - \tau_3 = 2 \cdot 168 + 10 \cdot 168 - 168 = 11 \cdot 168 = 1848$$

2. *megoldás.*

Az összes osztó száma:

$$\tau(2^{13}\cdot 3^9\cdot 5^3\cdot 7\cdot 23^2)=14\cdot 10\cdot 4\cdot 2\cdot 3=20\cdot 168$$

A 21-gyel osztható osztók számát megkapjuk, ha az eredeti számból leválasztjuk $3\cdot 7$-et, és vesszük ennek az osztóit.

$$\tau(2^{13}\cdot 3^8\cdot 5^3\cdot 23^2)=14\cdot 9\cdot 4\cdot 3=9\cdot 168$$

A kettő különbsége adja a megoldást.

$$20\cdot 168-9\cdot 168=11\cdot 168=1848$$

■

2.2-3. A szultán 100 cellájában száz rab raboskodik. A szultán leküldi egymás után 100 emberét. A k-adik alkalommal leküldött ember minden k-adik cella zárján állít egyet, ha nyitva volt, bezárja, ha zárva volt, akkor kinyitja. Kezdetben minden cella zárva volt. Mely sorszámú cellák lesznek a végén nyitva?

Megoldás. Azok a cellák lesznek a végén kinyitva, amelyek sorszámában az osztók száma páratlan. $\tau(n)$ értéke akkor páratlan, ha (I) mindegyik tényezője páratlan, ez pedig akkor teljesül, ha a szám kanonikus alakjában minden kitevő páros. Az ilyen tulajdonságú számok éppen a négyzetszámok. A feltételeknek az 1 és 100 közötti négyzetszámok felelnek meg. ■

2.2-4. Határozzuk meg azt a legkisebb n természetes számot, amelyre
a. $\tau(n)=23$; **b.** $\tau(n)=25$; **c.** $\tau(n)=24$.

Megoldás.

a. $\tau(n)$	$=$	23	n	$=$	2^{22}	$=$	4 194 304
b. $\tau(n)$	$=$	25	n	$=$	$2^4\cdot 3^4$	$=$	1296
c. $\tau(n)$	$=$	24	n	$=$	$2^3\cdot 3^2\cdot 5$	$=$	360

■

2.2-5. Mi a szükséges és elégséges feltétele annak, hogy egy n természetes számnak ugyanannyi páros osztója legyen, mint ahány páratlan?

Megoldás. Legyen $n = 2^k \cdot y$, ahol $(2, y) = 1$. Ekkor $\tau(n) = (k + 1) \cdot \tau(y)$. A páratlan osztók száma éppen $\tau(y)$, ami a feltétel szerint megegyezik a páros osztók számával, és így

$$\tau(n) = 2 \cdot \tau(y).$$

Ebből $k + 1 = 2$, tehát $k = 1$. A feltételnek az $n = 4s + 2$ alakú számok felelnek meg, ahol s tetszőleges nem negatív egész szám.

■

2.3. Prímszámok

Vizsgáljuk meg, hogyan lehet egy n számról eldönteni, hogy prímszám-e vagy sem. Nyilvánvaló, hogy ha n összetett szám és p az n legkisebb prímosztója, akkor $p \le \frac{n}{2}$. Ennél azonban kisebb felső korlátot is lehet adni p-re.

1. tétel. Az n összetett szám legkisebb prímosztója nem lehet nagyobb $\sqrt{n}$ -nél.

Bizonyítás. Legyen p az n legkisebb prímosztója, és $n = pk$. p választása miatt $p \le k$. Ezért $p^2 \le pk$, $p^2 \le n$, amiből $p \le \sqrt{n}$. ■

Ha tehát egy számról el akarjuk dönteni, hogy prímszám-e, vagy összetett, elég a $\sqrt{n}$ -nél nem nagyobb prímszámokkal való oszthatóságot vizsgálni. Ha ezen prímek egyike sem osztója n-nek, akkor n prím.

Példa. Az $n = 83$ szám nem osztható 2, 3, 5, 7 egyikével sem. Ezek a $\sqrt{83}$ -nál nem nagyobb prímek. Ezért 83 maga is prím.

A következő módszer segítségével adott N számig előállíthatjuk az összes prímet.

Eratoszthenészi szita

Írjuk fel a számokat 2-től N-ig. A sorban az első – a 2 – prím. A 2 többszöröseit húzzuk ki a sorból. A következő legkisebb, amelyik megmaradt – a 3 – szintén prím. Most húzzuk ki 3 többszöröseit. A megmaradó legkisebb megint prím. És így tovább. Az eljárás végén a sorban megmaradt számok valamennyien prímek.

Az eljárást elég addig folytatni, amíg a megmaradó legkisebb szám nem nagyobb $\sqrt{N}$ -nél.

A következő tétel bizonyítása Euklidésztől származik.

2. tétel. A prímszámok száma végtelen.

Bizonyítás. Tegyük fel az állítással ellentétben, hogy $p_1, p_2, \ldots, p_k$ valamilyen $k \in \mathbb{N}$-re az összes létező prímszám. Képezzük az

$$N = p_1 p_2 \ldots p_k + 1 \tag{I}$$

számot. $N > 1$, mert például 2 a prímszámok között szerepel. A számelmélet alaptételéből következik, hogy N-nek létezik p prímosztója. Ennek a p prímnek az előbb felsoroltak között kell lennie. De $p|N$ és $p|p_1 \dots p_k$-ból (I) alapján $p|1$ következik, ami ellentmondás. Hibás volt tehát az a feltevésünk, mely szerint véges sok prím van, tehát a prímszámok száma végtelen. ∎

Az (I) képzési módszerrel előállított számok nem mind prímek.

$$2 + 1 = 3$$

$$2 \cdot 3 + 1 = 7$$

$$2 \cdot 3 \cdot 5 + 1 = 31$$

$$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

Az első öt esetben prímet kapunk, az utolsó azonban összetett szám.

A következő bizonyítás Vinogradovtól származik, és felhasználja az Euler-féle φ függvény fogalmát. (Lásd 2.6. fejezet.)

Bizonyítás. (**A 2. tétel 2. bizonyítása.**) Tegyük fel állításunkkal ellentétben, hogy véges sok prímszám van, $p_1, p_2, \dots, p_k$. Legyen $M = p_1 p_2 \dots p_k$. $M > 2$, mert például 2 és 3 prímek, és ezért $\varphi(M)$ páros. Másrészt azonban $1 < t < M$ esetén t osztói a fent említett prímek közül kerülnek ki – nem lévén más prím a feltevésünk szerint –, tehát $(M, t) > 1$ teljesül, vagyis $\varphi(M) = 1$, ami ellentmond annak, hogy páros. ∎

A szomszédos prímek között tetszőlegesen nagy hézag található.

3. tétel. Tetszőleges nagy N pozitív egész számhoz meg lehet adni N számú szomszédos összetett számot.

Bizonyítás. Legyen N adott, és p az N-nél nagyobb prímek közül a legkisebb. Ilyen prím biztosan létezik az előző tétel alapján. Vizsgáljuk meg a következő N egymás utáni számot.

$$\begin{aligned}
a_1 &= 2 \cdot 3 \cdot 5 \cdot 7 \dots p + 2 \\
a_2 &= 2 \cdot 3 \cdot 5 \cdot 7 \dots p + 3 \\
a_3 &= 2 \cdot 3 \cdot 5 \cdot 7 \dots p + 4 \\
&\vdots \\
a_{N-1} &= 2 \cdot 3 \cdot 5 \cdot 7 \dots p + N \\
a_N &= 2 \cdot 3 \cdot 5 \cdot 7 \dots p + (N + 1)
\end{aligned}$$

Ezek mindegyike összetett. Nézzük ugyanis a_i-t valamely $1 \le i \le N$ esetén. a_i előállításában a második tagnak valamely p_k prímosztója szerepel az első tagban is, hiszen $p \geq N+1$, így p_k osztója a_i-nek. Másrészt p_k valódi osztója a_i-nek, hiszen $a_i > p \geq p_k$, a_i tehát valóban összetett szám. ■

Ugyanakkor időnként előfordulnak egymáshoz igen közeli prímek, úgynevezett *ikerprímek.* q és p ikerprímek, ha $q = p+2$ teljesül $p, q \in \mathbb{N}$ prímekre. Például 3, 5; 5, 7; 11, 13; 17, 19 ikerprímek. Máig megoldatlan az a probléma, hogy vajon létezik-e végtelen sok ikerprím. Az 1996-ban ismert legnagyobb ikerprímek $242206083 \cdot 2^{38880} \pm 1$. Ezeket a 11713 jegyű számokat Karl-Heinz Indlekofer és Járai Antal találták.

Belátható, hogy bármely természetes szám és a kétszerese közé esik prím. 1937 óta tudjuk, hogy két szomszédos köbszám közé is esik prím elég nagy értéktől kezdve. Az azonban máig megoldatlan kérdés, hogy két szomszédos négyzetszám között van-e minden esetben prím.

4. tétel. (Dirichlet (1805 – 1859)) Legyenek a, b egészek, $a^2 + b^2 \neq 0$. Ha $(a, b) \neq 1$, akkor az $ak + b$ $(k \in \mathbb{N})$ sorozatban legfeljebb véges sok prím van. Ha $(a, b) = 1$, akkor az előbbi sorozatban végtelen sok prím van.

5. tétel. A

$$\sum_{p \text{ prím}} \frac{1}{p}$$

végtelen sor divergens.

Ez a tétel úgy is megfogalmazható, hogy a prímek viszonylag sűrűn helyezkednek el a természetes számok sorozatában.

Az alábbi tételt Hadamard és de la Vallée Poussin bizonyította 1896-ban.

6. tétel. (Nagy prímszámtétel.) Legyen $\pi(x)$ az x-nél nem nagyobb prímszámok száma. Ekkor

$$\lim_{x \to \infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = 1,$$

azaz $\pi(x)$ és $\frac{x}{\log x}$ aszimptotikusan egyenlőek.

Példák

2.3-1. Bizonyítsuk be, hogy végtelen sok $4k-1$ alakú prímszám van.
Megoldás.

Először belátjuk, hogy $4k-1$ alakú számnak van $4k-1$ alakú prímosztója. Nézzük két páratlan szám szorzatát 4-gyel való oszthatóság szempontjából. A következő esetek fordulhatnak elő:

$$(4k+1)(4s+1) = 4m+1$$

$$(4k+1)(4s-1) = 4m-1$$

$$(4k-1)(4s-1) = 4m+1$$

Ha csupa 4k+1 alakú prím szorzata lenne, a szorzat maga is ilyen alakú lenne.

Tegyük fel most, hogy véges sok $4k-1$ alakú prímszám van:

$$p_1,\ p_2,\ \dots,\ p_r$$

Legyen

$$N = 4p_1 \dots p_r - 1. \tag{1}$$

N-nek van $4k-1$ alakú prímosztója, ez legyen p. Ekkor $p|N$ és $p|p_1 \dots p_r$. Ebből (1) miatt $p|1$ következik, ami ellentmondás. ∎

2.3-2. Bizonyítsuk be, hogy végtelen sok $6k-1$ alakú prímszám van.
Megoldás.

Először belátjuk, hogy $6k-1$ alakú N számnak van $6k-1$ alakú prímosztója. A prímosztók $2, 3, 6k \pm 1$ alakúak lehetnek. $2 \nmid N$ és $3 \nmid N$. Két $6k+1$ alakú szám szorzata is ilyen, tehát kell legyen legalább egy $6k-1$ alakú prímtényező is.

Tegyük fel most, hogy véges sok $6k-1$ alakú prímszám van:

$$p_1,\ p_2,\ \dots,\ p_r$$

Legyen

$$N = 6p_1 \dots p_r - 1. \tag{1}$$

N-nek van $6k-1$ alakú prímosztója. Ekkor $p|N$ és $p|p_1 \dots p_r$. Ebből (1) miatt $p|1$ következik, ami ellentmondás. ∎

2.3-3. Lássuk be, hogy végtelen sok $4k+1$ alakú prím van.
Megoldás. A bizonyításhoz felhasználjuk, hogy $n \in \mathbb{N}$ esetén az n^2+1 szám minden páratlan prímosztója $4k+1$ alakú. (Lásd a 2.7.1-1. példát.)

Tegyük fel indirekt módon, hogy véges sok $4k+1$ alakú prím van, $p_1,\ p_2,\ \dots,\ p_s$. Képezzük ezekből az $A = 4(p_1 \cdot p_2 \cdot \ldots \cdot p_s)^2 + 1$ számot. Az előző példa szerint A-nak van $4k+1$ alakú prímosztója, amelyik az előző s prímtől mind különbözik. Van tehát a feltételezett s prímen kívül még más $4k+1$ alakú prím is. Ez ellentmondás, s így igaz az állítás. ∎

2.3-4. Határozzuk meg azokat a p prímszámokat (a negatívakat is), melyekre $p+10$ és $p+14$ is prímszám.
Megoldás.

$p-1$, p és $p+1$ egyike osztható 3-mal. Ha $3|p-1$, akkor $3|p+14$, ha pedig $3|p+1$, akkor $3|p+10$ is. $p, p+10$ és $p+14$ egyike tehát osztható 3-mal. Ez a szám akkor lesz prím, ha ± 3.

Ha $p=3$, akkor $p+10=13$, $p+14=17$.
Ha $p=-3$, akkor $p+10=7$, $p+14=11$.
Ha $p+10=3$, akkor $p=-7$, $p+14=7$.
Ha $p+10=-3$, akkor $p=-13$, $p+14=1$.
Ha $p+14=3$, akkor $p=-11$, $p+10=-1$.
Ha $p+14=-3$, akkor $p=-17$, $p+10=-7$.

Tehát a következő számhármasok maradnak.

p	$p+10$	$p+14$
3	13	17
-3	7	11
-7	3	7
-17	-7	-3

■

2.3-5. A kapitánynak három unokája van, életkoruk három különböző prímszám. Ezek négyzetének összege ismét prímet ad. Hány éves a kapitány legkisebb unokája?

Megoldás. Legyen az unokák életkora x, y és z. Ekkor $x^2+y^2+z^2=p$, valamint $x<y<z<p$. $x\neq 2$, mert különben $2|p$ lenne. Ha $x\neq 3$, akkor $x^2=3k+1$, és y, z is ilyenek. Ekkor $3|p$, ami ellentmondás. $x=3$ éves lehet csak a legkisebb unoka.

Van megoldása a feladatnak, mert például $3^2+5^2+7^2=83$. ■

2.4. Euklideszi algoritmus

Maradékos osztás

Ha $a, b\in\mathbb{Z}, b\neq 0$, akkor egyértelműen létezik olyan $q, r\in\mathbb{Z}$, melyre $a=bq+r$, ahol $0\leq r<|b|$.

Euklideszi algoritmus

Legyen $a, b \in \mathbb{Z}, b \neq 0$. A maradékos osztást végezzük el két rögzített számra. Ha a maradék nem nulla, akkor az osztót és a maradékot újra osszuk el maradékosan. Ezt mindaddig ismételjük, amíg nulla maradékot nem kapunk. Így az euklideszi algoritmushoz jutunk. (Euklidész Kr. e. 300 körül élt görög matematikus.)

$$
\begin{array}{lll}
a = bq_0 + r_0, & 0 \leq r_0 < |b|; & \text{ha } r_0 \neq 0, \text{ akkor} \\
b = r_0q_1 + r_1, & 0 \leq r_1 < r_0; & \text{ha } r_1 \neq 0, \text{ akkor} \\
r_0 = r_1q_2 + r_2, & 0 \leq r_2 < r_1; & \text{ha } r_2 \neq 0, \text{ akkor} \\
\vdots & \vdots & \vdots \\
r_{n-2} = r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1}; & \text{ha } r_n \neq 0, \text{ akkor} \\
r_{n-1} = r_nq_{n+1} & &
\end{array} \tag{I}
$$

Ez az eljárás minden esetben véges lesz, mert $r_0, r_1, \ldots, r_n$ pozitív egészek szigorúan csökkenő sorozata.

1. tétel. Ha $b|a$, akkor $(a, b) = |b|$. Ha $b \nmid a$, akkor az a, b számokkal végzett euklideszi algoritmus utolsó nem nulla maradéka az a és b legnagyobb közös osztója. Ha $(a, b) = d$, akkor léteznek olyan x és y egészek, melyekkel $ax + by = d$. (Más szóval d-t elő lehet állítani a és b egész együtthatós lineáris kombinációjaként.) •

A tételben szereplő lineáris kombinációt a következő módon készíthetünk. Sorban előállítjuk $r_0, r_1, \ldots, r_n$-et a és b lineáris kombinációjaként, felhasználva az euklideszi algoritmus számításait. Először r_0-at kifejezzük (I) első egyenletéből,

$$r_0 = a - bq_0.$$

Azután a másodikból kifejezzük r_1-et, és r_0 előállítását beírjuk.

$$r_1 = b - r_0q_1 = b - (a - bq_0)q_1$$

Rendezés után r_1 előállítását kapjuk meg a és b lineáris kombinációjaként. Az i-edik lépésben az i-edik egyenletből kifejezzük r_i-t, majd a benne szereplő r_{i-1} és r_{i-2} helyére írjuk be a korábban kapott lineáris kombinációt, stb. (Lásd a 2. példát.)

Megjegyzés. Végtelen sok x, y számpár van, amelyekkel elő lehet állítani a legnagyobb közös osztót. (Lásd az 5. fejezetet.)

Példák

2.4-1. Legyenek $a, b \in \mathbb{Z}, a^2 + b^2 \neq 0$. Tekintsük az

$$ax + by \quad (x, y \in \mathbb{Z}) \tag{1}$$

számokat. Lássuk be, hogy az ilyen alakú pozitív egészek közül a legkisebb szám legnagyobb közös osztója az a, b számpárnak.
Megoldás. A (1) alakú számok között van pozitív, ami következik az 1. tételből, amely szerint ebben a halmazban ott van a és b legnagyobb közös osztója. Jelöljük a legkisebb pozitív számot m-mel, s legyen $m = ax_0 + by_0$. Másrészt d-vel jelölve a pozitív legnagyobb közös osztót, tudjuk, hogy
$d = ax_1 + by_1$ alkalmas x_1, y_1 egész számokkal. Vizsgáljuk meg m és d kapcsolatát. Először tegyük fel, hogy $m \nmid d$. Ekkor létezik olyan q_1, r_1 számpár, amellyel

$$d = mq_1 + r_1, \quad 0 < r_1 < m$$

teljesül. Ebből

$$r_1 = d - mq_1 = ax_1 + by_1 - (ax_0 + by_0)q_1 = a(x_1 - x_0q_1) + b(y_1 - y_0q_1),$$

vagyis egy m-nél kisebb pozitív számot állítottunk elő (1) alakban. Mivel m a legkisebb ilyen volt, ellentmondásra jutottunk. Ezek szerint $m|d$. Ekkor azonban, mivel $d|a$ és $d|b$, (1)-ből $d|m$ is teljesül, s így $m = d$, lévén mindkettő pozitív. ∎

2.4-2. Az euklideszi algoritmussal számítsuk ki $a = 86$ és $b = 31$ legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat. Számítsuk ki a legkisebb közös többszöröst is.

Megoldás.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$86 = 31 \cdot 2 + 24$	$24 = 86 \cdot 1 + 31 \cdot (-2)$
$31 = 24 \cdot 1 + 7$	$7 = 31 - 24 \cdot 1 =$
	$= 31 - (86 \cdot 1 + 31 \cdot (-2)) =$
	$= 86 \cdot (-1) + 31 \cdot 3$
$24 = 7 \cdot 3 + 3$	$3 = 24 - 7 \cdot 3 =$
	$= (86 \cdot 1 + 31 \cdot (-2)) - (86 \cdot (-1) + 31 \cdot 3) \cdot 3 =$
	$= 86 \cdot 4 + 31 \cdot (-11)$
$7 = 3 \cdot 2 + 1$	$1 = 7 - 3 \cdot 2 =$
	$= (86 \cdot (-1) + 31 \cdot 3) - (86 \cdot 4 + 31 \cdot (-11)) \cdot 2 =$
	$= 86 \cdot (-9) + 31 \cdot 25$
$3 = 1 \cdot 3 + 0$	$0 = 86 \cdot 31 + 31 \cdot (-86)$

$\mathrm{lnko}(86, 31) = 1$, a lineáris kombinációs együtthatók: $x = -9$ és $y = 25$, amit az utolsó előtti sorból olvashatunk le. $\mathrm{lkkt}(86, 31) = \frac{86 \cdot 31}{\mathrm{lnko}(86,31)} = 2666.$

■

2.4-3. Az euklideszi algoritmussal számítsuk ki $a = 139$ és $b = 102$ legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

Megoldás.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$139 = 102 \cdot 1 + 37$	$37 = 139 \cdot 1 + 102 \cdot (-1)$
$102 = 37 \cdot 2 + 28$	$28 = 139 \cdot (-2) + 102 \cdot 3$
$37 = 28 \cdot 1 + 9$	$9 = 139 \cdot 3 + 102 \cdot (-4)$
$28 = 9 \cdot 3 + 1$	$1 = 139 \cdot (-11) + 102 \cdot 15$
$9 = 1 \cdot 9 + 0$	$0 = 139 \cdot 102 + 102 \cdot (-139)$

$\mathrm{lnko}(139, 102) = 1$, a lineáris kombinációs együtthatók: $x = -11$ és $y = 15$.

■

2.4-4. Az euklideszi algoritmussal számítsuk ki $a = 255$ és $b = 111$

legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat. Számítsuk ki a legkisebb közös többszöröst is.
Megoldás.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$255 = 111 \cdot 2 + 33$	$33 = 255 \cdot 1 + 111 \cdot (-2)$
$111 = 33 \cdot 3 + 12$	$12 = 255 \cdot (-3) + 111 \cdot 7$
$33 = 12 \cdot 2 + 9$	$9 = 255 \cdot 7 + 111 \cdot (-16)$
$12 = 9 \cdot 1 + 3$	$3 = 255 \cdot (-10) + 111 \cdot 23$
$9 = 3 \cdot 3 + 0$	$0 = 255 \cdot 37 + 111 \cdot (-85)$

$\mathrm{lnko}(255, 111) = 3$, a lineáris kombinációs együtthatók: $x = -10$ és $y = 23$.

$\mathrm{lkkt}(255, 111) = \frac{255 \cdot 111}{\mathrm{lnko}(255,111)} = 9435$. ■

2.4-5. Az euklideszi algoritmussal számítsuk ki $a = 332$ és $b = 88$ legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.
Megoldás.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$332 = 88 \cdot 3 + 68$	$68 = 332 \cdot 1 + 88 \cdot (-3)$
$88 = 68 \cdot 1 + 20$	$20 = 332 \cdot (-1) + 88 \cdot 4$
$68 = 20 \cdot 3 + 8$	$8 = 332 \cdot 4 + 88 \cdot (-15)$
$20 = 8 \cdot 2 + 4$	$4 = 332 \cdot (-9) + 88 \cdot 34$
$8 = 4 \cdot 2 + 0$	$0 = 332 \cdot 22 + 88 \cdot (-83)$

$\mathrm{lnko}(332, 88) = 4$, a lineáris kombinációs együtthatók: $x = -9$ és $y = 34$. ■

2.4-6. Az euklideszi algoritmussal számítsuk ki $a = 124$ és $b = 46$ legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

Megoldás.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$124 = 46 \cdot 2 + 32$	$32 = 124 \cdot 1 + 46 \cdot (-2)$
$46 = 32 \cdot 1 + 14$	$14 = 124 \cdot (-1) + 46 \cdot 3$
$32 = 14 \cdot 2 + 4$	$4 = 124 \cdot 3 + 46 \cdot (-8)$
$14 = 4 \cdot 3 + 2$	$2 = 124 \cdot (-10) + 46 \cdot 27$
$4 = 2 \cdot 2 + 0$	$0 = 124 \cdot 23 + 46 \cdot (-62)$

$\mathrm{lnko}(124, 46) = 2$, a lineáris kombinációs együtthatók: $x = -10$ és $y = 27$. ■

2.5. Kétváltozós lineáris diofantikus egyenletek

Legyenek a, b, c egész számok, $a \neq 0$ és $b \neq 0$. Keressünk olyan x, y egészeket, melyek kielégítik az

$$ax + by = c \tag{I}$$

egyenletet.

1. tétel. Az (I) diofantikus egyenlet akkor és csak akkor oldható meg, ha $(a, b)|c$ teljesül. Ha megoldható az egyenlet, akkor végtelen sok megoldása van. Ha $x_0,\ y_0$ megoldás, akkor az összes megoldás

$$x_t = x_0 + t\frac{b}{(a,b)} \qquad \text{és} \qquad y_t = y_0 - t\frac{a}{(a,b)} \tag{II}$$

alakban állítható elő valamilyen $t \in \mathbb{Z}$-vel, és (II) minden $t \in \mathbb{Z}$ esetén megoldást szolgáltat.

Bizonyítás.

1. A feltétel szükséges. Legyen ugyanis $x_0,\ y_0$ megoldása (I)-nek, tehát

$$ax_0 + by_0 = c. \tag{III}$$

Mivel (a, b) osztója a és b lineáris kombinációjának, (III) miatt osztója c-nek is.

2. A feltétel elégséges is. Legyen ugyanis $(a, b) = d$ és $d|c$. Az euklideszi algoritmusra vonatkozó tétel szerint az $ax + by = d$ egyenlet megoldható. Legyen x', y' egy megoldás, s így

$$ax' + by' = d.$$

Szorozzuk be az egyenletet a $\frac{c}{d}$ egész számmal.

$$ax'\frac{c}{d} + by'\frac{c}{d} = c$$

Az $x_0 = x'\frac{c}{d}$ és $y_0 = y'\frac{c}{d}$ számok (I)-nek megoldását szolgáltatják.

3. Tegyük fel most, hogy $x_0,\ y_0$ megoldása (I) -nek. Ekkor

$$x_t = x_0 + t\frac{b}{(a,b)} \quad \text{és} \quad y_t = y_0 - t\frac{a}{(a,b)} \quad t \in \mathbb{Z} \tag{IV}$$

szintén megoldást adnak, mert

$$ax_t + by_t = ax_0 + t\frac{ab}{(a,b)} + by_0 - t\frac{ab}{(a,b)} = ax_0 + by_0 = c.$$

4. Megmutatjuk, hogy egy tetszőleges $x_0,\ y_0$ megoldáspárból (IV) segítségével minden megoldás előállítható.

Tegyük fel, hogy $x_0,\ y_0$ és $x_t,\ y_t$ megoldáspárok. Ekkor

$$ax_0 + by_0 = c \quad \text{és} \quad ax_t + by_t = c,$$

amiből

$$ax_0 + by_0 = ax_t + by_t \tag{V}$$
$$b(y_0 - y_t) = a(x_t - x_0)$$
$$b | a(x_t - x_0).$$

Ebből

$$\frac{b}{(a,b)} \,\Bigg|\, \frac{a}{(a,b)}(x_t - x_0),$$

s mivel

$$\left(\frac{b}{(a,b)}, \frac{a}{(a,b)}\right) = 1,$$
$$\frac{b}{(a,b)} \,\Bigg|\, x_t - x_0,$$

amiből $x_t = x_0 + t\frac{b}{(a,b)}$ valamilyen $t \in \mathbb{Z}$ számmal. (V) jobb oldalán helyettesítsük be x_t kapott alakját:

$$ax_0 + by_0 = ax_0 + t\frac{ab}{(a,b)} + by_t$$

Ebből y_t-t kifejezve

$$y_t = y_0 - t\frac{a}{(a,b)}$$

lesz, amivel bebizonyítottuk az utolsó állításunkat is. ∎

Lineáris diofantikus egyenlet megoldása

1. *módszer.* Az euklideszi algoritmus alkalmazása hatékony módszert kínál a kétváltozós lineáris diofantikus egyenlet megoldására.

Tekintsük az

$$ax + by = c \tag{VI}$$

egyenletet. a és b legnagyobb közös osztója legyen d. Az euklideszi algoritmussal számítsuk ki d-t, és állítsuk elő a és b lineáris kombinációjaként.

$$ax' + by' = d$$

Ha $d|c$, tehát $\frac{c}{d}$ egész szám, akkor megoldható a (VI) egyenlet, és az

$$x_0 = x'\frac{c}{d} \qquad y_0 = y'\frac{c}{d}$$

számok (VI)-nak egy megoldását szolgáltatják. Az összes megoldás az előző tétel szerint

$$x_t = x_0 + t\frac{b}{(a,b)} \quad \text{és} \quad y_t = y_0 - t\frac{a}{(a,b)} \quad t \in \mathbb{Z}$$

2. *módszer.* A kétváltozós lineáris diofantikus egyenlet ekvivalens egy lineáris kongruenciával. A kongruencia megoldására és ebből a diofantikus egyenlet megoldására lásd a *Lineáris kongruenciák* című fejezetet.

Példák

Oldjuk meg az alábbi diofantikus egyenleteket

2.5-1. $172x + 62y = 38$

Megoldás. Az euklideszi algoritmussal számítsuk ki 172 és 62 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat. (Lásd a 2.4. fejezetet és a 2.4-2. példát.)

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$172 = 62 \cdot 2 + 48$	$48 = 172 \cdot 1 + 62 \cdot (-2)$
$62 = 48 \cdot 1 + 14$	$14 = 172 \cdot (-1) + 62 \cdot 3$
$48 = 14 \cdot 3 + 6$	$6 = 172 \cdot 4 + 62 \cdot (-11)$
$14 = 6 \cdot 2 + 2$	$2 = 172 \cdot (-9) + 62 \cdot 25$
$6 = 2 \cdot 3 + 0$	$0 = 172 \cdot 31 + 62 \cdot (-86)$

lnko(172, 62) = 2, a lineáris kombinációs együtthatók pedig $x' = -9$ és $y' = 25$ – ami a táblázat utolsó előtti sorából olvasható le. Mivel 2|38, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = (-9) \cdot 19 = -171 \qquad y_0 = y'\frac{c}{d} = 25 \cdot 19 = 475$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = -171 + 31t \qquad y_t = y_0 - t\frac{a}{(a,b)} = 475 - 86t \quad t \in \mathbb{Z}$$

■

2.5-2. $82x + 22y = 34$

Megoldás. Az euklideszi algoritmussal számítsuk ki 82 és 22 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$82 = 22 \cdot 3 + 16$	$16 = 82 \cdot 1 + 22 \cdot (-3)$
$22 = 16 \cdot 1 + 6$	$6 = 82 \cdot (-1) + 22 \cdot 4$
$16 = 6 \cdot 2 + 4$	$4 = 82 \cdot 3 + 22 \cdot (-11)$
$6 = 4 \cdot 1 + 2$	$2 = 82 \cdot (-4) + 22 \cdot 15$
$4 = 2 \cdot 2 + 0$	$0 = 82 \cdot 11 + 22 \cdot (-41)$

lnko(82, 22) = 2, a lineáris kombinációs együtthatók: $x' = -4$ és $y' = 15$.

Mivel 2|34, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = (-4) \cdot 17 = -68 \qquad y_0 = y'\frac{c}{d} = 15 \cdot 17 = 255$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = -68 + 11t \qquad y_t = y_0 - t\frac{a}{(a,b)} = 255 - 41t \quad t \in \mathbb{Z}$$

■

2.5-3. $450x + 86y = 100$
Megoldás. Az euklideszi algoritmussal számítsuk ki 450 és 86 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$450 = 86 \cdot 5 + 20$	$20 = 450 \cdot 1 + 86 \cdot (-5)$
$86 = 20 \cdot 4 + 6$	$6 = 450 \cdot (-4) + 86 \cdot 21$
$20 = 6 \cdot 3 + 2$	$2 = 450 \cdot 13 + 86 \cdot (-68)$
$6 = 2 \cdot 3 + 0$	$0 = 450 \cdot (-43) + 86 \cdot 225$

$\text{lnko}(450, 86) = 2$, a lineáris kombinációs együtthatók: $x' = 13$ és $y' = -68$.
Mivel $2|100$, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = 13 \cdot 50 = 650 \qquad y_0 = y'\frac{c}{d} = -68 \cdot 50 = -3400$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = 650 + 43t \qquad y_t = y_0 - t\frac{a}{(a,b)} = -3400 - 225t \quad t \in \mathbb{Z}$$

■

2.5-4. $125x + 45y = -20$
Megoldás. Az euklideszi algoritmussal számítsuk ki 125 és 45 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$125 = 45 \cdot 2 + 35$	$35 = 125 \cdot 1 + 45 \cdot (-2)$
$45 = 35 \cdot 1 + 10$	$10 = 125 \cdot (-1) + 45 \cdot 3$
$35 = 10 \cdot 3 + 5$	$5 = 125 \cdot 4 + 45 \cdot (-11)$
$10 = 5 \cdot 2 + 0$	$0 = 125 \cdot (-9) + 45 \cdot 25$

$\text{lnko}(125, 45) = 5$, a lineáris kombinációs együtthatók: $x' = 4$ és $y' = -11$.
Mivel $5| -20$, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = 4 \cdot (-4) = -16 \qquad y_0 = y'\frac{c}{d} = (-11) \cdot (-4) = 44$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = -16 + (-9)t \qquad y_t = y_0 - t\frac{a}{(a,b)} = 44 - (-25)t \quad t \in \mathbb{Z}$$

■

2.6. Euler-féle φ függvény

Legyen $n > 0$ egész szám, és jelölje $\varphi(n)$ az n-hez relatív prím számok számát az $1,\ 2,\ \ldots,\ n$ számok között.

n	n-nél nem nagyobb, n-hez relatív prím pozitív egészek	$\varphi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1, 3	2
5	1, 2, 3, 4	4
6	1, 5	2
7	1, 2, 3, 4, 5, 6	6
8	1, 3, 5, 7	4
$\vdots$	$\vdots$	$\vdots$

1. tétel. Ha $n \geq 3$ természetes szám, akkor $\varphi(n)$ páros.

Bizonyítás. Ha n páratlan, $\frac{n}{2}$ nem természetes szám, ha pedig n páros és $n > 2$, akkor $\frac{n}{2} > 1$ egész szám, és nem lesz n-hez relatív prím. Az n-hez relatív prímeket tehát a többi 1 és n közötti szám között kell keresnünk.

Legyen $1 \leq k \leq n$. Ekkor $(k, n) = (n-k, n)$. Ha ugyanis $d = (k, n)$, $d|k$ és $d|n$, akkor $d|n-k$ és $d|n$ miatt $d|(n-k, n)$ is teljesül. Fordítva, ha $d = (n-k, n)$ akkor $d|(k, n)$ ugyanígy belátható.

Eszerint k pontosan akkor relatív prím n-hez, ha $n-k$ az, tehát a relatív prímek $\frac{n}{2}$ -höz képest szimmetrikusan helyezkednek el, tehát párba állíthatók, ami igazolja az állításunkat. ■

2. tétel. Az Euler-féle φ függvény multiplikatív, vagyis

$$\varphi(ab) = \varphi(a) \cdot \varphi(b), \quad \text{ha } (a, b) = 1.$$

(A tételre adott mindkét bizonyítás felhasznál olyan fogalmakat, amelyek kongruenciákkal és maradékrendszerekkel kapcsolatosak, lásd a 2.7. fejezetet.)

Bizonyítás. Legyen $(a, b) = 1$, és rendezzük az 1 és ab közé eső számokat táblázatba az alábbi módon:

$$\begin{array}{cccc} 1 & 2 & \dots & a \\ a+1 & a+2 & \dots & 2a \\ \vdots & \vdots & \vdots & \vdots \\ ra+1 & ra+2 & \dots & (r+1)a \\ \vdots & \vdots & \vdots & \vdots \\ (b-1)a+1 & (b-1)a+2 & \dots & ba \end{array}$$

Ebben a táblázatban $\varphi(ab)$ olyan szám van, amelyik ab-hez relatív prím. Egy szám pontosan akkor relatív prím ab-hez, ha a-hoz és b-hez külön-külön relatív prím. Keressük meg a táblázatban azon elemek számát, amelyek a-hoz is és b-hez is relatív prímek.

Mivel egy-egy oszlop modulo a ugyanabba a maradékosztályba tartozik, és minden sorban egy teljes maradékrendszer van modulo a, így $\varphi(a)$ olyan oszlop van a táblázatban, amelyiknek az elemei relatív prímek a-hoz. Egy ilyen oszlop legyen

$$s, a+s, 2a+s, \dots, (b-1)a+s.$$

Belátjuk, hogy ez az oszlop modulo b teljes maradékrendszer. Valóban, a

$$0,\ 1,\ \dots,\ b-1$$

számok teljes maradékrendszert alkotnak modulo b, és a b-hez relatív prím a-val szorozva, majd mindegyik elemhez s-et adva, továbbra is teljes maradékrendszert kapunk. (Lásd az omnibusztételt 2.7.-ben.)

Ezért minden ilyen oszlopban $\varphi(b)$ olyan elem van, amelyik b-hez relatív prím. Így az a-hoz és b-hez egyszerre relatív prímek száma $\varphi(a)\cdot\varphi(b)$, másrészt ez a szám előzetes megjegyzésünk alapján $\varphi(ab)$-vel is egyenlő, a φ függvény tehát multiplikatív. ∎

Bizonyítás. (2. tétel. 2. bizonyítása.)

Legyen $(a, b) = 1$, és tekintsük az

$$ak + bt, \quad 1 \le k \le b, \quad 1 \le t \le a \tag{I}$$

számokat, ahol k és t ezeket az értékeket egymástól függetlenül felveszik, így (I)-ben ab szám van.

1. Először megmutatjuk azt, hogy az (I)-beli számok modulo ab teljes maradékrendszert alkotnak.

Legyen (k,t) és (k_1,t_1) két különböző számpár, ami azt jelenti, hogy a $k=k_1$ és $t=t_1$ egyenlőségek közül legalább az egyik nem áll fenn. Tegyük fel, hogy

$$ak+bt \equiv ak_1+bt_1 \pmod{ab}. \tag{II}$$

Ebből következik az, hogy modulo a tekintve is kongruensek a fenti számok.

$$\begin{aligned} ak+bt &\equiv ak_1+bt_1 \pmod{a} \\ bt &\equiv bt_1 \pmod{a}, \end{aligned}$$

és mivel $(a,b)=1$,

$$t \equiv t_1 \pmod{a},$$

sőt $t=t_1$, tekintettel t és t_1 lehetséges értékeire.

A (II) kongruenciából hasonlóan

$$\begin{aligned} ak+bt &\equiv ak_1+bt_1 \pmod{b} \\ ak &\equiv ak_1 \pmod{b} \\ k &\equiv k_1 \pmod{b} \\ k &= k_1 \end{aligned}$$

is következik.

Ha tehát (II) teljesül, akkor feltevésünkkel ellentétben $t=t_1$ és $k=k_1$. Mivel így az (I)-beli számok inkogruensek és számuk ab, valóban teljes maradékrendszert alkotnak, s a köztük levő ab-hez relatív prímek száma $\varphi(ab)$.

2. Belátjuk, hogy $(a,t)>1$ esetén $(ak+bt,ab)>1$ is teljesül. Legyen $d|(a,t)$ és $d>1$. Ekkor egyrészt $d|a$ miatt $d|ab$, másrészt $d|a$ és $d|t$ miatt $d|ak+bt$, és így $d|(ak+bt,ab)$, tehát $(ak+bt,ab)>1$. Hasonlóan látható be, hogy $(b,k)>1$ esetén $(ak+bt,ab)>1$.

3. Végül megmutatjuk, hogy $(a,t)=1$ és $(b,k)=1$ esetén $(ak+bt,ab)=1$. Tegyük fel, hogy $(a,t)=1$ és $(b,k)=1$, valamint $(ak+bt,ab)=d>1$. Ekkor létezik olyan p prím, melyre $p|d$, s így

$$p|ak+bt \tag{III}$$

és

$$p|ab. \tag{IV}$$

(IV) miatt $p|a$ vagy $p|b$. Az általánosság megszorítása nélkül feltehetjük, hogy

$$p|a. \tag{V}$$

(V) és (III) miatt $p|bt$, amiből

$$p|b \tag{VI}$$

vagy

$$p|t. \tag{VII}$$

Az utóbbi kettő ellentmondásra fog vezetni. (VI) és (V) miatt ugyanis $p|(a,b)=1$ lenne. (VII) és (V) miatt pedig $p|(a,t)=1$ teljesülne. Így csak az $(ak+bt,ab)=1$ lehetőség marad.

2. és 3.-ból látszik, hogy pontosan akkor lesz $ak+bt$ relatív prím ab-hez, ha $(a,t)=1$ és $(b,k)=1$ egyszerre teljesül. Ez éppen $\varphi(a)\varphi(b)$ esetben fog bekövetkezni, ami 1. miatt $\varphi(ab)$-vel egyezik meg. ∎

Mivel φ multiplikatív, elég értékeit prímhatvány helyeken ismerni.

3. tétel. Legyen p prím, $\alpha \in \mathbb{N}$. Ekkor $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

Bizonyítás. Keressük az 1 és p^α közötti p^α-hoz relatív prímek számát. E p^α darab szám között csupán azok nem lesznek relatív prímek p^α-hoz, amelyek p-nek többszörösei, tehát a

$$p, 2p, 3p, \ldots, p^{\alpha-1}p.$$

Ezeknek a száma $p^{\alpha-1}$. Így $p^\alpha-p^{\alpha-1}$ olyan szám van a vizsgáltak között, amelyik p^α-hoz relatív prím. ∎

Az Euler-féle φ függvény kiszámítása

1. $n=1$ esetén $\varphi(n)=1$.
2. $n>1$ esetén legyen n kanonikus alakja:

$$n=\prod_{i=1}^{r} p_i^{\alpha_i}$$

Ekkor

$$\varphi(n)=\prod_{i=1}^{r}\varphi(p_i^{\alpha_i})=\prod_{i=1}^{r}(p_i^{\alpha_i}-p_i^{\alpha_i-1})= \tag{VIII}$$

$$=\prod_{i=1}^{r}(p_i^{\alpha_i-1}(p_i-1))= \tag{IX}$$

$$=n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right). \tag{X}$$

Példa.

$$\varphi(20)=\varphi(2^2\cdot 5)=\varphi(2^2)\varphi(5)=(2^2-2)(5-1)=2\cdot 4=8$$

Tehát 1 és 20 között 8 olyan szám van, amelyik a 20-hoz relatív prím.

Példák

2.6-1. Számítsuk ki az értéküket:

a. $\varphi(9)$ **b.** $\varphi(540)$ **c.** $\varphi(900)$ **d.** $\varphi(6!)$ **e.** $\varphi(7!)$

Megoldás.

a. $\varphi(9) = \varphi(3^2) = 3^2 - 3 = 6$

b. $\varphi(540) = \varphi(2^2 \cdot 3^3 \cdot 5) = 2 \cdot 18 \cdot 4 = 144$

c. $\varphi(900) = \varphi(2^2) \cdot \varphi(5^2) \cdot \varphi(3^2) = 2 \cdot 20 \cdot 6 = 240$

d. $\varphi(6!) = \varphi(2^4) \cdot \varphi(3^2) \cdot \varphi(5) = (2^4 - 2^3) \cdot (3^2 - 3) \cdot (5 - 1) = 8 \cdot 6 \cdot 4 = 192$

e. $\varphi(7!) = \varphi(2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7) = \varphi(2^4 \cdot 3^2 \cdot 5 \cdot 7) = 8 \cdot 6 \cdot 4 \cdot 6 = 1152$

■

2.6-2. Melyek azok a természetes számok, amelyekre $\varphi(n) = 1$?

Megoldás.

Az $n = 1$ megoldása az egyenletnek.

Egyébként

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = \prod_{i=1}^{r} (p_i^{\alpha_i - 1}(p_i - 1)) = 1.$$

Ebből $r = 1$ és $p - 1 = 1$, tehát $p = 2$. $p^{\alpha-1} = 1$ miatt pedig $\alpha = 1$.

Tehát a megoldás $n = 1$ és $n = 2$. ■

2.6-3. Melyek azok a természetes számok, amelyekre $\varphi(n)$ értéke páratlan?

Megoldás.

1. *megoldás.* $\varphi(1) = 1$ és $\varphi(2) = 1$, különben $\varphi(n)$ értéke páros. Nézzük (IX)-et. Ha n kanonikus alakjában előfordul $p > 2$ prím valamilyen α kitevővel, akkor $p^\alpha - p^{\alpha-1}$ páros, s így a $\varphi(n)$ értéke páros. Ha pedig n kanonikus alakjában szerepel 2^α, $\alpha > 1$, akkor szintén (IX)-ben $2^{\alpha-1}$ értéke páros, s emiatt $\varphi(n)$ értéke megint páros.

2. *megoldás.* $\varphi(1) = 1$ és $\varphi(2) = 1$. Legyen most $m > 2$. Ha $(x, m) = 1$, akkor $(m - x, m) = 1$, és ha $m > 2$, akkor $\frac{m}{2}$ nem egész, vagy $(\frac{m}{2}, 1) > 1$. Az m-hez relatív prímek tehát párba állíthatók, s így $\varphi(n)$ értéke ezekre az n-ekre páros. ■

2.6-4. Bizonyítsuk be, hogy ha $m \geq 2$ egész szám, akkor az m-nél kisebb, m-hez relatív prím számok összege $\frac{1}{2}m\varphi(m)$.

Megoldás. $m = 2$ esetén $\frac{1}{2} \cdot 2 \cdot \varphi(2) = 1$, ami igazolja az állítást. Legyen most $m > 2$. Az 1. tétel bizonyításában beláttuk, hogy ekkor az m-nél kisebb, m-hez relatív prím számok párba állíthatók. Mivel k párja $m - k$, egy ilyen pár összege m, és $\varphi(m)$ pár van, így a párok összege $\frac{1}{2} m\varphi(m)$. ■

2.6-5. Bizonyítsuk be, hogy minden n természetes számra

$$\varphi(n^2) = n\varphi(n).$$

Megoldás. Legyen n kanonikus alakja:

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

(X) alapján

$$\varphi(n^2) = n^2 \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) = n\varphi(n).$$

■

2.6-6. Oldjuk meg a $\varphi(2x) = \varphi(3x)$ egyenletet.
Megoldás. Legyen

$$x = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot y, \quad \text{ahol } (y, 6) = 1.$$

Ekkor az egyenlet így alakul:

$$\varphi(2^{\alpha_1+1} \cdot 3^{\alpha_2} \cdot y) = \varphi(2^{\alpha_1} \cdot 3^{\alpha_2+1} \cdot y)$$
$$\varphi(2^{\alpha_1+1} \cdot 3^{\alpha_2}) \cdot \varphi(y) = \varphi(2^{\alpha_1} \cdot 3^{\alpha_2+1}) \cdot \varphi(y)$$

$\varphi(y)$-nal egyszerűsítve, és beírva a φ függvény értékeit:

$$(2^{\alpha_1+1} - 2^{\alpha_1}) \cdot (3^{\alpha_2} - 3^{\alpha_2-1}) = (2^{\alpha_1} - 2^{\alpha_1-1}) \cdot (3^{\alpha_2+1} - 3^{\alpha_2})$$

Ha $\alpha_2 > 0$, akkor a jobb oldalon eggyel több 3-as tényező szerepel, így csak $\alpha_2 = 0$ teljesülhet.

$$(2^{\alpha_1+1} - 2^{\alpha_1}) = (2^{\alpha_1} - 2^{\alpha_1-1}) \cdot (3 - 1)$$

Ebből leolvashatjuk, hogy α_1 tetszőleges 0-nál nagyobb érték lehet. Az egyenlet megoldása $x = 2^{\alpha} \cdot y$, ahol $(y, 6) = 1$, α tetszőleges pozitív szám. ■

2.7. Kongruenciák, maradékrendszerek, Euler–Fermat-tétel

Legyen $m \in \mathbb{N}$ rögzített érték, $a, b \in \mathbb{Z}$. *a kongruens b-vel modulo m*, ha $m|a-b$. Ezt a tényt $a \equiv b \pmod{m}$-mel jelöljük. Ha ez az oszthatóság nem teljesül, akkor az $a \not\equiv b \pmod{m}$ jelölést használjuk. Például

$$\begin{array}{rlr} 21 \equiv 3 \pmod{6}, & \text{mert} & 6|21-3. \\ 19 \equiv -1 \pmod{5}, & \text{mert} & 5|19+1. \\ -11 \not\equiv 2 \pmod{10}, & \text{mert} & 10 \nmid -11-2. \end{array}$$

Legyen $m \in \mathbb{N}$ tetszőleges rögzített szám, és tekintsük a következő relációt: $R = \{(a,b) \big| a, b \in \mathbb{Z}, m|a-b\}$. R ekvivalenciareláció. A kongruenciák segítségével tehát az egész számok osztályozásához jutunk. A keletkezett osztályokat *maradékosztályoknak* nevezzük.

$a \equiv b \pmod{m}$ pontosan akkor teljesül, ha a és b m-mel való osztási maradéka azonos. Tehát azok az egészek kerülnek egy osztályba, amelyek m-mel osztva ugyanazt a maradékot szolgáltatják, és mivel a maradékok 1, 2, ..., $m-1$ lehetnek, m különböző maradékosztály van modulo m. A modulo m a0,-val kongruens elemek halmazát az a elem által reprezentált maradékosztálynak nevezzük, és $\overline{a} \pmod{m}$-mel jelöljük.

Ha az m szerinti maradékosztályok mindegyikéből kiemelünk egy reprezentáns elemet, akkor m szerinti *teljes maradékrendszert* kapunk.

Modulo 8 teljes maradékrendszer például $\{8,\ -1,\ 10,\ 19,\ 4,\ 29,\ -10,\ 7\}$. Általában modulo m teljes maradékrendszert alkotnak az m-mel való maradékos osztásnál keletkező legkisebb nem negatív maradékok, $\{0,\ 1,\ \ldots,\ m-1\}$, valamint a legkisebb abszolút értékű maradékok, páratlan modulus esetén

$$\{0,\ \pm 1,\ \pm 2,\ \ldots,\ \pm\frac{m-1}{2}\},$$

páros modulus esetén pedig

$$\{0,\ \pm 1,\ \pm 2,\ \ldots,\ \pm\left(\frac{m}{2}-1\right),\ \frac{m}{2}\}.$$

Az utóbbi esetben $\frac{m}{2}$ helyett $-\frac{m}{2}$ is választható.

Az $a_1,\ a_2,\ \ldots,\ a_s$ egészek akkor és csak akkor alkotnak teljes maradékrendszert modulo m, ha $s = m$, és $a_i \not\equiv a_j \pmod{m}, i \neq j$ esetén.

Ha $a \equiv b \pmod{m}$, akkor $(a, m) = (b, m)$. Az állítás fordítva nem igaz. Például $(2, 10) = 2, (4, 10) = 2$, de $2 \not\equiv 4 \pmod{10}$. Ha $a \equiv b \pmod{m}$ esetén a és b egyike relatív prím m-hez, akkor a másik is az.

Az előbbiek szerint ha az $\overline{a} \pmod{m}$ maradékosztályban van m-hez relatív prím, akkor ennek a maradékosztálynak minden eleme relatív prím m-hez.

Ez indokolja a következő definíciót. Az $\overline{a}$ (mod m) maradékosztály *redukált maradékosztály*, ha elemei az m-hez relatív prímek. Ha minden m szerinti redukált maradékosztályból veszünk egy reprezentáns elemet, akkor m szerinti *redukált maradékrendszert* kapunk. Mivel az $1,\ 2,\ \ldots,\ m$ számok teljes maradékrendszert alkotnak, a köztük található, m-hez relatív prímek redukált maradékrendszert képeznek. Ezek száma pedig $\varphi(m)$. Az m szerinti redukált maradékosztályok száma tehát $\varphi(m)$. Például modulo 8 redukált maradékrendszer $\{-1,\ 19,\ 29,\ 7\}$.

Az $a_1,\ a_2,\ \ldots,\ a_s$ egészek akkor és csak akkor alkotnak redukált maradékrendszert modulo m, ha $s=\varphi(m)$, $a_i \not\equiv a_j \pmod{m}$ $(i \neq j)$, valamint $(a_i, m) = 1$ $(1 \leq i \leq s)$.

Műveletek kongruenciákkal

1. $\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \rightarrow a + c \equiv b + d \pmod{m}$

2. $\left.\begin{array}{l} a \equiv b \pmod{m} \\ c \equiv d \pmod{m} \end{array}\right\} \rightarrow ac \equiv bd \pmod{m}$

3. $ac \equiv bc \pmod{m} \quad \Leftrightarrow \quad a \equiv b \pmod{\frac{m}{(m,c)}}$

4. $(m,c) = 1$ esetén $ac \equiv bc \pmod{m} \rightarrow a \equiv b \pmod{m}$

5. $a \equiv b \pmod{k} \quad \rightarrow \quad ac \equiv bc \pmod{kc}$

Az első három állítás bizonyítása megtalálható a feladatok megoldásait tartalmazó fejezetben.

3. speciális esete 4. Ha $m = kc$, akkor 3. második része 5. szerint fogalmazható meg.

Fermat-számok, Fermat-prímek

Az $F_n = 2^{2^n} + 1 \quad (n \in \mathbb{N}_0)$ sorozattal kapcsolatban Pierre Fermat(1601–1665) azt vizsgálta, hogy az elemei prímek-e. Nézzük az első hat elemet. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\ 537$, $F_5 = 2^{32} + 1 = 4\ 294\ 967\ 297$. Az első öt szám valóban prím, F_5 azonban nem az, ami – a szám nagyságát tekintve – kézi számolással igen hosszadalmasan lenne igazolható. Fermat egyetlen utóbb hamisnak bizonyult sejtése az volt, hogy ez is prím. Leonhard Euler (1707–1783) kongruenciák segítségével látta be, hogy $641 | 2^{32} + 1$. Ez a megoldás megtalálható a feladatok megoldásait tartalmazó fejezetben.

Teljes maradékrendszer, illetve redukált maradékrendszer lineáris transzformációi

Omnibusztétel.

Legyen $a_1,\ a_2,\ \ldots,\ a_m$ teljes maradékrendszer, $b_1,\ b_2,\ \ldots,\ b_{\varphi(m)}$ redukált maradékrendszer modulo m, és $a, c \in \mathbb{Z}$.

1. $(a,m)=1 \quad \rightarrow \quad aa_1+c,\ aa_2+c,\ \ldots,\ aa_m+c$ teljes maradékrendszer modulo m

2. $(a,m)=1 \quad \rightarrow \quad ab_1,\ ab_2,\ \ldots,\ ab_{\varphi(m)}$ redukált maradékrendszer modulo m

Ezeknek az állításoknak a bizonyítása megtalálható a feladatok megoldásait tartalmazó fejezetben.

Euler-féle kongruenciatétel

Legyen $a \in \mathbb{Z}$. Ha $(a,m)=1$, akkor $a^{\varphi(m)} \equiv 1 \pmod m$.

Megjegyzés.

A tételben szereplő $(a,m)=1$ feltétel szükséges. Ha ez nem teljesül, nem igaz az állítás sem. Tegyük fel ugyanis, hogy $(a,m)=d>1$, és így $d|a$ és $d|m$. Ekkor azonban $d|(a^{\varphi(m)},m)$. Ha $a^{\varphi(m)} \equiv 1 \pmod m$ fennállna, akkor $(a^{\varphi(m)},m)=(1,m)=1$ lenne, ami szerint $d>1$ nem fordulhatna elő.

Bizonyítás.

Legyen $b_1,\ b_2,\ \ldots,\ b_{\varphi(m)}$ redukált maradékrendszer modulo m.
$ab_1,\ ab_2,\ \ldots,\ ab_{\varphi(m)}$ is redukált maradékrendszer, hiszen $(a,m)=1$. Ez azt jelenti, hogy mindkét halmazban ott van minden egyes redukált maradékosztálynak egy-egy képviselője, esetleg más sorrendben. Így párba állíthatók a reprezentánsok. Minden egyes b_i-hez egyértelműen megtalálható az az ab_{j_i} szám, amelyikkel

$$b_i \equiv ab_{j_i} \pmod m \quad (1 \le i \le \varphi(m)).$$

Szorozzuk össze ezeket a kongruenciákat.

$$\prod_{1\le i\le\varphi(m)} b_i \equiv \prod_{1\le i\le\varphi(m)} ab_{j_i} \pmod m$$

Amiből

$$\prod_{1\le i\le\varphi(m)} b_i \equiv a^{\varphi(m)} \prod_{1\le i\le\varphi(m)} b_{j_i} \pmod m$$

és $(b_i,m)=1$ $(1 \le i \le \varphi(m))$ miatt $1 \equiv a^{\varphi(m)} \pmod m$, ami igazolja az állításunkat. ∎

Ha $m = p$ prím, akkor $\varphi(p) = p - 1$. Az Euler-tétel ekkor a következő alakot ölti.

A Fermat-tétel 1. alakja.

Legyen p prím, $a \in \mathbb{Z}$.

$$\text{Ha } p \nmid a, \text{ akkor } a^{p-1} \equiv 1 \pmod{p}. \tag{I}$$

A Fermat-tétel 2. alakja.

Legyen p prím, $a \in \mathbb{Z}$. Ekkor $a^p \equiv a \pmod{p}$.

Bizonyítás. Ha $p \nmid a$, akkor (I)-et a-val megszorozva megkapjuk egyenletünket. Ha pedig $p|a$, akkor $a \equiv 0 \pmod{p}$ és $a^p \equiv 0 \pmod{p}$, amiből $a^p \equiv a \pmod{p}$ szintén teljesül. ∎

Hatványozás ismételt négyzetre emeléssel (Gyorshatványozás)

Az alábbi módszer alkalmazásával viszonylag kevés művelet elvégzésével megkapjuk a^b-t vagy a^b maradékát modulo m, ahol a egész szám, b 1-nél nagyobb egész, m pozitív egész.

Legyen $c = \lfloor \log_2 b \rfloor$. Fejtsük b-t kettes alapú számrendszerbe.

$$b = 2^{b_1} + 2^{b_2} + \ldots + 2^{b_r}, \qquad \text{ahol} \qquad 0 \le b_1 < b_2 < \ldots < b_r \le c.$$

Ezután ismételt négyzetre emeléssel (és modulo m minden lépésben redukálva) számoljuk ki az

$$a^2,\ a^4,\ a^8,\ \ldots,\ a^{2^c}$$

értékeket (illetve az értékek maradékát modulo m). Végül

$$a^b = a^{2^{b_1}} a^{2^{b_2}} \ldots\ a^{2^{b_r}}$$

alapján megkapjuk a keresett hatványt (illetve a maradékot). Ezzel a módszerrel legfeljebb $5 \log_2 b$ lépésben megkapjuk a kívánt eredményt, ahol egy lépés két egész szám összeadását, kivonását, szorzását, illetve maradékos osztását jelenti.

Példa. a^{23} kiszámítása a következő lépések szerint történhet.

$$23 = 2^4 + 2^2 + 2 + 1$$

Elvégezzük a megfelelő négyzetre emeléseket.

$$a,\ a^2,\ a^4 = (a^2)^2,\ a^8 = (a^4)^2,\ a^{16} = (a^8)^2,$$

s ebből

$$a^{23} = a^{2^4} \cdot a^{2^2} \cdot a^2 \cdot a^1 = a^{16} \cdot a^4 \cdot a^2 \cdot a^1.$$

Ha a feladat a^{23} kiszámítása valamilyen m modulus szerint, akkor minden lépésben érdemes a modulo m szerinti maradékot venni, és a továbbiakban mindig azzal számolni.

Példák

2.7.1. Kongruenciák, maradékrendszerek

2.7-1. Bizonyítsuk be kongruenciákkal az alábbi állításokat. Legyen $a, b \in \mathbb{Z}, k, n \in \mathbb{N}$. **Ekkor:**

a. $a - b | a^n - b^n$
b. $a + b | a^{2k} - b^{2k}$
c. $a + b | a^{2k-1} + b^{2k-1}$

Megoldás.

a. Mivel $a - b | a - b$, ezért $a \equiv b \pmod{a - b}$. A kongruenciák szorzási tulajdonságát felhasználva $a^n \equiv b^n \pmod{a-b}$, ami az $a-b|a^n-b^n$ állítással ekvivalens.

A **b.** és **c.** állítás bizonyításához felhasználjuk, hogy $a - b | a^n - b^n$. Ebből $a + b = a - (-b) | a^n - (-b)^n$ alapján az $n = 2k$, illetve az $n = 2k - 1$ helyettesítéssel következnek az állítások. ■

2.7-2. Lássuk be, hogy

$$25,\ -20,\ 16,\ 46,\ -21,\ 18,\ 37,\ -17$$

teljes maradékrendszert alkot modulo 8.

Megoldás.

Nézzük azokat a maradékokat, amelyek a számok 8-cal való maradékos osztása során keletkeznek.

25	−20	16	46	−21	18	37	−17
1	4	0	6	3	2	5	7

A pozitív legkisebb maradékok mindegyike pontosan egyszer szerepel, így modulo 8 teljes maradékrendszerről van szó. ■

2.7-3. Teljes maradékrendszer-e

$$1,\ 11,\ 21,\ 31,\ 41,\ \ldots,\ 751,\ 761 \pmod{77}?$$

Megoldás. Az adott számok $k10+1$ alakúak, ahol $0 \leq k \leq 76$. A $\pmod{77}$ legkisebb pozitív maradékokból álló teljes maradékrendszerből 10-zel való szorzással és 1 hozzáadásával keletkeznek. Mivel $(10, 77) = 1$, az "omnibusz-tétel" szerint ez a halmaz is teljes maradékrendszert alkot. ■

2.7-4. Teljes maradékrendszer-e

$$7,\ 22,\ 37,\ 52,\ 67,\ \ldots,\ 11632,\ 11647 \pmod{777}?$$

Megoldás.

Az adott számok $15s+7$ alakúak, ahol $0 \leq s \leq 776$. Azonban $3 = (15, 777) \neq 1$, és így az "omnibusztétel" nem alkalmazható. Legyen $15s+7$ és $15k+7$ az adott halmazból, és vizsgáljuk meg, mikor lesznek egymással kongruensek $\pmod{777}$.

$$15s + 7 \equiv 15k + 7 \pmod{777}$$

A kongruencia mindkét oldalából kivonunk 7-et.

$$15s \equiv 15k \pmod{777}$$

Alkalmazzuk a 3. műveleti tulajdonságot, a kongruencia mindkét oldalát elosztjuk 15-tel, a modulust pedig $(15, 777) = 3$-mal.

$$s \equiv k \pmod{259}$$

Az adott halmazból lehet egymással kongruens két különböző szám. Például 7 és $15 \cdot 259 + 7$ ugyanabba a maradékosztályba esnek. ■

2.7-5. Határozzuk meg $3,\ 8,\ 17,\ -17,\ 120,\ 54,\ -40,\ 236,\ 237$

a. legkisebb nemnegatív maradékait $\pmod{11}$**,**

b. abszolút legkisebb maradékait $\pmod{11}$**.**

c. A fenti számok közül melyek kongruensek egymással $\pmod{11}$**?**

Megoldás.

	3	8	17	−17	120	54	−40	236	237
a.	3	8	6	5	10	10	4	5	6
b.	3	−3	−5	5	−1	−1	4	5	−5

Ezek alapján könnyen megállapítható, hogy a következő párok tagjai kongruensek egymással: $(17, 237)$, $(-17, 236)$, $(120, 54)$. ■

2.7-6. Redukált maradékrendszer-e

$$5, 15, 25, 35, 45, 55, \ldots, 155 \pmod{32}? \tag{1}$$

Megoldás.

1. *megoldás.*

Az adott halmaz elemei $10k + 5$ alakúak, ahol $0 \leq k \leq 15$.

a. Egy redukált maradékrendszer elemeinek a száma $\varphi(32) = \varphi(2^5 - 2^4) = 16$. A megadott halmaznak éppen ennyi eleme van.

b. Belátjuk, hogy az adott számok páronként inkongruensek. Tegyük fel, hogy

$$10k + 5 \equiv 10s + 5 \pmod{32}$$

Mindkét oldalból kivonjuk az 5-öt.

$$10k \equiv 10s \pmod{32}$$

Alkalmazzuk a 3. műveleti tulajdonságot, a kongruencia mindkét oldalát elosztjuk 10-zel, a modulust pedig $(10, 32) = 2$-vel.

$$k \equiv s \pmod{16}$$

Ha $k \equiv s \pmod{16}$, akkor $k = s$, mert $0 \leq k, s < 16$.

c. Az adott számok relatív prímek a modulushoz.

Ezek alapján (1) redukált maradékrendszer.

2. *megoldás.*

Az $1,\ 3,\ 5,\ \ldots,\ 31$ redukált maradékrendszerből 5-tel szorozva kapjuk (1)-et. $(5, 32) = 1$ s így az „omnibusztétel” alapján, (1) is redukált maradékrendszer. ■

2.7.2. Euler–Fermat-tétel

2.7-7. Lássuk be, hogy $n \in \mathbb{N}$ esetén az $n^2 + 1$ szám minden páratlan prímosztója $4k + 1$ alakú.

Megoldás. Legyen $p | n^2 + 1$ és páratlan prím, tehát $p \neq 2$. Ekkor

$$n^2 \equiv -1 \pmod{p}.$$

Mivel $\frac{p-1}{2}$ egész, vehetjük az előbbi egyenlet $\frac{p-1}{2}$ -dik hatványát.

$$(n^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p},$$

vagyis

$$n^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

A feltételből következik, hogy $p \nmid n$, s így a Fermat-tétel 1. alakjából

$$n^{p-1} \equiv 1 \pmod{p},$$

tehát

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

amiből

$$(-1)^{\frac{p-1}{2}} = 1$$

is következik, tehát $\frac{p-1}{2} = 2k$ valamilyen $k \in \mathbb{N}$-re, vagyis $p = 4k + 1$, ami az állításunk volt. ∎

2.7-8. Bizonyítsuk be, hogy ha valamely n egész szám nem osztható 17-tel, akkor $n^8 - 1$ vagy $n^8 + 1$ osztható 17-tel.
Megoldás.

$17 \nmid n$, így a Fermat-tétel első alakja szerint $n^{16} \equiv 1 \pmod{17}$. Írjuk ezt át oszthatósággá: $17 | n^{16} - 1 = (n^8 - 1)(n^8 + 1)$. 17 prímszám, a prímtulajdonság szerint ha osztója egy szorzatnak, akkor valamelyik tényezőnek biztosan osztója. Ez pedig éppen az állítás. ∎

2.7-9. Határozzuk meg 109^{355} 14-gyel való osztási maradékát.
Megoldás. Olyan x értéket keresünk, amelyre $x \equiv 109^{355} \pmod{14}$.

$$109 \equiv 11 \pmod{14}$$

Mindkét oldalt 355-dik hatványra emelve

$$109^{355} \equiv 11^{355} \pmod{14}.$$

$(11, 14) = 1$ és $\varphi(14) = \varphi(2 \cdot 7) = 6$, így alkalmazhatjuk az Euler-tételt: $11^6 \equiv 1 \pmod{14}$. $355 = 6 \cdot 59 + 1$ miatt

$$11^{355} \equiv 11^{6 \cdot 59 + 1} \equiv (11^6)^{59} \cdot 11 \equiv 11 \pmod{14}.$$

Tehát az osztási maradék 11. ∎

2.7-10. Határozzuk meg 293^{275} 48-cal való osztási maradékát.
Megoldás. Olyan x értéket keresünk, amelyre $x \equiv 293^{275} \pmod{48}$. Mivel $293 = 6 \cdot 48 + 5$ és $293 \equiv 5 \pmod{48}$, ezért $x \equiv 5^{275} \pmod{48}$. Kiszámítjuk $\varphi(48)$ értékét.

$$\varphi(48) = \varphi(2^4 \cdot 3) = 8 \cdot 2 = 16$$

Felhasználva, hogy $275 = 16 \cdot 17 + 3$ és $5^{\varphi(48)} = 5^{16} \equiv 1 \pmod{48}$, azt kapjuk, hogy

$$x \equiv 5^{16\cdot 17+3} \equiv (5^{16})^{17} \cdot 5^3 \equiv 5^3 = 125 \equiv 29 \pmod{48}.$$

Eszerint az osztási maradék 29. ∎

2.7-11. Mi a $39^{39^{390}}$ szám utolsó két számjegye a tízes számrendszerben?
Megoldás. Olyan x értéket keresünk, amelyre $x \equiv 39^{39^{390}} \pmod{100}$. Mivel $(39, 100) = 1$, alkalmazható az Euler-tétel: $39^{\varphi(100)} = 1$.

$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2 \cdot 20 = 40$ miatt a kitevő 40-nel való osztási maradékát kell megkeresnünk, vagyis az $y \equiv 39^{390} \pmod{40}$ kongruenciát kell megoldanunk. $39 \equiv -1 \pmod{40}$, ezért $39^{390} \equiv (-1)^{390} \equiv 1 \pmod{40}$, és így $39^{39^{390}} \equiv 39 \pmod{100}$. ∎

2.7-12. Lássuk be, hogy ha $(a, 10) = 1$, akkor

$$a^{100n+1} \equiv a \pmod{1000},$$

ahol n természetes szám.
Megoldás.

Mivel $\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3) \cdot \varphi(5^3) = 4 \cdot 100 = 400$, az Euler-tételből csupán

$$a^{400} \equiv 1 \pmod{1000},$$

illetve n-edik hatványra emelve és a-val szorozva

$$a^{400n+1} \equiv a \pmod{1000}$$

következik. Más módon kell megtalálnunk a megoldást. Be fogjuk látni, hogy a kongruencia fennáll modulo 8 és modulo 125, így fennáll modulo $8 \cdot 125 = 1000$ is. Egyrészt

$$a^{\varphi(8)} = a^4 \equiv 1 \pmod{8},$$

ebből $a^{100} \equiv 1 \pmod 8$, s így

$$a^{100n+1} \equiv a \pmod 8. \tag{1}$$

Másrészt

$$a^{\varphi(125)} = a^{100} \equiv 1 \pmod{125},$$

amiből

$$a^{100n+1} \equiv a \pmod{125}. \tag{2}$$

Mivel 8 és 25 relatív prímek, ezért (1)-ből és (2)-ből következik az állítás. ■

2.7-13. Bizonyítsuk be, hogy

$$2^{19\cdot 73-1} \equiv 1 \pmod{19\cdot 73}.$$

Megoldás. 19 és 73 prímek, így a megoldás során alkalmazhatjuk a Fermat-tételt. Egyrészt:

$$2^{19\cdot 73-1} = 2^{18\cdot 73}\cdot 2^{72} = (2^{18})^{73}\cdot 2^{72} \equiv 2^{72} = (2^{18})^4 \equiv 1 \pmod{19}$$

Másrészt:

$$2^{19\cdot 73-1} = 2^{19\cdot 72+18} = (2^{72})^{19}\cdot 2^{18} \equiv 2^{18} = 64^3 \equiv (-9)^3 =$$

$$= -81\cdot 9 \equiv -72 \equiv 1 \pmod{73}$$

Mivel $(19, 73) = 1$, a kongruencia modulo $19\cdot 73$ is fennáll. ■

2.7-14. Melyek azok a p prímek, amelyekre

$$5^{p^2} + 1 \equiv 0 \pmod{p^2}? \tag{1}$$

Megoldás. $p \neq 5$, mert (1)-ből $5|1$ következne, ami nem lehetséges. Végezzük el a következő átalakítást.

$$5^{p^2} + 1 = 5(5^{p^2-1}) - 5 + 6 = 5((5^{p-1})^{p+1} - 1) + 6 \equiv 0 \pmod{p^2} \tag{2}$$

(2) modulo p is fennáll, a Fermat-tétel szerint pedig $5^{p-1} \equiv 1 \pmod p$, így (2)-ből $6 \equiv 0 \pmod p$ következik. Ez $p = 2$ vagy $p = 3$ esetén lehetséges. $p = 2$ nem lehet, mert $5^4+1 \not\equiv 0 \pmod 4$, vagyis $626 \not\equiv 0 \pmod 4$. Vizsgáljuk meg a $p = 3$ esetet.

$$5^9 + 1 \equiv 5\cdot 625^2 + 1 \equiv 5\cdot 4^2 + 1 = 5\cdot 16 + 1 \equiv 81 \equiv 0 \pmod 9$$

Tehát $p = 3$ az egyetlen megoldása a kongruenciának. ■

2.7-15. Határozzuk meg a 439^{291} szám osztási maradékát 60-nal.
Megoldás. Olyan x értéket keresünk, amelyre $x \equiv 439^{291} \pmod{60}$.

$$439 \equiv 19 \pmod{60}$$

$$439^{291} \equiv 19^{291} \pmod{60}$$

Mivel $\varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = 2 \cdot 2 \cdot 4 = 16$ és $(19, 60) = 1$, az Euler-tétel szerint $19^{16} \equiv 1 \pmod{60}$. Ezt felhasználva:

$$19^{291} = 19^{16 \cdot 18 + 3} = (19^{16})^{18} \cdot 19^3 \equiv 19^3 = 19 \cdot 361 \equiv 19 \pmod{60}$$

Az osztási maradék 19. ■

2.7-16. Lássuk be, hogy ha p és q különböző prímszámok, akkor

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{p \cdot q}.$$

Megoldás. A Fermat-tétel szerint $q^{p-1} \equiv 1 \pmod{p}$. Nyilván $p^{q-1} \equiv 0 \pmod{p}$ is fennáll. A két kongruenciát összeadva kapjuk, hogy

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Hasonlóan juthatunk el a

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{q} \tag{2}$$

kongruenciához. Mivel $(p, q) = 1$, (1)-ből és (2)-ből következik, hogy

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{p \cdot q},$$

ami maga az állítás. ■

2.8. Lineáris kongruenciák

Legyenek a, b egész számok. Az

$$ax \equiv b \pmod{m} \tag{I}$$

alakú kongruenciát *egyismeretlenes lineáris kongruenciának* nevezzük, és olyan x egész értékeket keresünk, melyek kielégítik. Ha x_1 egész szám kielégíti (I)-et, és $x_2 \equiv x_1 \pmod{m}$, akkor x_2 is kielégíti (I)-et. Tehát ha van megoldása

(I)-nek, akkor végtelen sok egész szám van, amelyek szintén megoldást adnak, tudniillik a vele egy maradékosztályban levők. Ez indokolja azt, hogy a megoldások számánál a maradékosztályokat vegyük figyelembe. Az (I) *kongruencia megoldásszáma* a kongruenciát kielégítő elemek maradékosztályainak a száma.

1. tétel. Az $ax \equiv b \pmod m$ kongruencia megoldhatóságának szükséges és elégséges feltétele az, hogy $(a,m)|b$ teljesüljön. Ha a kongruencia megoldható, akkor megoldásainak a száma (a,m).

Bizonyítás.

I. A feltétel szükséges. Ha ugyanis x_0 megoldása az (I) kongruenciának, akkor $ax_0 \equiv b \pmod m$ miatt $m|ax_0 - b$, s így létezik olyan q egész szám, amellyel $mq = ax_0 - b$. Így $b = ax_0 - mq$, amiből leolvasható, hogy $(a,m)|b$.

II. Tegyük fel, hogy $(a,m)|b$.

1. Nézzük először az $(a,m) = 1$ esetet. Legyen a_0, a_1, ..., a_{m-1} modulo m teljes maradékrendszer. Az omnibusztétel szerint (lásd az előző fejezetet) aa_0, aa_1, ..., aa_{m-1} modulo m is teljes maradékrendszer, következésképpen pontosan egy olyan elem van közöttük, amelyik kongruens b-vel. Legyen ez az aa_i, ami $aa_i \equiv b \pmod m$ miatt megoldása (I)-nek, s ez az egyetlen megoldás.

2. Nézzük most az $(a,m) > 1$ esetet. Az

$$ax \equiv b \pmod m \tag{II}$$

és az

$$\frac{a}{(a,m)}x \equiv \frac{b}{(a,m)} \pmod{\frac{m}{(a,m)}} \tag{III}$$

kongruenciákat pontosan ugyanazok az egész számok elégítik ki.

Ezek után csupán azt kell megvizsgálnunk, hogy a modulo $\frac{m}{(a,m)}$ egyetlen maradékosztályt alkotó megoldások hány különböző maradékosztályt jelentenek modulo m.

Legyen x_0 megoldása (III)-nak, s így (II)-nek is. Ekkor

$$x_0, \quad x_0 + \frac{m}{(a,m)}, \quad x_0 + 2\frac{m}{(a,m)}, \quad \ldots, \quad x_0 + ((a,m)-1)\frac{m}{(a,m)}$$

mind különböző maradékosztályba esnek modulo m, a többi $\overline{x_0}$ $(\text{mod } \frac{m}{(a,m)})$-beli elem azonban az előbb felsoroltak valamelyikével kongruens lesz modulo m.

Ezek szerint (II)-nek (a,m) darab olyan megoldását kapjuk, melyek inkongruensek modulo m, tehát (a,m) különböző megoldása van. ∎

2. tétel. Ha $(a,m) = 1$, akkor az $ax \equiv b \pmod m$ kongruenciának az egyetlen megoldása az $x_0 \equiv a^{\varphi(m)-1}b \pmod m$ számnak megfelelő maradékosztály.

Bizonyítás. Azt az állítást, mely szerint a fenti kongruenciának pontosan egy megoldása van, már beláttuk az előző tételben. Tegyük fel, hogy x_0 megoldás. Ekkor

$$ax_0 \equiv b \pmod{m}.$$

Beszorozva $a^{\varphi(m)-1}$-nel

$$a^{\varphi(m)}x_0 \equiv a^{\varphi(m)-1}b \pmod{m}$$

Mivel $(a, m) = 1$, ezért az Euler-féle kongruenciatétel szerint $m|a^{\varphi(m)} - 1$, így kongruenciánk bal oldala az alábbiak szerint alakul:

$$a^{\varphi(m)}x_0 = x_0 + \left(a^{\varphi(m)} - 1\right) x_0 \equiv x_0 \pmod{m},$$

s így $x_0 \equiv a^{\varphi(m)-1}b$ a megoldás. ∎

Kongruenciák megoldásának menete

Az

$$ax \equiv b \pmod{m}$$

kongruencia akkor és csak akkor oldható meg, ha $d = (a, m)|b$. Áttérünk az

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

kongruenciára. Az egyetlen megoldást jelölje x_0. Az eredeti kongruencia megoldásai:

$$x_t \equiv x_0 + t\frac{m}{d}, \quad 0 \le t \le d - 1$$

Megoldás során a kongruencia mindkét oldalát oszthatjuk a modulushoz relatív prím számmal, bármelyik együtthatót helyettesíthetjük egy vele kongruens számmal, például a modulus konstansszorosát hozzáadhatjuk az egyik oldalhoz (a modulus a 0 maradékosztályt képviseli). Lásd a kongruenciák műveleti tulajdonságait az előző fejezetben.

Lineáris diofantikus egyenletek és lineáris kongruenciák kapcsolata

A korábban tárgyalt lineáris diofantikus egyenletek és a lineáris kongruenciák között szoros kapcsolat van. Legyen ugyanis x_0 az $ax \equiv b \pmod{m}$ kongruencia megoldása. Ekkor $m|b - ax_0$, vagyis létezik olyan y_0 egész, melyre $my_0 = b - ax_0$, így

$$ax_0 + my_0 = b, \tag{IV}$$

tehát x_0, y_0 az a, m, b együtthatós lineáris diofantikus egyenlet egyik megoldása.

Okoskodásunkat visszafelé alkalmazva látható, hogy a (IV) alakú diofantikus egyenlet megoldása az $ax \equiv b \pmod{m}$ kongruencia megoldását is szolgáltatja.

Ezek szerint a diofantikus egyenletek megoldhatók a kongruenciák segítségével, és fordítva, a lineáris kongruenciákat meg lehet oldani a diofantikus egyenletek megoldására alkalmas módszerekkel is.

Példák

Oldjuk meg az alábbi kongruenciákat

2.8-1. $21x \equiv 14 \pmod{35}$
Megoldás. Mivel $(21, 35) = 7|14$, ezért megoldható a kongruencia, és 7 különböző megoldása van. Ezek egyikét – miután a kongruenciát 7-tel elosztottuk – a

$$3x \equiv 2 \pmod{5}$$

kongruenciából kapjuk.

$$\begin{aligned} x_0 &\equiv 3^{\varphi(5)-1} \cdot 2 \pmod{5} \\ x_0 &\equiv 3^3 \cdot 2 \pmod{5} \\ x_0 &\equiv 54 \pmod{5} \\ x_0 &\equiv 4 \pmod{5} \end{aligned}$$

Tehát a $\overline{4} \pmod{5}$ maradékosztály lesz a megoldása $3x \equiv 2 \pmod{5}$-nek. Egy másik lehetőség ennek az egyszerűsített kongruenciának a megoldására a következő.

$$3x \equiv 2 \pmod{5}$$

A jobb oldalból 5-öt kivonunk.

$$3x \equiv 2 - 5 = -3 \pmod{5}$$

Mindkét oldalt 3-mal osztjuk. $(3, 5) = 1$, így a modulus változatlan marad.

$$\begin{aligned} x &\equiv -1 \pmod{5} \\ x_0 &\equiv 4 \pmod{5} \end{aligned}$$

Az eredeti kongruencia megoldása a következő hét maradékosztály lesz:

$$\overline{4},\ \overline{9},\ \overline{14},\ \overline{19},\ \overline{24},\ \overline{29},\ \overline{34} \pmod{35}$$

■

2.8-2. $172x \equiv 6 \pmod{62}$
Megoldás. $\mathrm{lnko}(172, 62) = 2|6$, így a kongruencia megoldható, és két maradékosztály elemei adják a megoldást. Osszuk el az egyenletet – a modulust is – a legnagyobb közös osztóval, ekkor a következőt kapjuk:

$$86x \equiv 3 \pmod{31}$$

86-ot a vele kongruens 24-gyel helyettesítjük.

$$24x \equiv 3 \pmod{31}$$

3-mal osztunk. $(3, 31) = 1$, így a modulus változatlan marad.

$$8x \equiv 1 \pmod{31}$$

A jobb oldalhoz 31-et adunk hozzá.

$$8x \equiv 32 \pmod{31}$$

8-cal osztunk.

$$x \equiv 4 \pmod{31}$$

A megoldást a $\overline{4} \pmod{62}$ és a $\overline{35} \pmod{62}$ maradékosztályokban lévő számok adják. ■

2.8-3. $3x \equiv 8 \pmod{13}$
Megoldás. $(3, 13) = 1$, így a kongruencia megoldható, és egyetlen maradékosztály elemei adják a megoldást.

$$3x \equiv 8 \pmod{13}$$

A jobb oldalhoz adjunk 13-mat.

$$3x \equiv 21 \pmod{13}$$

3-mal osztunk.

$$x \equiv 7 \pmod{13}$$

■

2.8-4. $12x \equiv 9 \pmod{15}$
Megoldás. $(12, 15) = 3|9$, a kongruencia megoldható, 3-mal osztjuk a kongruenciát, a modulust is.

$$4x \equiv 3 \pmod{5}$$

A jobb oldalhoz hozzáadjuk a modulus értékét, 5-öt.

$$4x \equiv 8 \pmod 5$$

$$x \equiv 2 \pmod 5$$

Ebből $x_0 \equiv 2 \pmod 5$ és $x_t \equiv 2{+}5{\cdot}t \pmod 5$, $0 \le t < 3$. A $\overline{2}, \overline{7}, \overline{12} \pmod{15}$ maradékosztályok elemei adják a megoldást. ■

2.8-5. $12x \equiv 9 \pmod{18}$

Megoldás. $(12, 18) = 6 \nmid 9$, s így a kongruenciának nincs megoldása. ■

2.8-6. $20x \equiv 10 \pmod{25}$
Megoldás. $(20, 25) = 5|10$, a kongruencia megoldható, 5-tel osztjuk a kongruenciát, a modulust is.

$$4x \equiv 2 \pmod 5$$

$2 \cdot 5$-öt hozzáadunk a jobb oldalhoz.

$$4x \equiv 12 \pmod 5$$

4-gyel osztunk.

$$x \equiv 3 \pmod 5$$

A $\overline{3}, \overline{8}, \overline{13}, \overline{18}, \overline{23} \pmod{25}$ maradékosztályok elemei adják a megoldást. ■

2.8-7. $10x \equiv 25 \pmod{35}$
Megoldás. $(10, 35) = 5|25$, a kongruencia megoldható, 5-tel osztjuk a kongruenciát, a modulust is.

$$2x \equiv 5 \pmod 7$$

A jobb oldalhoz 7-et adunk.

$$2x \equiv 12 \pmod 7$$

2-vel osztunk.

$$x \equiv 6 \pmod 7$$

Az eredeti kongruencia megoldása $x \equiv 6,\ 13,\ 20,\ 27,\ 34 \pmod{35}$, tehát a $\overline{6}, \overline{13}, \overline{20}, \overline{27}, \overline{34} \pmod{35}$ maradékosztályok elemei adják a megoldást. ■

2.8-8. $90x + 18 \equiv 0 \pmod{138}$
Megoldás. $90 = 2 \cdot 3^2 \cdot 5,\ 138 = 2 \cdot 3 \cdot 23,\ (90, 138) = 6|18$, a kongruencia megoldható.

$$90x \equiv -18 \pmod{138}$$

6-tal osztjuk a kongruenciát, a modulust is.

$$15x \equiv -3 \pmod{23}$$

3-mal osztjuk mindkét oldalt.

$$\begin{aligned} 5x &\equiv -1 \pmod{23} \\ 5x &\equiv -1 + 46 = 45 \pmod{23} \\ x &\equiv 9 \pmod{23} \end{aligned}$$

A $\overline{9},\ \overline{32},\ \overline{55},\ \overline{78},\ \overline{101},\ \overline{124} \pmod{138}$ maradékosztályok elemei adják a megoldást. ■

2.8-9. Tegyük fel, hogy $a^{100} \equiv 2 \pmod{73}$ és $a^{101} \equiv 69 \pmod{73}$. Határozzuk meg a-nak a 73-mal történő osztáskor keletkező legkisebb nemnegatív osztási maradékát.
Megoldás. Keressük az $x \equiv a \pmod{73}$ kongruencia megoldását.

$$a^{100} \equiv 2 \pmod{73}$$

a-val szorozva mindkét oldalt:

$$\begin{aligned} a^{101} &\equiv 2a \equiv 69 \pmod{73} \\ 2a &\equiv 69 \pmod{73} \\ 2a &\equiv 69 + 73 = 142 \pmod{73} \\ a &\equiv 71 \pmod{73} \end{aligned}$$

■

Keressük meg a következő egyenletek egész megoldásait kongruenciák felhasználásával

2.8-10. $84x + 37y = 2$
Megoldás. $(84, 37) = 1|2$, ezért a diofantikus egyenlet megoldható. Áttérünk a következő kongruenciára. (Ugyanígy dolgozhatnánk a $37y \equiv 2 \pmod{84}$

kongruenciával is, a következő – kisebb modulusú – könnyebben kezelhető, esetünkben ez a jobb választás.)

$$84x \equiv 2 \pmod{37}$$

84-et a vele kongruens 10-zel helyettesítjük.

$$10x \equiv 2 \pmod{37}$$

2-vel osztunk.

$$5x \equiv 1 \pmod{37}$$

A jobb oldalhoz $2 \cdot 37$-et adunk.

$$5x \equiv 75 \pmod{37}$$

5-tel osztunk.

$$x \equiv 15 \pmod{37}$$

$x = 15 + 37t,\ t \in \mathbb{Z}, \quad y = \frac{2-84x}{37} = \frac{2-84(15+37t)}{37} = -34 - 84t.$

Az $x = 15+37t, y = -34-84t,\ t \in \mathbb{Z}$ számpárok adják a diofantikus egyenlet megoldásait. ■

2.8-11. $41x + 30y = 3$
Megoldás. $(41, 30) = 1|3$, ezért a diofantikus egyenlet megoldható. Áttérünk a következő kongruenciára.

$$41x \equiv 3 \pmod{30}$$

41-et a vele kongruens 11-gyel helyettesítjük.

$$11x \equiv 3 \pmod{30}$$

A jobb oldalhoz 30-at adunk.

$$11x \equiv 33 \pmod{30}$$

11-gyel osztunk.

$$x \equiv 3 \pmod{30}$$

$x = 3 + 30t,\ t \in \mathbb{Z}, \quad y = \frac{3-41x}{30} = \frac{3-41(3+30t)}{30} = -4 - 41t.$

Az $x = 3+30t,\ y = -4-41t,\ t \in \mathbb{Z}$ számpárok alkotják a diofantikus egyenlet megoldásait. ■

2.8-12. Pajkos százlábúak futkároznak a ládában. Az egyik fajtának

14 lába van, a másiknak 20. Kölyök (alias Gorcsev Iván) összesen 232 lábat számolt meg. Hány százlábú van a ládában?
Megoldás. Legyen x 14 lábú és y 20 lábú. A következő diofantikus egyenletet kell megoldanunk.

$$14x + 20y = 232$$

Alakítsuk kongruenciává az egyenletet.

$$20y \equiv 232 \pmod{14}$$

$(20, 14) = 2|232$, tehát megoldható a kongruencia. Osszuk el 2-vel.

$$\begin{aligned} 10y &\equiv 116 \pmod 7 \\ 3y &\equiv 4 \equiv -3 \pmod 7 \\ y &\equiv -1 \equiv 6 \pmod 7 \end{aligned}$$

A kongruenciát az $y = 6 + 7t, \quad t \in \mathbb{Z}$ számok elégítik ki. Ezt írjuk vissza az eredeti egyenletbe.

$$x = \frac{232 - 20y}{14} = \frac{232 - 20(6 + 7t)}{14} = 8 - 10t$$

A diofantikus egyenlet megoldása $x = 8 - 10t, \ y = 6 + 7t, \quad t \in \mathbb{Z}$. Csak $t = 0$ esetén lesz mindkét érték pozitív, így a feladat megoldása $x = 8, y = 6$ felhasználásával $8 + 6 = 14$. 14 százlábú szaladgál a ládában. ■

2.8-13. Bontsuk fel 463-at két természetes szám összegére úgy, hogy az egyik szám osztható legyen 14-gyel, a másik 23-mal. Oldjuk meg a feladatot kongruenciák segítségével.
Megoldás. A következő egyenletet kell megoldanunk:

$$14x + 23y = 463$$

Áttérünk kongruenciára.

$$\begin{aligned} 23y &\equiv 463 \pmod{14} \\ 9y &\equiv 1 \pmod{14} \end{aligned}$$

A jobb oldalból kivonunk $2 \cdot 14$-et.

$$9y \equiv -27 \pmod{14}$$

9-cel osztunk.

$$\begin{aligned} y &\equiv -3 \pmod{14} \\ y &\equiv 11 \pmod{14} \end{aligned}$$

A diofantikus egyenlet megoldása:

$$y = 11 + 14k,\ k \in \mathbb{Z}, \quad x = \frac{463 - 23(11 + 14k)}{14} = 15 - 23k.$$

x és y egyszerre csak $k = 0$ esetén lesz pozitív. A feladat megoldása:

$$14x = 14 \cdot 15 = 210 \text{ és } 23y = 23 \cdot 11 = 253.$$

■

2.9. Lineáris kongruencia-rendszerek, a kínai maradéktétel

Ebben a fejezetben lineáris kongruenciák közös megoldását keressük. Legyen

$$n \in \mathbb{N}, \quad m_1,\ m_2,\ \ldots,\ m_n \in \mathbb{N},\ a_i, b_i \in \mathbb{Z} \quad (1 \le i \le n).$$

Az

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\ \vdots \\ a_nx &\equiv b_n \pmod{m_n} \end{aligned} \tag{I}$$

kongruencia-rendszer *szimultán megoldása* az x_0 egész szám, ha egyszerre kielégíti az (I)-beli összes kongruenciát.

Egy szimultán kongruencia-rendszer nyilván csak akkor oldható meg, ha minden egyes kongruencia külön-külön megoldható. Legyen $c_1,\ c_2,\ \ldots,\ c_n$ rendre a kongruenciák megoldása. Elegendő tehát az alábbi kongruencia-rendszert vizsgálni:

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\ \vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned} \tag{II}$$

Ha külön-külön van is az (I)-beli kongruenciáknak megoldása, ez nem feltétlenül jár azzal, hogy létezik szimultán megoldás.

Például az

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 4 \end{aligned}$$

kongruenciák külön-külön megoldhatóak (a felírás maga már szolgáltatja is a megoldást), szimultán megoldása a rendszernek nyilván nincs.

Vizsgáljuk először a két kongruenciából álló rendszereket.

1. tétel.

I. Az

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned} \tag{III}$$

szimultán kongruencia-rendszer akkor és csak akkor oldható meg, ha

$$(m_1, m_2) | c_1 - c_2.$$

II. Ha megoldható a rendszer, akkor a megoldás egy maradékosztályt alkot modulo $[m_1, m_2]$.

Bizonyítás. I. (III) átírható az

$$x = c_1 + z_1 m_1, \quad x = c_2 + z_2 m_2, \quad z_1,\ z_2 \in \mathbb{Z}$$

alakba, amiből

$$c_1 + z_1 m_1 = c_2 + z_2 m_2,$$

illetve

$$c_1 - c_2 = z_2 m_2 - z_1 m_1. \tag{IV}$$

A (III) kongruencia-rendszer a (IV) lineáris diofantikus egyenlettel ekvivalens. Ez utóbbi megoldhatóságának szükséges és elégséges feltétele

$$(m_1, m_2) | c_1 - c_2.$$

(Lásd a 2.5. fejezetet.)

II. bizonyításához gondoljuk meg a következőket. Legyen r egy megoldás, vagyis

$$r \equiv c_1 \pmod{m_1} \quad \text{és} \quad r \equiv c_2 \pmod{m_2}.$$

Valamely s egész szám akkor és csak akkor megoldás, ha

$$s \equiv c_1 \pmod{m_1} \quad \text{és} \quad s \equiv c_2 \pmod{m_2},$$

vagyis

$$r \equiv s \pmod{m_1} \quad \text{és} \quad r \equiv s \pmod{m_2}.$$

Ebből

$$m_1 | r - s \quad \text{és} \quad m_2 | r - s.$$

Ez utóbbi pedig azzal ekvivalens, hogy $[m_1, m_2] | r - s$, tehát

$$r \equiv s \pmod{[m_1, m_2]}.$$

■

2. tétel. Az

$$\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\vdots \\ x &\equiv c_n \pmod{m_n} \end{aligned}$$

szimultán kongruencia-rendszer akkor és csak akkor oldható meg, ha

$$\text{minden } 1 \le i < j \le k \quad \text{esetén} \quad (m_i, m_j) | c_i - c_j$$

teljesül. •

A kérdést nem fogjuk teljes egészében tárgyalni, csupán egy speciális esetet nézünk. Az alábbi tétel azért kapta a kínai maradéktétel nevet, mert Sun Tsu, a Kr. u. I. században élt kínai matematikus munkáiban már megtalálható.

3. tétel. (Kínai maradéktétel) Tekintsük az (I) kongruencia-rendszert, és legyen

$$(a_i, m_i) = 1 \quad (i = 1, ..., n),$$

valamint

$$(m_i, m_j) = 1 \quad (i \ne j, \quad 1 \le i, j \le n).$$

Ekkor az (I) kongruencia-rendszernek van megoldása, s a megoldások egyetlen maradékosztályba esnek modulo m, ahol $m = m_1 \cdot m_2 \cdots m_n$.

Bizonyítás. A feltétel szerint az $a_i x \equiv b_i \pmod{m_i}$ kongruencia mindegyik i-re megoldható, hiszen $(a_i, m_i) = 1 | b_i$. Tudjuk, hogy egy megoldást ad a $c_i = a_i^{\varphi(m_i)-1} b_i$.

Ezekkel a c_i értékekkel a (II) egyenletrendszerhez jutunk, amelyik ekvivalens az (I) alattival.

A továbbiakban (II) megoldását keressük. Vezessük be az

$$M_j = \frac{m}{m_j} = m_1 \cdot m_2 \cdots m_{j-1} \cdot m_{j+1} \cdots m_n \quad (1 \le j \le n)$$

jelölést, és nézzük az

$$\begin{aligned} M_1 y &\equiv 1 \pmod{m_1} \\ M_2 y &\equiv 1 \pmod{m_2} \\ &\vdots \\ M_n y &\equiv 1 \pmod{m_n} \end{aligned} \tag{V}$$

kongruenciákat.

Ezek külön-külön megoldhatóak, mert $(M_i, m_i) = 1 \quad (1 \le j \le n)$. Jelöljük a kongruenciák megoldását sorban $y_1, y_2, \ldots, y_n$-nel, és a segítségükkel fogjuk előállítani (II) megoldását. Legyen ugyanis

$$x_0 = M_1 y_1 c_1 + M_2 y_2 c_2 + \ldots + M_n y_n c_n.$$

1. Először azt mutatjuk meg, hogy x_0 megoldása (II)-nek. Helyettesítsük be x_0-at az i-edik egyenletbe $(1 \le j \le n)$. Ekkor

$$x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + \ldots + M_n y_n c_n \equiv M_i y_i c_i \pmod{m_i},$$

hiszen M_i kivételével a többi M_j osztható m_i-vel, tehát a megfelelő tagok 0-val lesznek kongruensek modulo m_i. De $M_i y_i c_i \equiv c_i \pmod{m_i}$, mivel y_i az (V)-beli i-edik egyenlet megoldása volt. Ezért

$$x_0 \equiv c_i \pmod{m_i} \quad (1 \le i \le n);$$

x_0 tehát sorban kielégíti a (II)-beli egyenleteket, és így szimultán megoldás.

2. Most lássuk be azt, hogy az $\overline{x}_0 \pmod{m}$ maradékosztályban lévő elemek mind megoldásai (II)-nek. Legyen

$$x_1 \equiv x_0 \pmod{m},$$

vagyis

$$m | x_1 - x_0.$$

De ekkor

$$m_i | x_1 - x_0 \quad (1 \le i \le n),$$

s így

$$x_1 \equiv x_0 \pmod{m_i} \quad (1 \le i \le n),$$

tehát x_1 is kielégíti (II) mindegyik egyenletét.

3. Hátra van még annak a belátása, hogy minden megoldás ugyanabba az egyetlen maradékosztályba esik modulo m.

Tegyük fel, hogy x_0 és x_1 megoldásai (II)-nek, s így

$$x_1 \equiv x_0 \pmod{m_i} \quad \text{minden } i\text{-re } (1 \le i \le n).$$

Ebből

$$m_i | x_1 - x_0 \quad \text{minden } i\text{-re } (1 \le i \le n).$$

De

$$(m_i, m_j) = 1 \quad (i \ne j)$$

miatt

$$m | x_1 - x_0,$$

s így

$$x_1 \equiv x_0 \pmod{m}$$

is teljesül. ■

Összetett modulusú kongruenciák megoldása

A kínai maradéktételből következik, hogy tetszőleges összetett szám modulusú kongruencia visszavezethető prímhatvány modulusú kongruenciákra.

Legyen ugyanis $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ az m szám kanonikus alakja, és keressük az

$$f(x) \equiv 0 \pmod{m} \tag{VI}$$

kongruencia megoldását. Ez ekvivalens az

$$\begin{aligned} f(x) &\equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) &\equiv 0 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ f(x) &\equiv 0 \pmod{p_k^{\alpha_k}} \end{aligned} \tag{VII}$$

szimultán kongruencia-rendszerrel. A (VII) rendszerben minden kongruenciát külön-külön megoldunk. Ha valamelyiknek nincs megoldása, akkor (VI) sem oldható meg. Ha mindegyik megoldható, és $c_1,\ c_2\ \dots\ c_k$ egy-egy megoldás, akkor az

$$\begin{aligned} x &\equiv c_1 \pmod{p_1^{\alpha_1}} \\ x &\equiv c_2 \pmod{p_2^{\alpha_2}} \\ &\vdots \\ x &\equiv c_k \pmod{p_k^{\alpha_k}} \end{aligned}$$

szimultán kongruencia-rendszert kell megoldanunk, így megkapjuk (VI) egyik megoldását. Az összes megoldást megkapjuk, ha $c_1,\ c_2\ \dots\ c_k$ végigfut (VII) minden lehetséges megoldásrendszerén.

Maradékszámrendszerek

A kínai maradéktétel számítástechnikai alkalmazása az úgynevezett *maradékszámrendszerekkel* történő műveletvégzés. Sok olyan művelet van, amelyet egész számok összeadásának, szorzásának sorozatából épít fel a számítógép. Fontos, hogy ezeket a műveleteket lehetőleg gyorsan el lehessen végezni.

Tegyük fel, hogy a számolás során egy bizonyos A értéknél kisebb abszolút értékű egészek fordulnak csak elő. Ez nem jelent megszorítást, hiszen minden számítógép csak egy bizonyos korlátig képes a számokat ábrázolni. Legyen $m = p_1 p_2 \dots p_k$ az első k darab pozitív prímszám szorzata, ahol k-t úgy választjuk meg, hogy $m > 2A$ teljesüljön. Ezzel elérjük, hogy egy A-nál kisebb abszolút értékű egész szám megegyezzen a modulo m legkisebb abszolút értékű maradékával. Tekintsük az illető szám modulo p_i maradékainak rendszerét, ezek lesznek a szám számjegyei maradékszámrendszerben.

A számjegyek lényegében egy szimultán kongruencia-rendszert jelentenek, ahol a p_i modulusok páronként relatív prímek, s ezért ezekből a szám modulo m maradéka egyértelműen előállítható, ami jelen esetben maga a szám. Két szám összeadásakor vagy szorzásakor a megfelelő maradékokat, vagyis a számjegyeket kell összeadni, illetve szorozni, majd az így kapott modulo p_i maradékok rendszeréből kell a modulo m maradékot meghatározni. Több művelet esetén csak a végén érdemes visszaváltani.

Lényeges előnye a módszernek, hogy a műveletek számjegyenként külön végezhetők, ami egy n pozitív egész szám alapú számrendszer esetében nem tehető meg az átvitelek miatt. Ha több párhuzamos processzor áll rendelkezésre, akkor ez a módszer jól használható.

Példák

2.9-1. Oldjuk meg a következő kongruencia-rendszert:

$$5x \equiv 3 \pmod 7$$
$$3x \equiv 7 \pmod 8$$

Megoldás. Az első kongruencia a következő alakban írható:

$$5x \equiv 3 \pmod 7$$
$$5x \equiv 10 \pmod 7$$
$$x \equiv 2 \pmod 7$$

Tehát az
$$x = 2 + 7t \quad t \in \mathbb{Z} \tag{1}$$
számok alkotják a megoldást. Ezt helyettesítsük be a második kongruenciába, és rendezzük, majd oldjuk meg.

$$\begin{aligned} 3(2+7t) &\equiv 7 \pmod 8 \\ 21t &\equiv 1 \pmod 8 \\ -3t &\equiv 9 \pmod 8 \\ t &\equiv -3 \pmod 8 \\ t &\equiv 5 \pmod 8 \end{aligned}$$

A $t = 5 + 8s \quad s \in \mathbb{Z}$ számok alkotják ennek a megoldását. Ezt visszahelyettesítve (1)-be:
$$x = 2 + 7(5+8s) = 37 + 56s \quad s \in \mathbb{Z}$$

Az összes megoldás tehát $\overline{37} \pmod{56}$. Figyeljük meg, hogy $56 = \mathrm{lkkt}(7,8)$.

∎

2.9-2. Oldjuk meg az

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 1 \pmod 5 \end{aligned}$$

kongruencia-rendszert a kínai maradéktétel segítségével.
Megoldás. A kínai maradéktétel feltételei teljesülnek, így alkalmazhatjuk a módszert. A tétel jelöléseit használva

$$m = 3 \cdot 4 \cdot 5 = 60, \qquad M_1 = 20, \qquad M_2 = 15, \qquad M_3 = 12,$$

ami az alábbi kongruenciák egyenkénti megoldásához vezet:

$$\begin{array}{rcl} 20y &\equiv& 1 \pmod 3 \\ 20y &\equiv& 1 - 21 \pmod 3 \\ 20y &\equiv& -20 \pmod 3 \\ y &\equiv& -1 \pmod 3 \\ y &\equiv& 2 \pmod 3 \\ y_1 &=& 2 \end{array} \qquad \begin{array}{rcl} 15y &\equiv& 1 \pmod 4 \\ 15y &\equiv& 1 - 16 \pmod 4 \\ 15y &\equiv& -15 \pmod 4 \\ y &\equiv& -1 \pmod 4 \\ y &\equiv& 3 \pmod 4 \\ y_2 &=& 3 \end{array}$$

$$\begin{aligned}
12y &\equiv 1 \pmod 5\\
12y &\equiv 1-21 \pmod 5\\
12y &\equiv -24 \pmod 5\\
y &\equiv -2 \pmod 5\\
y &\equiv 3 \pmod 5\\
y_3 &= 3
\end{aligned}$$

A kapott y_i értékek segítségével előállítandó x_0 megoldást modulo 60 vesszük.

$$x_0 \equiv M_1y_1c_1 + M_2y_2c_2 + M_3y_3c_3 \equiv 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 1 \equiv$$
$$\equiv 80 + 135 + 36 \equiv 20 + 15 + 36 \equiv 71 \equiv 11 \pmod{60}$$

Visszahelyettesítve, valóban $11 \equiv 2 \pmod 3$, $11 \equiv 3 \pmod 4$ és $11 \equiv 1 \pmod 5$. A szimultán rendszer megoldása $\overline{11} \pmod{60}$. ■

2.9-3. Oldjuk meg a következő kongruencia-rendszert a kínai maradéktétel segítségével:

$$\begin{aligned}
4x &\equiv 2 \pmod 3\\
3x &\equiv 2 \pmod 7\\
9x &\equiv 7 \pmod{11}
\end{aligned}$$

Megoldás. A kínai maradéktétel feltételei teljesülnek, így alkalmazhatjuk a módszert. Először megoldjuk külön-külön a kongruenciákat.

$$\begin{aligned}
4x &\equiv 2 \pmod 3 & 3x &\equiv 2 \pmod 7 & 9x &\equiv 7 \pmod{11}\\
2x &\equiv 1 \pmod 3 & 3x &\equiv 9 \pmod 7 & 9x &\equiv 18 \pmod{11}\\
2x &\equiv 4 \pmod 3 & x &\equiv 3 \pmod 7 & x &\equiv 2 \pmod{11}\\
x &\equiv 2 \pmod 3 & & & &
\end{aligned}$$

$$m = 3 \cdot 7 \cdot 11 = 231, \qquad M_1 = 77, \qquad M_2 = 33, \qquad M_3 = 21,$$

ami az alábbi kongruenciák egyenkénti megoldásához vezet:

$$\begin{aligned}
77y &\equiv 1 \pmod 3 & 33y &\equiv 1 \pmod 7\\
2y &\equiv 1 \pmod 3 & 5y &\equiv 1 \pmod 7\\
2y &\equiv 4 \pmod 3 & 5y &\equiv -20 \pmod 7\\
y &\equiv 2 \pmod 3 & y &\equiv -4 \pmod 7\\
& & y &\equiv 3 \pmod 7\\
y_1 &= 2 & y_2 &= 3
\end{aligned}$$

$$\begin{aligned}
21y &\equiv 1 \pmod{11}\\
10y &\equiv 1 \pmod{11}\\
10y &\equiv -10 \pmod{11}\\
y &\equiv -1 \pmod{11}\\
y &\equiv 10 \pmod{11}\\
y_3 &= 10
\end{aligned}$$

A kapott y_i értékek segítségével előállítandó x_0 megoldást modulo 231 vesszük.

$$x_0 \equiv M_1y_1c_1 + M_2y_2c_2 + M_3y_3c_3 \equiv 77 \cdot 2 \cdot 2 + 33 \cdot 3 \cdot 3 + 21 \cdot 10 \cdot 2 \equiv$$

$$\equiv 308 + 297 + 420 \equiv 77 + 66 + 189 \equiv 332 \equiv 101 \pmod{231}$$

A szimultán rendszer megoldása $\overline{101} \pmod{231}$. ■

2.9-4. Legyen $k \in \mathbb{N}$. Bizonyítsuk be, hogy van k számú egymásutáni egész úgy, hogy bármelyiknek van egynél nagyobb négyzetszám osztója.

Megoldás. Vegyünk k különböző prímet $(2, 3, \ldots, p_k)$, és nézzük a következő kongruencia-rendszert:

$$\begin{gathered}
x \equiv 1 \pmod{2^2}\\
x \equiv 2 \pmod{3^2}\\
\vdots\\
x \equiv k \pmod{p_k^2}
\end{gathered}$$

A kínai maradéktétel szerint ez a szimultán kongruencia-rendszer megoldható. Legyen egy megoldás A. Ekkor

$$2^2|A-1 \qquad 3^2|A-2 \qquad \ldots \qquad p_k^2|A-k.$$

Tehát az A előtti k számú egész eleget tesz a feltételnek. ■

2.9-5. Oldjuk meg a a következő kongruencia-rendszert a kínai maradéktétel segítségével:

$$\begin{aligned}
3x &\equiv 2 \pmod{5}\\
2x &\equiv 2 \pmod{7}\\
5x &\equiv 2 \pmod{11}
\end{aligned}$$

Megoldás. A kínai maradéktétel feltételei teljesülnek, így alkalmazhatjuk a módszert. Először megoldjuk külön-külön a kongruenciákat.

$$\begin{array}{rcll} 3x & \equiv & 2 & \pmod 5 \\ 3x & \equiv & -3 & \pmod 5 \\ x & \equiv & -1 & \pmod 5 \\ x & \equiv & 4 & \pmod 5 \end{array} \qquad \begin{array}{rcll} 2x & \equiv & 2 & \pmod 7 \\ x & \equiv & 1 & \pmod 7 \end{array} \qquad \begin{array}{rcll} 5x & \equiv & 2 & \pmod{11} \\ 5x & \equiv & 35 & \pmod{11} \\ x & \equiv & 7 & \pmod{11} \end{array}$$

$$m = 5 \cdot 7 \cdot 11 = 385 \qquad M_1 = 77 \qquad M_2 = 55 \qquad M_3 = 35$$

Az alábbi kongruenciákat egyenként oldjuk meg:

$$\begin{array}{rcll} 77y & \equiv & 1 & \pmod 5 \\ 2y & \equiv & 6 & \pmod 5 \\ y & \equiv & 3 & \pmod 5 \\ y_1 & = & 3 & \end{array} \qquad \begin{array}{rcll} 55y & \equiv & 1 & \pmod 7 \\ -y & \equiv & 1 & \pmod 7 \\ y & \equiv & 6 & \pmod 7 \\ y_2 & = & 6 & \end{array} \qquad \begin{array}{rcll} 35y & \equiv & 1 & \pmod{11} \\ 2y & \equiv & 12 & \pmod{11} \\ y & \equiv & 6 & \pmod{11} \\ y_3 & = & 6 & \end{array}$$

A kapott y_i értékek segítségével előállítandó x_0 megoldást modulo 385 vesszük.

$$x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 \equiv 77 \cdot 3 \cdot 4 + 55 \cdot 6 \cdot 1 + 35 \cdot 6 \cdot 7 \equiv$$

$$\equiv 924 + 330 + 1470 \equiv 2724 \equiv 29 \pmod{385}$$

A szimultán rendszer megoldása $\overline{29}$ (mod 385). ∎

2.9-6. Keressük meg a kínai maradéktétel alkalmazásával az alábbi kongruenciák szimultán megoldását:

$$5x \equiv 1 \pmod 7$$
$$4x \equiv 1 \pmod 9$$
$$8x \equiv 1 \pmod{13}$$

Megoldás. A kínai maradéktétel feltételei teljesülnek, így alkalmazhatjuk a módszert. Először megoldjuk külön-külön a kongruenciákat.

$$\begin{array}{rcll} 5x & \equiv & 1 & \pmod 7 \\ 5x & \equiv & -20 & \pmod 7 \\ x & \equiv & -4 & \pmod 7 \\ x & \equiv & 3 & \pmod 7 \end{array} \qquad \begin{array}{rcll} 4x & \equiv & 1 & \pmod 9 \\ 4x & \equiv & 28 & \pmod 9 \\ x & \equiv & 7 & \pmod 9 \end{array} \qquad \begin{array}{rcll} 8x & \equiv & 1 & \pmod{13} \\ 8x & \equiv & 40 & \pmod{13} \\ x & \equiv & 5 & \pmod{13} \end{array}$$

$$m = 7 \cdot 9 \cdot 13 = 819 \qquad M_1 = 117 \qquad M_2 = 91 \qquad M_3 = 63$$

Az alábbi kongruenciákat egyenként oldjuk meg:

$$\begin{array}{rcll} 117y & \equiv & 1 & \pmod 7 \\ 5y & \equiv & 1 & \pmod 7 \\ 5y & \equiv & 15 & \pmod 7 \\ y & \equiv & 3 & \pmod 7 \\ y_1 & = & 3 & \end{array} \qquad \begin{array}{rcll} 91y & \equiv & 1 & \pmod 9 \\ y & \equiv & 1 & \pmod 9 \\ & & & \\ & & & \\ y_2 & = & 1 & \end{array}$$

$$\begin{array}{rcll} 63y & \equiv & 1 & \pmod{13} \\ -2y & \equiv & 1 & \pmod{13} \\ -2y & \equiv & -12 & \pmod{13} \\ y & \equiv & 6 & \pmod{13} \\ y_3 & = & 6 & \end{array}$$

A kapott y_i értékek segítségével előállítandó x_0 megoldást modulo 819 vesszük.

$$x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 \equiv 117 \cdot 3 \cdot 3 + 91 \cdot 1 \cdot 7 + 63 \cdot 6 \cdot 5 \equiv$$

$$\equiv 3580 \equiv 304 \pmod{819}$$

A szimultán rendszer megoldása $\overline{304} \pmod{819}$. ∎

2.9-7. Legyen $A = 1000$, és végezzük el a $23 \cdot 37$ szorzást maradékszámrendszerben.

Megoldás. $m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. Keressük meg 23 és 37 számjegyeit maradékszámrendszerben, tehát a modulo p_i maradékokat.

$$23 = (1,\ 2,\ 3,\ 2,\ 1) \qquad 37 = (1,\ 1,\ 2,\ 2,\ 4)$$

Végezzük el a szorzást a maradékokkal.

$$23 \cdot 37 = (1 \cdot 1,\ 2 \cdot 1,\ 3 \cdot 2,\ 2 \cdot 2,\ 1 \cdot 4) = (1,\ 2,\ 1,\ 4,\ 4)$$

Oldjuk meg a következő szimultán kongruencia-rendszert:

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 4 \pmod 7 \\ x &\equiv 4 \pmod{11} \end{aligned}$$

Megoldjuk az $M_i y \equiv 1 \pmod{p_i}$ kongruenciákat, ahol az M_i értékek sorban 1155, 770, 462, 330 és 210. A megoldások

$$y_1 = 1, \quad y_2 = 2, \quad y_3 = 3, \quad y_4 = 1, \quad y_5 = 1.$$

Ennek felhasználásával

$$x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 + M_4 y_4 c_4 + M_5 y_5 c_5 \equiv$$

$$\equiv 1155 \cdot 1 \cdot 1 + 770 \cdot 2 \cdot 2 + 462 \cdot 3 \cdot 1 + 330 \cdot 1 \cdot 4 + 210 \cdot 1 \cdot 4 \equiv 851 \pmod{2310}$$

A számolás eredménye $23 \cdot 37 = 851$. ■

2.9-8. Legyen $A = 1000$, **és végezzük el a** $24 \cdot 33$ **szorzást maradékszámrendszerben.**

Megoldás. $m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. Keressük meg 24 és 33 számjegyeit maradékszámrendszerben, tehát a modulo p_i maradékokat.

$$24 = (0,\ 0,\ 4,\ 3,\ 2) \qquad 33 = (1,\ 0,\ 3,\ 5,\ 0)$$

Végezzük el a szorzást a maradékokkal.

$$24 \cdot 33 = (0 \cdot 1,\ 0 \cdot 0,\ 4 \cdot 3,\ 3 \cdot 5,\ 2 \cdot 0) = (0,\ 0,\ 2,\ 1,\ 0)$$

Oldjuk meg a következő szimultán kongruencia-rendszert:

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 1 \pmod{7} \\ x &\equiv 0 \pmod{11} \end{aligned}$$

Az M_i értékek sorban 1155, 770, 462, 330 és 210. Az $M_i y \equiv 1 \pmod{p_i}$ kongruenciák közül csak a modulo 5 és a modulo 7 kongruenciák megoldására van szükség, mert a többi értéke x_0-ban 0-val szorzódik. A megoldások

$$y_3 = 3, \quad y_4 = 1.$$

Ennek felhasználásával

$$x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 + M_4 y_4 c_4 + M_5 y_5 c_5 \equiv$$

$$\equiv 1155 \cdot y_1 \cdot 0 + 770 \cdot y_2 \cdot 0 + 462 \cdot 3 \cdot 2 + 330 \cdot 1 \cdot 1 + 210 \cdot y_5 \cdot 0 \equiv 792 \pmod{2310}$$

A számolás eredménye $24 \cdot 33 = 792$. ■

2.10. Lánctörtek, diofantikus approximációelmélet

Lánctörtön általában a következő alakú kifejezést értjük:

$$x_1 + \cfrac{1}{x_2 + \frac{1}{x_3 + \frac{1}{\dots}}}, \tag{I}$$

ahol x_1 valós, $x_i \ \ (2 \leq i)$ pedig pozitív valós szám.

$i \in \mathbb{N}$ futhat egy rögzített n-ig vagy végtelenig. Az első esetben *véges,* a másodikban *végtelen lánctörtről* beszélünk.

Az (I) lánctörtet a továbbiakban jelölje $//x_1,\ x_2,\ x_3,\ \dots,\ x_n//$, ha véges és az i index legnagyobb értéke n, ha pedig végtelen, akkor $//x_1,\ x_2,\ x_3,\ \dots//$. $x_1,\ x_2,\ x_3,\ \dots$ a *lánctört jegyei.* Minden véges lánctörtet kiszámíthatunk oly módon, hogy elemeivel véges sok racionális műveletet végzünk. Tehát minden véges lánctört egy valós szám, sőt – ha a jegyek racionálisak – racionális szám. Ezzel szemben egy végtelen lánctörtnek nem tudunk minden további nélkül számértéket tulajdonítani. *Egyszerű lánctörtről* beszélünk, ha a jegyek egész számok. Tetszőleges α valós számból kiindulva eljuthatunk egy véges vagy végtelen egyszerű lánctörthöz, amint azt az alábbi eljárásból láthatjuk.

Lánctörtbe fejtési eljárás

Tekintsünk egy $\gamma \in \mathbb{R}$ számot, legyen $\gamma_1 = \gamma$, és bontsuk egész és tört részére:

$$\gamma_1 = [\gamma_1] + \{\gamma_1\}, \quad 0 \leq \{\gamma_1\} < 1$$

Ha $\{\gamma_1\} > 0$, akkor $\frac{1}{\{\gamma_1\}}$ nagyobb, mint 1, s a $\gamma_2 = \frac{1}{\{\gamma_1\}}$ számot újra egész és tört részére bonthatjuk. A kapott egész részeket jelölje sorban $a_1,\ a_2,\ \dots,$ és $\gamma_i = \frac{1}{\{\gamma_{i-1}\}}$.

Az $s-1$-edik lépésben, ha γ_{s-1} nem egész, akkor

$$\gamma_{s-1} = a_{s-1} + \frac{1}{\gamma_s}, \text{ ahol } a_{s-1} = [\gamma_{s-1}] \text{ és } \gamma_s = \frac{1}{\{\gamma_{s-1}\}} = \frac{1}{\gamma_{s-1} - a_{s-1}}.$$

Ezt mindaddig ismételjük, amíg a kapott tört rész nem 0.

Ha γ_i-t $i = 2, ..., s-1$ esetén sorban visszahelyettesítjük a megelőző kifejezésekbe, akkor γ-t előállító emeletes törtekhez jutunk.

$$\gamma = a_1 + \frac{1}{\gamma_2} = a_1 + \frac{1}{a_2 + \frac{1}{\gamma_3}} = \dots = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \frac{1}{a_{s-1} + \frac{1}{\gamma_s}}}} \tag{II}$$

•

Az eljárás akkor ér véget, ha γ_s egész szám. Ha ez véges sok lépésben bekövetkezik, akkor a γ számot *véges egyszerű lánctörtbe* fejtettük, ellenkező esetben a γ szám *végtelen egyszerű lánctörtbe* fejtett alakjához jutunk. Az első esetben kapott tört értéke nyilván γ.

Az $//a_1,\ a_2,\ a_3,\ \ldots,\ a_n//$ lánctört *s-edik szelete* $//a_1,\ a_2,\ a_3,\ \ldots,\ a_s//$ $(1 \leq s \leq n)$, amit δ_s-sel fogunk jelölni.

Például

$$\delta_1 = a_1, \quad \delta_2 = a_1 + \frac{1}{a_2} = \frac{a_1a_2+1}{a_2}, \quad \delta_3 = a_1 + \frac{1}{a_2 + \frac{1}{a_3}}, \ldots$$

Látható a definícióból, hogy δ_s-ből δ_{s+1}-et úgy származtathatjuk, hogy a_s helyébe $a_s + \frac{1}{a_{s+1}}$-et írunk. Az alábbi rekurziós képletek segítségével a lánctört szeleteit állíthatjuk elő.

1. tétel. Tekintsük az $//a_1,\ a_2,\ a_3, \ldots,\ a_n//$ lánctörtet. Legyen

$$P_0 = 1 \qquad Q_0 = 0$$

$$P_1 = a_1 \qquad Q_1 = 1$$

és $2 \leq s \leq n$ esetén

$$P_s = a_sP_{s-1} + P_{s-2} \qquad Q_s = a_sQ_{s-1} + Q_{s-2}. \tag{III}$$

Ekkor $\frac{P_s}{Q_s} = \delta_s$, ahol δ_s a lánctört s-edik szelete.

Bizonyítás.

$s = 0$-ra P_s-et és Q_s-et értelmeztük, δ_s-et azonban nem.

$s = 1$ esetén $P_1 = a_1,\ Q_1 = 1$, s mint előbb láttuk, $\delta_1 = a_1$, ami megegyezik $\frac{P_1}{Q_1}$-gyel.

$s = 2$ esetén $P_2 = a_2a_1 + 1,\ Q_2 = a_2 \cdot 1 + 0,\ \delta_2 = \frac{a_1a_2+1}{a_2}$, ami $\frac{P_2}{Q_2}$-vel egyezik meg.

Tegyük fel, hogy $s > 2$, és $s - 1$-ig igaz az állításunk. Ekkor az indukciós feltevés miatt:

$$\delta_{s-1} = \frac{P_{s-1}}{Q_{s-1}} = \frac{a_{s-1}P_{s-2} + P_{s-3}}{a_{s-1}Q_{s-2} + Q_{s-3}}$$

δ_{s-1}-ből δ_s-et megkapjuk, ha a_{s-1} helyébe $a_{s-1} + \frac{1}{a_s}$ -et írjuk. Mivel δ_{s-1} előző alakjában P_{s-2}, P_{s-3} és Q_{s-2}, Q_{s-3} burkolt formában sem tartalmazza a_{s-1}-et, ezért ebből

$$\delta_s = \frac{\left(a_{s-1} + \frac{1}{a_s}\right) P_{s-2} + P_{s-3}}{\left(a_{s-1} + \frac{1}{a_s}\right) Q_{s-2} + Q_{s-3}} = \frac{a_s(a_{s-1}P_{s-2} + P_{s-3}) + P_{s-2}}{a_s(a_{s-1}Q_{s-2} + Q_{s-3}) + Q_{s-2}} =$$

$$= \frac{a_s P_{s-1} + P_{s-2}}{a_s Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s},$$

ami minden megfelelő s esetén igazolja az állításunkat. ∎

Az $//a_1,\ a_2,\ a_3,\ \ldots,\ a_n//$ lánctört *s-edik közelítő törtje* $\frac{P_s}{Q_s}$ $(1 \le s \le n)$, ahol P_s és Q_s a (III)-ban megadott módon keletkeznek.

Az előző tétel szerint egy lánctört s-edik közelítő törtje az s-edik szelet egyik előállítását adja.

Legyen a továbbiakban $//a_1,\ a_2,\ a_3,\ \ldots,\ a_n//$ egyszerű lánctört. Ekkor P_s és Q_s egész számok. A Q_s $(s = 0,\ 1,\ 2,\ \ldots)$ sorozat növekvő, sőt $s > 2$-től szigorúan monoton növekvő.

Szoros kapcsolat van egy racionális szám lánctörtbe fejtése és az euklideszi algoritmus között. Nézzük ugyanis $a, b \in \mathbb{Z}$, $b > 0$ esetén az a, b párra vonatkozó euklideszi algoritmust, és az egyenleteket osszuk végig sorban b, r_1, r_2, $\ldots$-vel, a mindenkori osztóval.

$$\begin{array}{lclllclcl}
a & = & bq_1 + r_1 & 0 < r_1 < b & \qquad & \frac{a}{b} & = & q_1 + \frac{r_1}{b} & 0 < \frac{r_1}{b} < 1 \\
b & = & r_1 q_2 + r_2 & 0 < r_2 < r_1 & & \frac{b}{r_1} & = & q_2 + \frac{r_2}{r_1} & 0 < \frac{r_2}{r_1} < 1 \\
r_1 & = & r_2 q_3 + r_3 & 0 < r_3 < r_2 & & \frac{r_1}{r_2} & = & q_3 + \frac{r_3}{r_2} & 0 < \frac{r_3}{r_2} < 1 \\
\vdots & & & \vdots & & \vdots & & & \vdots
\end{array}$$

Mint látjuk, a $q_1,\ q_2,\ q_3,\ \ldots$ számok a bal oldalon álló szám egész részei, $\frac{r_i}{r_{i-1}}$ pedig a tört részeket szolgáltatják, vagyis a q_i értékek a lánctörtbe fejtés jegyei, és q_2-től kezdve természetes számok.

Említettük, hogy egy véges egyszerű lánctört racionális számot állít elő. Fordítva is igaz, racionális szám véges egyszerű lánctörtbe fejthető, hiszen a megfelelő euklideszi algoritmus véges sok lépés után véget ér. Irracionális számok egyszerű lánctört alakja nyilvánvalóan csak végtelen lehet.

Legyenek $\delta_1,\ \delta_2,\ \ldots,\ \delta_n$ az $//a_1,\ a_2,\ a_3,\ \ldots,\ a_n//$ egyszerű lánctört szeletei. Vizsgáljuk meg két szelet különbségét:

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{P_s Q_{s-1} - P_{s-1} Q_s}{Q_s Q_{s-1}},$$

s nézzük ebben az előállításban a számlálót.

2. tétel. Legyenek az $//a_1,\ a_2,\ a_3,\ \ldots,\ a_n//$ egyszerű lánctört közelítő törtjei $\frac{P_s}{Q_s}$ $(1 \le s \le n)$. Ekkor

$$P_s Q_{s-1} - P_{s-1} Q_s = (-1)^s. \tag{IV}$$

Bizonyítás. A bal oldalon szereplő kifejezést jelöljük h_s-sel, és alkalmazzuk az előző tételben szereplő rekurziós kifejezéseket P_s és Q_s előállítására.

$$h_s = P_s Q_{s-1} - P_{s-1} Q_s = (a_s P_{s-1} + P_{s-2}) Q_{s-1} - P_{s-1}(a_s Q_{s-1} + Q_{s-2}) =$$

$$= P_{s-2}Q_{s-1} - P_{s-1}Q_{s-2} = -h_{s-1},$$

vagyis a h_s értékek ugyanannak a számnak a ± 1-szeresei. h_1 egyszerűen kiszámítható.

$$h_1 = P_1Q_0 - P_0Q_1 = a_1 \cdot 0 - 1 \cdot 1 = -1 = (-1)^1,$$

s így $h_s = (-1)^s$, ami igazolja az állításunkat. ∎

I. Következmény.

A (IV) formulából közvetlenül leolvasható, hogy

$$(P_s, Q_s) = 1 \quad (1 \le s \le n),$$

tehát egyszerű lánctört közelítő törtjének számlálója és nevezője relatív prímek.

II. Következmény.

Az előző tétel következményeként

$$\delta_s - \delta_{s-1} = \frac{(-1)^s}{Q_sQ_{s-1}} \quad 2 \le s \le n \text{ esetén.} \tag{V}$$

Nézzük most a második szomszédok eltérését $s > 2$ esetén:

$$\delta_s - \delta_{s-2} = \frac{(-1)^{s-1}a_s}{Q_sQ_{s-2}}$$

Tehát

$$\frac{P_s}{Q_s} - \frac{P_{s-2}}{Q_{s-2}} = \frac{(-1)^{s-1}a_s}{Q_sQ_{s-2}}, \tag{VI}$$

ami a

$$P_sQ_{s-2} - P_{s-2}Q_s = (-1)^{s-1}a_s$$

alakban is felírható.

III. Következmény.

Vizsgáljuk a (VI) alakot. Mivel $s > 2$ esetén a_s pozitív, ezért a páratlan indexű közelítő törtek növekvő, a párosak csökkenő sorozatot alkotnak, és – (V)-öt is figyelembe véve – bármely páros indexű nagyobb bármely páratlan indexűnél. Ha γ racionális, tehát egyszerű lánctört alakja véges, akkor, mivel valamilyen n-re $\gamma = \frac{P_n}{Q_n}$, az is igaz, hogy a többi közelítő tört közrefogja γ-t, vagyis

$$\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \frac{P_5}{Q_5} < \ldots \le //a_1,\ a_2,\ a_3,\ \ldots,\ a_n// \le \ldots < \frac{P_4}{Q_4} < \frac{P_2}{Q_2}.$$

3. tétel. Legyen $\gamma \in \mathbb{Q}$, $\frac{P_s}{Q_s}$ $(1 \leq s \leq n)$ pedig γ egyszerű lánctört-előállításának a közelítő törtjei. Ekkor

$$\left|\gamma - \frac{P_{s-1}}{Q_{s-1}}\right| \leq \frac{1}{Q_s Q_{s-1}} \qquad (2 \leq s \leq n).$$

Egyenlőség pontosan akkor áll fenn, ha $s = n$.

•

Legyen most $\gamma \in \mathbb{R}$ irracionális szám, $//a_1,\ a_2,\ a_3,\ \ldots//$ az egyszerű lánctörtbe fejtett alakja, $\frac{P_s}{Q_s}$ $(1 \leq s)$ pedig a közelítő törtjei. Ezekre a törtekre is igaz, hogy

$$\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \frac{P_5}{Q_5} < \ldots < \gamma < \ldots < \frac{P_4}{Q_4} < \frac{P_2}{Q_2}. \tag{VII}$$

A $\lim_{n\to\infty} \frac{P_n}{Q_n}$ létezik, és ezt a határértéket tekintjük az $//a_1,\ a_2,\ a_3,\ \ldots//$ végtelen egyszerű lánctört értékének. Ez az érték (VII) szerint éppen γ.

4. tétel. Ha $\gamma \in \mathbb{R}$ irracionális szám, $\frac{P_s}{Q_s}$ $(1 \leq s)$ pedig γ egyszerű lánctört-előállításának a közelítő törtjei, akkor

$$\left|\gamma - \frac{P_{s-1}}{Q_{s-1}}\right| < \frac{1}{Q_s Q_{s-1}} \quad (s = 2, 3, ...).$$

•

Legyen $//a_1,\ a_2,\ a_3,\ \ldots,\ a_n//$ tetszőleges véges egyszerű lánctört, és $a_n \geq 2$. Ekkor

$$//a_1,\ a_2,\ a_3,\ \ldots,\ a_n// = //a_1,\ a_2,\ a_3,\ \ldots,\ a_{n-1},\ a_n - 1,\ 1//,$$

vagyis ugyanannak a racionális számnak két különböző lánctört-előállítását kaptuk. Belátható, hogy ettől a kivételtől eltekintve a valós számok egyszerű lánctört-előállítása lényegében egyértelmű.

Érdekes az a tény, hogy racionális szám lánctörtbe fejtett alakja véges, irracionálisé végtelen, szemben például a tizedes törtekkel, melyek bizonyos racionális számokat végtelen, jóllehet szakaszos törttel állítanak elő.

Diofantikus approximációelmélet.

A lánctörtek igen jó szolgálatot tesznek az úgynevezett *diofantikus approximációelméletben,* mely elmélet olyan kérdésekkel foglalkozik, hogy egy függvénybe egész vagy racionális számokat helyettesítve a megfelelő függvényértékek milyen közel kerülhetnek valamilyen előre adott számhoz.

Legyen $\gamma \in \mathbb{R}$. Vizsgáljuk meg, hogy alkalmas $\frac{p}{q}$ $(p \in \mathbb{Z}, q \in \mathbb{N})$ racionális számokra milyen kicsivé tehető a $\left|\gamma - \frac{p}{q}\right|$ kifejezés. Az olyan $\frac{p}{q} \in \mathbb{Q}$ számokat, melyekre ez például q függvényében kicsi, *γ-t jól approximáló számoknak,* ilyen $\frac{p}{q}$ számok keresését pedig γ racionális számokkal való *approximációjának* mondjuk.

Legyen a továbbiakban γ irracionális szám, bár az állításokat megfelelően módosítva racionális γ esetére is alkalmazhatjuk.

Bármely $\gamma \in \mathbb{R}$ és $(q \in \mathbb{N})$ számokhoz található olyan $p \in \mathbb{Z}$, melyre $|q\gamma - p| \leq \frac{1}{2}$, mert a $q\gamma$-t közrefogó két egész szám közül a közelebbi megfelel p-nek. Ebből azt kapjuk, hogy

$$\left|\gamma - \frac{p}{q}\right| \leq \frac{1}{2q}. \tag{VIII}$$

Amint azt a $\frac{2k+1}{2}$ $(k \in \mathbb{N})$ alakú racionális számokhoz közeli γ irracionális számok mutatják, ez a becslés rögzített q mellett általában nem javítható. Igaz azonban a következő, P. G. L. Dirichlet által bizonyított tétel.

5. tétel. Dirichlet tétele. γ rögzített irracionális számhoz található végtelen sok olyan $q \in \mathbb{N}$, hogy alkalmas $p \in \mathbb{Z}$ számokra

$$\left|\gamma - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{IX}$$

Bizonyítás. Ezt az állítást lényegében már megtárgyaltuk, sőt konstruktív módszerünk van az ilyen számok előállítására. Fejtsük ugyanis γ-t egyszerű lánctörtbe. Irracionális lévén, végtelen sok $\frac{P_n}{Q_n}$ alakú közelítő törtet kapunk, melyekre

$$\left|\gamma - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n Q_{n+1}}.$$

Ez pedig $n \geq 2$ esetén

$$< \frac{1}{Q_n^2}.$$

■

A (IX)-ben lévő állítás sokkalta élesebb a (VIII)-ban lévőnél. Ha azonban még ezt a becslést is lényegesen javítani szeretnénk, akadályba ütközünk. Igaz ugyanis, hogy bármely $q \in \mathbb{N}, p \in \mathbb{Z}$ esetén

$$\left|\sqrt{2} - \frac{p}{q}\right| > \frac{1}{4q^2},$$

vagyis a 4 konstans a jobb oldal nevezőjében már túl nagy. Geometriai számelmélettel vagy lánctörtekkel igazolható, hogy $\frac{1}{\sqrt{5}}$ még írható, vagyis tetszőleges γ irracionális számhoz végtelen sok $q \in \mathbb{N}$ létezik, melyekre alkalmas $p \in \mathbb{Z}$-vel

$$\left|\gamma - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}. \tag{X}$$

Ha a $\gamma = \frac{1+\sqrt{5}}{2}$ esetet vizsgáljuk, azt tapasztaljuk, hogy az $\frac{1}{\sqrt{5}}$ konstans tovább nem csökkenthető, s így ez a becslés tetszőleges γ-ra tovább nem javítható.

Ha a γ irracionális számot egyszerű lánctörtbe fejtjük, nemcsak az igaz, hogy a közelítő törtek kielégítik (IX)-et, hanem az is, hogy bármely két egymást követő közelítő tört közül az egyik kielégíti a

$$\left|\gamma - \frac{p}{q}\right| < \frac{1}{2q^2} \tag{XI}$$

összefüggést, és bármely három egymást követő közül az egyik (X)-et.

Másrészt az is igaz, hogy ilyen jól approximáló törtek csak a közelítő törtek körében fordulhatnak elő. Nevezetesen, ha $\frac{p}{q} \in \mathbb{Q}$ kielégíti (XI)-et és $(p, q) = 1$, akkor $\frac{p}{q}$ közelítő törtje γ-nak.

Példák

2.10-1.

a. Fejtsük egyszerű lánctörtbe a $\frac{139}{102}$ számot.

b. Számítsuk ki a P_n, Q_n értékeket, és állítsuk elő a közelítő törteket.

c. Oldjuk meg a következő diofantoszi egyenletet:

$$139x + 102y = 1$$

Hasonlítsuk össze ezeket az adatokat azokkal, amelyek az *Euklideszi algoritmus* fejezetben $\mathrm{lnko}(139, 102)$ **kiszámítása közben keletkeztek.**

Megoldás.

a.

$$\frac{139}{102} = 1 + \frac{37}{102} = 1 + \frac{1}{\frac{102}{37}} = 1 + \frac{1}{2 + \frac{28}{37}} = 1 + \frac{1}{2 + \frac{1}{\frac{37}{28}}} = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{28}{9}}}} =$$

$$= 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{9}}}} = //1,\ 2,\ 1,\ 3,\ 9//$$

b.

$$\begin{array}{ll}
P_0 = 1 & Q_0 = 0 \\
P_1 = 1 & Q_1 = 1 \\
P_2 = 2 \cdot 1 + 1 = 3 & Q_2 = 2 \cdot 1 + 0 = 2 \\
P_3 = 1 \cdot 3 + 1 = 4 & Q_3 = 1 \cdot 2 + 1 = 3 \\
P_4 = 3 \cdot 4 + 3 = 15 & Q_4 = 3 \cdot 3 + 2 = 11 \\
P_5 = 9 \cdot 15 + 4 = 139 & Q_5 = 9 \cdot 11 + 3 = 102
\end{array}$$

$$\frac{P_1}{Q_1} = 1 \qquad \frac{P_2}{Q_2} = \frac{3}{2} \qquad \frac{P_3}{Q_3} = \frac{4}{3} \qquad \frac{P_4}{Q_4} = \frac{15}{11} \qquad \frac{P_5}{Q_5} = \frac{139}{102}$$

Az utolsó közelítő tört maga a lánctörtbe fejtett szám.

c. Az egyenlet megoldható, mert $(139, 102) = 1$, és ha $\frac{139}{102}$ lánctörtbe fejtett alakjának segítségével a (IV) képletben a $P_n = 139$, $Q_n = 102$ és $P_{n-1} = 15, Q_{n-1} = 11$ helyettesítést alkalmazzuk, akkor

$$139 \cdot 11 - 102 \cdot 15 = (-1)^5,$$

s ebből

$$139 \cdot (-11) + 102 \cdot (15) = 1$$

miatt az egyik megoldás közvetlenül leolvasható: $x_0 = -11, y_0 = 15$. Az összes megoldás

$$x_t = -11 + 102t \quad \text{és} \quad y_t = 15 - 139t, \ t \in \mathbb{Z}$$

alakban állítható elő. ■

2.10-2.

a. Fejtsük egyszerű lánctörtbe a $\frac{172}{62}$ számot. Írjuk fel a szeleteit.

b. Számítsuk ki a P_n, Q_n értékeket, valamint a közelítő törteket.

c. Oldjuk meg a következő diofantoszi egyenletet:

$$172x + 62y = 38$$

Hasonlítsuk össze ezeket az adatokat azokkal, amelyek a *Diofantikus egyenletek* fejezetben $\mathrm{lnko}(172, 62)$ kiszámítása közben keletkeztek.

Megoldás.

a.

n	$\gamma_1 = \gamma, \quad \gamma_{n+1} = \frac{1}{\gamma_n - q_n}$	$q_n = [\gamma_n]$
1	$\frac{172}{62}$	$[\frac{172}{62}] = 2$
2	$\frac{1}{\frac{172}{62}-2} = \frac{1}{\frac{48}{62}} = \frac{62}{48}$	$[\frac{62}{48}] = 1$
3	$\frac{1}{\frac{62}{48}-1} = \frac{1}{\frac{14}{48}} = \frac{48}{14}$	$[\frac{48}{14}] = 3$
4	$\frac{1}{\frac{48}{14}-3} = \frac{1}{\frac{6}{14}} = \frac{14}{6}$	$[\frac{14}{6}] = 2$
5	$\frac{1}{\frac{14}{6}-2} = \frac{1}{\frac{2}{6}} = \frac{6}{2}$	$[\frac{6}{2}] = 3$

A $\frac{172}{62} = //2,\ 1,\ 3,\ 2,\ 3//$. A szeletek ennek alapján:

$$2, \quad 2+1=3, \quad 2+\frac{1}{1+\frac{1}{3}}, \quad 2+\frac{1}{1+\frac{1}{3+\frac{1}{2}}}, \quad 2+\frac{1}{1+\frac{1}{3+\frac{1}{2+\frac{1}{3}}}}$$

Az utolsó szelet éppen a $\frac{172}{62}$ lánctört alakban megadva.

b.

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	2	2	1	2
2	1	$1 \cdot 2 + 1 = 3$	$1 \cdot 1 + 0 = 1$	3
3	3	$3 \cdot 3 + 2 = 11$	$3 \cdot 1 + 1 = 4$	$\frac{11}{4}$
4	2	$2 \cdot 11 + 3 = 25$	$2 \cdot 4 + 1 = 9$	$\frac{25}{9}$
5	3	$3 \cdot 25 + 11 = 86$	$3 \cdot 9 + 4 = 31$	$\frac{86}{31}$

Az utolsó közelítő érték, $\frac{86}{31}$ a $\frac{172}{62}$ szám redukált alakja.

c. Az egyenlet megoldható, mert $(172, 62) = 2|38$, és ha $\frac{172}{62}$ lánctörtbe fejtett alakjának segítségével a (IV) képletben a $P_n = 86,\ Q_n = 31$ és $P_{n-1} = 25, Q_{n-1} = 9$ helyettesítést alkalmazzuk, akkor

$$86 \cdot 9 - 31 \cdot 25 = (-1)^5.$$

Ezt szorozzuk 2-vel:

$$172 \cdot 9 - 62 \cdot 25 = (-1)^5 \cdot 2,$$

s ebből

$$172 \cdot (-9) + 62 \cdot (25) = 2.$$

Szorozzunk $\frac{38}{2} = 19$-cel:

$$172 \cdot (-171) + 62 \cdot (475) = 38$$

miatt az egyik megoldás közvetlenül leolvasható: $x_0 = -171,\ y_0 = 475$. Az összes megoldás

$$x_t = -171 + 31t \quad \text{és} \quad y_t = 475 - 86t,\ t \in \mathbb{Z}$$

alakban állítható elő. ∎

2.10-3. Fejtsük lánctörtbe $\sqrt{2}$-t.
Megoldás.

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{\sqrt{2} + 1} = 1 + \frac{1}{2 + (\sqrt{2} - 1)}$$

Mivel a $\sqrt{2}-1$ felbontása egyszer már előkerült számításaink során, láthatjuk, hogy a $\sqrt{2}$ előállítása periodikus, és

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2+\ldots}}.$$

∎

2.10-4. Melyik γ számnak a lánctörtbe fejtett alakja az alábbi? Állítsuk elő γ közelítő törtjeit.

$$1 + \frac{1}{1 + \frac{1}{1+\ldots}}.$$

Megoldás. Mivel $\gamma = 1 + \frac{1}{\gamma}$, vagyis $\gamma^2 - \gamma - 1 = 0$, így $\gamma_{1,2} = \frac{1 \pm \sqrt{5}}{2}$. Ebből $\gamma > 0$ miatt $\gamma = \frac{1+\sqrt{5}}{2}$ következik. Állítsuk elő a közelítő törteket.

$$\begin{array}{ll}
P_0 = 1 & Q_0 = 0 \\
P_1 = 1 & Q_1 = 1 \\
P_2 = 2 & Q_2 = 1 \\
P_3 = 3 & Q_3 = 2 \\
P_4 = 5 & Q_4 = 3 \\
P_5 = 8 & Q_5 = 5 \\
\vdots & \vdots
\end{array}$$

Általában $P_n = P_{n-1} + P_{n-2}$ és $Q_n = Q_{n-1} + Q_{n-2}$, valamint a megfelelő induló értékek miatt éppen a Fibonacci-számokhoz jutunk, s így $\frac{P_n}{Q_n} = \frac{F_{n+1}}{F_n}$, ahol F_n az n-edik Fibonacci-szám. ■

2.10-5. Fejtsük lánctörtbe a $\pi = 3,1415926\ldots$-t.
Megoldás.

$$a_1 = [\pi] = 3,$$

$$\gamma_2 = \frac{1}{\gamma_1 - a_1} = \frac{1}{\pi - 3} = \frac{1}{0,14159\ldots} = 7 + \frac{1}{\gamma_3}$$

$$\gamma_3 = \frac{1}{\frac{1}{\pi-3} - 7} = \frac{1}{\frac{1}{0,14159} - 7} = 15,9\ldots$$

Ebből:

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \ldots}}$$

$$\begin{array}{ll}
P_0 = 1 & Q_0 = 0 \\
P_1 = 3 & Q_1 = 1 \\
P_2 = 7 \cdot 3 + 1 = 22 & Q_2 = 7 \\
P_3 = 15 \cdot 22 + 3 = 333 & Q_3 = 15 \cdot 7 + 1 = 106 \\
\vdots & \vdots
\end{array}$$

Így a közelítő törtek:

$$\frac{3}{1},\ \frac{22}{7},\ \frac{333}{106},\ \dots$$

a nevező négyzeténél jobban közelítik π-t. Két szomszédos közelítő tört egyikére pedig igaz, hogy a legfeljebb ekkora nevezőjű törtek között nincs más ilyen jól közelítő tört. Emiatt gyakran alkalmazzák a $\frac{22}{7} = 3\frac{1}{7}$ közelítést a π-re.

■

3. Feladatok

3.1. Oszthatóság

3.1-1. Bizonyítsuk be, hogy 6 osztója az $n(n+1)(2n+1)$-nek, ahol n egész szám.

3.1-2. Jelöljön m egész számot. Bizonyítsuk be, hogy $m^5 - m$ osztható 6-tal.

3.1-3. Bizonyítsuk be, hogy ha a 4-gyel nem osztható páros szám, akkor $a(a^2-1)(a^2-4)$ osztható 960-nal.

3.1-4. Bizonyítsuk be, hogy három egymás után következő egész szám köbének összege osztható

a. a középső szám 3-szorosával;
b. 9-cel.

3.1-5. Bizonyítsuk be, hogy ha a tízes számrendszerben ábrázolt bármelyik háromjegyű természetes számot kétszer egymás mellé írjuk, akkor az így kapott hatjegyű szám osztható 7-tel, 11-gyel és 13-mal.

3.1-6. Bizonyítsuk be, hogy $4 \nmid n^2 + 2$ minden egész n-re teljesül.

3.1-7. Bizonyítsuk be, hogy minden n egész szám esetén:
a. $n^2 - n$ osztható 2-vel,
b. $n^3 - n$ osztható 6-tal,
c. $n^5 - n$ osztható 30-cal.

3.1-8. Bizonyítsuk be, hogy ha n páratlan, akkor $n^2 - 1$ osztható 8-cal.

3.1-9. Bizonyítsuk be, hogy ha x és y páratlan, akkor $x^2 + y^2$ páros, de nem osztható 4-gyel.

3.1-10. Bizonyítsuk be, hogy négy egymást követő természetes szám között van olyan, amelyik az összes többihez relatív prím.

3.1-11. Bizonyítsuk be, hogy hat egymást követő természetes szám közül mindig kiválasztható egy úgy, hogy az összes többihez relatív prím legyen.

3.1-12. Bizonyítsuk be, hogy $4^{90} + 1$ osztható 17-tel.

3.1-13. Bizonyítsuk be, hogy ha n tetszőleges egész szám, akkor n^5 és n ugyanarra a számjegyre végződik.

3.1-14. Bizonyítsuk be, hogy ha $m^2 - m + 1$ és $2n^2 + n - 1$ oszthatók 3-mal, akkor $m - n$ is osztható 3-mal.

3.1-15. Bizonyítsuk be, hogy ha n páratlan szám, akkor $n^4 - 18n^2 + 17$ osztható 64-gyel.

3.1-16.
a. Bizonyítsuk be, hogy nincs olyan x és y egész szám, amelyekre $x + y = 100$ és $(x, y) = 3$.
b. Bizonyítsuk be, hogy végtelen sok x, y egész számpár létezik, amelyre $x + y = 100$ és $(x, y) = 5$.

3.1-17.
a. Legfeljebb hány egymás utáni négyzetmentes szám lehet? (Az n egész számot négyzetmentes számnak nevezzük, ha nem osztható egynél nagyobb

szám négyzetével.)

b. Legfeljebb hány egymás utáni köbmentes szám lehet? (Az n egész számot köbmentes számnak nevezzük, ha nem osztható egynél nagyobb szám köbével.)

3.1-18. Bizonyítsuk be, hogy ha x és y is relatív prím 3-hoz, akkor $x^2 + y^2$ nem lehet négyzetszám.

3.1-19. Mi 2^{400} utolsó számjegye a tízes számrendszerben?

3.1-20. Mutassuk meg, hogy minden n természetes számra 49 osztója a $2^{3n+3} - 7n + 41$ összegnek.

3.1-21. Határozzuk meg azt a két pozitív egész számot, amelynek szorzatához az összegüket hozzáadva 34-et kapunk.

3.1-22. Melyik az a négyjegyű szám, amellyel 25 855-öt elosztva 37-et, 33 835-öt elosztva pedig 73-at kapunk maradékul?

3.1-23. Bizonyítsuk be, hogy bármely n természetes számra a $35n + 57$ és a $45n + 76$ számok legnagyobb közös osztója 1 vagy 19.

3.1-24. Bizonyítsuk be, hogy ha egy négyzetszámot elosztunk 16-tal, akkor maradékul is négyzetszámot kapunk.

3.1-25. Bizonyítsuk be, hogy ha a, b és c olyan természetes szám, hogy az $a^3 + b^3 + c^3$ összeg osztható 9-cel, akkor az a, b és c közül valamelyik osztható 3-mal.

3.1-26. Igazoljuk, hogy minden 6-nál nagyobb természetes szám felírható két, egynél nagyobb relatív prím szám összegeként.

3.1-27. Bizonyítsuk be, hogy bármely n pozitív egészre $77 | 22^n - 15^n + 70^n$.

3.2. Osztók száma, a τ függvény

3.2-1. Számítsuk ki a következő értékeket. **a.** $\tau(900)$ **b.** $\tau(6!)$

3.2-2. Hány pozitív osztója van az alábbi számoknak?
a. 27 000 **b.** 2 100 **c.** 55 125 **d.** 41 250

3.2-3. Milyen n természetes szám esetén van $8n$-nek és $9n$-nek ugyanannyi pozitív osztója?

3.2-4. Bizonyítsuk be, hogy végtelen sok természetes számra $\tau(n+1) \geq 2\tau(n)$.

3.2-5. Bizonyítsuk be, hogy minden n természetes szám esetén $\tau(n) < 2\sqrt{n}$.

3.2-6. Állapítsuk meg, hogy az $n = 249\ 072\ 255\ 432$ számnak hány olyan pozitív osztója van, amely nem osztható 42-vel?

3.3. Prímszámok

3.3-1. Bizonyítsuk be, hogy ha egy prímszámot 30-cal osztunk, akkor maradéknak 1-et vagy ismét prímszámot kapunk.

3.3-2. Melyek azok a prímszámok, amelyekre $2p + 1$ teljes köbszám?

3.3-3. $p^2 + 2$ milyen p prím esetén prímszám?

3.3-4. Milyen n egész számokra lesz $n^4 + 4$ prímszám?

3.3-5.
a. Lássuk be, hogy ha $2^k - 1$ prím, akkor k prím. *(Mersenne-féle prím.)*
b. Keressünk $2^p - 1$ alakú összetett számot, ha p prím.

3.3-6. Lássuk be, hogy ha 2^k+1 prímszám, akkor $k = 2^n$. *(Fermat-féle prím.)*

3.3-7. Határozzuk meg mindazon p prímszámokat (a negatívakat is), melyekre $2p - 1$ és $2p + 1$ is prímszám!

3.3-8. Adjuk meg az összes olyan 5-tel nem osztható n természetes számot, amelyre $n^2 + 4$ és $n^2 + 16$ mindketten prímszámok.

3.4. Euklideszi algoritmus

Az alábbi feladatokban az euklideszi algoritmussal számítsuk ki a és b legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

3.4-1. $a = 675$, $b = 471$.

3.4-2. $a = 432$, $b = 300$.

3.4-3. $a = 756$, $b = 333$.

3.4-4. $a = 504$, $b = 150$.

3.4-5. $a = 420$, $b = 154$.

3.4-6. $a = 1080$, $b = 285$.

3.4-7. $a = 2016$, $b = 880$.

3.4-8. $a = 30$, $b = 22$.

3.4-9. $a = 430$, $b = 300$.

3.4-10. $a = 2355$, $b = 450$.

3.4-11. $a = 300$, $b = 132$.

3.4-12. $a = 518$, $b = 154$.

3.4-13. $a = 198$, $b = 72$.

3.4-14. $a = 1100$, $b = 480$.

3.5. Kétváltozós lineáris diofantikus egyenletek

Oldjuk meg az alábbi diofantikus egyenleteket.

3.5-1. $60x + 16y = 60$

3.5-2. $115x + 50y = 1100$

3.5-3. $374x + 99y = 297$

3.5-4. $432x + 160y = 208$

3.5-5. $117x + 81y = 891$

3.5-6. $323x + 85y = 323$

3.6. Euler-féle φ függvény

3.6-1. Lássuk be, hogy ha m és n természetes számok, és $m|n$, akkor $\varphi(m)|\varphi(n)$.

3.6-2. Oldjuk meg a $2\varphi(x) = x$ egyenletet.

3.6-3. Milyen n természetes számok elégítik ki a $\varphi(5n) = \varphi(7n)$ egyenletet?

3.6-4. Hány olyan 105-nél nem nagyobb páros i természetes szám van, melyre $(i, 105) = 1$?

3.6-5. Hány olyan 385-nél nem nagyobb páros i természetes szám van, melyre $(i, 385) = 1$?

3.6-6. Bizonyítsuk be, hogy tetszőleges m természetes számhoz létezik végtelen sok olyan n, amelyre $m|\varphi(n)$.

3.6-7. Határozzuk meg a 3600-nál nem nagyobb, 3600-hoz nem relatív prím pozitív egészek számát.

3.6-8. Határozzuk meg a 7200-nál nem nagyobb, 3600-hoz relatív prím pozitív egészeknek a számát.

3.6-9. Határozzuk meg a 25 200-nál nem nagyobb, 3600-hoz relatív prím pozitív egészeknek a számát.

3.6-10.

a. Jellemezzük az olyan pozitív egészek halmazát, amelyekre $\varphi(2n) = \varphi(n)$.

b. Jellemezzük az olyan pozitív egészek halmazát, amelyekre $\varphi(2n) > \varphi(n)$.

3.6-11. Bizonyítsuk be, hogy végtelen sok olyan n egész szám van, amelyre $3 \nmid \varphi(n)$.

3.6-12. Oldjuk meg a $\varphi(3^x) = 486$ egyenletet.

3.6-13. Tudjuk, hogy $\varphi(x) = 17\ 160$ és $x = p^2q^2$, ahol p, q különböző prímszámok. Határozzuk meg x-et.

3.6-14. Tudjuk, hogy $\varphi(x) = 2200$ és $x = p^2q^2$, ahol p, q különböző prímszámok. Határozzuk meg x-et.

3.6-15. Tudjuk, hogy $\varphi(x) = 120$ és $x = p^2q^2$, ahol p, q különböző prímszámok. Határozzuk meg x-et.

3.6-16. Tudjuk, hogy $\varphi(x) = 840$ és $x = p^2q^2$, ahol p, q különböző prímszámok. Határozzuk meg x-et.

3.6-17. Bizonyítsuk be, hogy tetszőleges m, n természetes számokra $\varphi(mn) \geq \varphi(m)\varphi(n)$.

3.6-18. Hány 2005-nél nem nagyobb és 150-hez relatív prím természetes szám létezik?

3.7. Kongruenciák, maradékrendszerek, Euler–Fermat-tétel

3.7.1. Kongruenciák, maradékrendszerek

3.7-1. Bizonyítsuk be, hogy érvényesek az alábbi, a kongruenciákkal való műveletvégzésre vonatkozó állítások.

$$1. \quad \left.\begin{aligned} a &\equiv b \pmod m \\ c &\equiv d \pmod m \end{aligned}\right\} \rightarrow \quad a+c \equiv b+d \pmod m$$

$$2. \quad \left.\begin{aligned} a &\equiv b \pmod m \\ c &\equiv d \pmod m \end{aligned}\right\} \rightarrow \quad ac \equiv bd \pmod m$$

$$3. \quad ac \equiv bc \pmod m \quad \Leftrightarrow \quad a \equiv b \pmod{\tfrac{m}{(m,c)}}$$

3.7-2. Bizonyítsuk be az alábbi, úgynevezett *omnibusztételt.* Legyen $a_1,\ a_2,\ \ldots,\ a_m$ teljes maradékrendszer, $b_1,\ b_2,\ \ldots,\ b_{\varphi(m)}$ redukált maradékrendszer modulo m, és $a, c \in \mathbb{Z}$.

1. $(a,m)=1 \quad \rightarrow \quad aa_1+c,\ aa_2+c,\ \ldots,\ aa_m+c$ teljes maradékrendszer modulo m

2. $(a,m)=1 \quad \rightarrow \quad ab_1,\ ab_2,\ \ldots,\ ab_{\varphi(m)}$ redukált maradékrendszer modulo m

3.7-3. Lássuk be kongruenciák segítségével, hogy $641|2^{32}+1$, s így az F_5 Fermat-szám nem prím.

3.7-4. Mutassuk meg, hogy $2, 4, 6, \ldots, 2m$ teljes maradékrendszer modulo m, ha m páratlan.

3.7-5. Mutassuk meg, hogy $1^2, 2^2, \ldots, m^2$ nem teljes maradékrendszer modulo m, ha $m > 2$.

3.7-6. Milyen m esetén igaz, hogy egy teljes maradékrendszer elemeinek összege kongruens nullával modulo m?

3.7-7. Keressünk redukált maradékrendszert

a. modulo 6, **b.** modulo 7, **c.** modulo 12,
d. modulo 18, **e.** modulo 20.

3.7-8. Bizonyítsuk be, hogy egy modulo p redukált maradékrendszer elemeinek összege osztható p-vel, ha $p > 2$ prím.

3.7-9. Bizonyítsuk be, hogy egy modulo m redukált maradékrendszer elemeinek összege kongruens nullával modulo m, ha $m > 2$.

3.7-10.

a. Vegyünk egy modulo 2004 teljes maradékrendszert, amelynek elemei a legkisebb pozitív reprezentánsok. Mennyi az elemek összege?

b. Vegyünk egy modulo 2004 redukált maradékrendszert, amelynek elemei a legkisebb pozitív reprezentánsok. Mennyi az elemek összege?

3.7-11.

a. Vegyünk egy modulo 2005 teljes maradékrendszert, amelynek elemei a legkisebb pozitív reprezentánsok. Mennyi az elemek összege?

b. Vegyünk egy modulo 2005 redukált maradékrendszert, amelynek elemei a legkisebb pozitív reprezentánsok. Mennyi az elemek összege?

3.7-12. Legyen $p > 2$ prímszám. Állapítsuk meg, hogy az

$$1 \cdot 2, 2 \cdot 3, 3 \cdot 4, \ldots, (p-2) \cdot (p-1), (p-1) \cdot 1$$

számok teljes maradékrendszert alkotnak-e modulo p.

3.7-13. Legyen $a_1,\ a_2,\ \ldots,\ a_n$ teljes maradékrendszer modulo n, valamint $b_1,\ b_2,\ \ldots,\ b_k$ teljes maradékrendszer modulo k. Lássuk be, hogy az $a_i + nb_j$, $i = 1, \ldots, n,\ j = 1, \ldots, k$ számok teljes maradékrendszert alkotnak modulo nk.

3.7-14. Tegyük fel, hogy a $\varphi(m)$ szám $3k + 2$ alakú. Lássuk be, hogy

$$a_1^3, a_2^3, \ldots, a_{\varphi(m)}^3 \tag{1}$$

akkor és csak akkor alkot redukált maradékrendszert modulo m, ha az

$$a_1,\ a_2,\ \ldots,\ a_{\varphi(m)} \tag{2}$$

számok is redukált maradékrendszert alkotnak modulo m.

3.7-15. Legyen $a_1,\ a_2,\ \dots,\ a_p$ és $b_1,\ b_2,\ \dots,\ b_p$ két tetszőleges teljes maradékrendszer modulo p, ahol $p > 2$ prím. Bizonyítsuk be, hogy

$$a_1 \cdot b_1,\ a_2 \cdot b_2,\ \dots,\ a_p \cdot b_p$$

nem lehet teljes maradékrendszer modulo p.

3.7-16. Bizonyítsuk be, hogy ha p prím és $r_1,\ r_2,\ \dots,\ r_{p-1}$ redukált maradékrendszer modulo p, akkor

$$\prod_{j=1}^{p-1} r_j \equiv -1 \pmod{p}.$$

3.7.2. Euler–Fermat-tétel

3.7-17.

a. Bizonyítsuk be, hogy $n^6 - 1$ osztható 7-tel, ha $(n, 7) = 1$.

b. Bizonyítsuk be, hogy $n^{12} - 1$ osztható 7-tel, ha $(n, 7) = 1$.

c. Bizonyítsuk be, hogy minden egész k-ra $n^{6k} - 1$ osztható 7-tel, ha $(n, 7) = 1$.

3.7-18. Bizonyítsuk be, hogy bármely egész x-re $x^7 \equiv x \pmod{42}$.

3.7-19. Határozzuk meg 3^{1003} utolsó három számjegyét.

3.7-20. Állapítsuk meg, hogy 173^{163} milyen maradékot ad 17-tel osztva.

3.7-21. Határozzuk meg (a tízes számrendszerben felírt) 143^{143} utolsó három jegyét hármas alapú számrendszerben.

3.7-22. Milyen maradékot ad 103-mal osztva a következő szám: $205^{206^{207}}$?

3.7-23. Határozzuk meg a $37^{39^{42}}$ szám utolsó két számjegyét.

3.7-24. Határozzuk meg 403^{402} utolsó három számjegyét tízes számrendszerben.

3.7-25. Határozzuk meg a következő szám utolsó két számjegyét tízes számrendszerben: 519^{6803}.

3.7-26. Mi 3^{400} utolsó számjegye a tízes számrendszerben?

3.7-27. Mi 3^{404} utolsó két számjegye a tízes számrendszerben?

3.7-28. Mi a $17^{3^{1997}}$ utolsó két számjegye nyolcas számrendszerben?

3.7-29. Mi a legkisebb nemnegatív maradéka
a. 323^{149}-nek a 63-mal
b. 423^{173}-nak az 52-vel
c. 495^{173}-nak a 98-cal
d. 457^{101}-nek a 90-nel
való osztáskor?

3.7-30. Mi a $11^{1999^{26}}$ utolsó két jegye 10-es számrendszerben?

3.7-31. Bizonyítsuk be, hogy $n^{13} - n$ minden n egészre osztható a 2, 3, 5, 7 és 13 számokkal.

3.7-32. Bizonyítsuk be, hogy $m, n \in \mathbb{N}$ esetén $13 \cdot 31 \cdot 61 | m \cdot n(m^{60} - n^{60})$.

3.7-33. Melyek azok a p prímek, amelyek szorzata osztója az $m \cdot n(m^{60} - n^{60})$ szorzatnak minden $m, n \in \mathbb{N}$ esetén?

3.7-34. Lássuk be, hogy $2^{341} \equiv 2 \pmod{341}$.

3.7-35. Lássuk be, hogy $a \in \mathbb{Z}$ esetén $a^{1729} \equiv a \pmod{1729}$. Megjegyzés: 1729 nem prím, mégis teljesül rá a Fermat-tétel második alakja. Az ilyen számokat *álprímeknek (abszolut pszeudoprímeknek)* nevezzük.

3.7-36. Lássuk be, hogy minden $a \in \mathbb{Z}$ számra
a. $a^{561} \equiv a \pmod{561}$,
b. $a^{1105} \equiv a \pmod{1105}$,
c. $a^{2465} \equiv a \pmod{2465}$.
Megjegyzés: Ezek a számok *álprímeknek*. (Lásd az előző feladatot.)

3.7-37. Bizonyítsuk be, hogy 1997 végtelen sok hatványa végződik 1997-re.

3.7-38. Bizonyítsuk be, hogy a 2 és 5 számoktól különböző p prím a $9, 99, 999, 9999, \ldots$ számok közül végtelen soknak osztója. Bizonyítsuk be, hogy a 2, 3 és 5 számoktól különböző p prím az 1, 11, 111, 1111, ... számok közül végtelen soknak osztója.

3.8. Lineáris kongruenciák

3.8-1. Hány megoldása van az a., b., ill. c. kongruenciának?
a. $15x \equiv 25 \pmod{35}$ **b.** $15x \equiv 24 \pmod{35}$ **c.** $15x \equiv 0 \pmod{35}$

Oldjuk meg az alábbi kongruenciákat.

3.8-2. $21x \equiv 57 \pmod{78}$

3.8-3. **a.** $26x \equiv 12 \pmod{22}$ **b.** $20x \equiv 19 \pmod{22}$

3.8-4. $16x \equiv 36 \pmod{28}$

3.8-5. $126x \equiv 45 \pmod{99}$

3.8-6. $126x \equiv 46 \pmod{99}$

3.8-7. $35x \equiv -15 \pmod{30}$

3.8-8.
a. $20x \equiv 4 \pmod{30}$ **b.** $20x \equiv 30 \pmod{4}$ **c.** $353x \equiv 254 \pmod{40}$

3.8-9. **a.** $30x \equiv 40 \pmod{15}$ **b.** $40x \equiv 25 \pmod{15}$

Keressük meg a következő egyenletek egész megoldásait kongruenciák felhasználásával.

3.8-10. $27x + 49y = 3$

3.8-11. $33x + 23y = 2$

3.8-12. $33x + 23y = 3$

3.8-13. Adjuk meg azt a legkisebb természetes számot, amely 28-as alapú számrendszerben felírva 3-ra, 19-es alapú számrendszerben felírva pedig 4-re végződik. Oldjuk meg a feladatot kongruenciák segítségével.

3.8-14. Melyek azok a száznál kisebb természetes számok, amelyek huszonháromszorosát hetes alapú számrendszerben felírva az utolsó jegy 5, az utolsó előtti jegy pedig 2? Oldjuk meg a feladatot kongruenciák segítségével.

3.8-15. Bizonyítsuk be, hogy ha

$$a \equiv b \pmod{p^n},$$

akkor

$$a^p \equiv b^p \pmod{p^{n+1}},$$

ahol p prímszám.

3.9. Lineáris kongruencia-rendszerek, a kínai maradéktétel

3.9-1. Oldjuk meg a következő kongruencia-rendszert:

$$\begin{aligned} 7x &\equiv 11 \pmod{12} \\ 13x &\equiv 17 \pmod{21} \end{aligned}$$

3.9-2. Egy négyjegyű természetes szám 72-vel osztva 46, 127-tel osztva 97 maradékot ad. Melyik ez a szám?

3.9-3. Keressük meg a kínai maradéktétel alkalmazásával azt az egytől különböző, legkisebb pozitív egész x számot, amely egyidejűleg kielégíti az

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 1 \pmod{7} \end{aligned}$$

kongruenciákat.

3.9-4. Keressük meg a kínai maradéktétel alkalmazásával az összes egész számot, amely egyidejűleg kielégíti az

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 2 \end{aligned}$$

kongruenciákat.

3.9-5. Oldjuk meg a kínai maradéktétel alkalmazásával az alábbi kongruencia-rendszert:

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

3.9-6. Keressük meg a kínai maradéktétel alkalmazásával azokat az egész számokat, amelyek 3-mal osztva 1-et, 4-gyel osztva 2-t, 5-tel osztva 3-at adnak maradékul.

3.9-7. Legyen $A = 1100$, és végezzük el a $29 \cdot 36$ szorzást maradékszámrendszerben.

3.9-8. Legyen $A = 1000$, és végezzük el a $19 \cdot 48$ szorzást maradékszámrendszerben.

3.9-9. Bizonyítsuk be, hogy tetszőleges k természetes számhoz található k számú, egymást követő természetes szám, melyek egyike sem teljes hatvány (azaz egyikük sem természetes szám 1-nél nagyobb egész kitevőjű hatványa).

3.10. Lánctörtek, diofantikus approximációelmélet

Fejtsük egyszerű lánctörtbe az alábbi számokat. Számítsuk ki a P_n, Q_n értékeket, és állítsuk elő a közelítő törteket.

3.10-1. $\frac{41}{31}$

3.10-2. $\frac{85}{37}$

3.10-3. $\frac{83}{22}$

3.10-4. $\frac{62}{23}$

Adjuk meg az alábbi lánctörteket $\frac{p}{q}$ alakban a P_n, Q_n értékek kiszámításával.

3.10-5. $//1,\ 2,\ 3,\ 4,\ 5//$

3.10-6. $//5,\ 4,\ 3,\ 2,\ 1//$

3.10-7. $//1,\ 2,\ 3,\ 1,\ 2//$

3.10-8. $//2,\ 3,\ 1,\ 2,\ 3//$

3.10-9. $//3,\ 2,\ 1,\ 3,\ 2//$

3.10-10. $//2,\ 1,\ 2,\ 1,\ 2//$

3.10-11. $//3,\ 1,\ 3,\ 1,\ 3//$

3.10-12. $//2,\ 3,\ 2,\ 3,\ 2//$

4. Megoldások

4.1. Oszthatóság

4.1-1.

$$
\begin{aligned}
n(n+1)(2n+1) &= n(n+1)(2n-2+3) = n(n+1)(2(n-1)+3) = \\
&= n(n+1)2(n-1) + n(n+1)3 \qquad (1)
\end{aligned}
$$

Ez a kifejezés osztható 2-vel, mert n vagy $n+1$ páros, és osztható 3-mal, mert $n-1$, n, $n+1$ három egymás utáni szám közül az egyik osztható 3-mal, és (1)-ben a második tagban szerepel a 3. Mivel a kifejezés osztható 2-vel és 3-mal, melyek relatív prímek, osztható 6-tal is. ■

4.1-2.

$$m^5 - m = m(m^4-1) = m(m^2-1)(m^2+1) = m(m-1)(m+1)(m^2+1)$$

Ebből az átalakításból látszik, hogy a kifejezés osztható 2-vel és 3-mal, tehát 6-tal is. ■

4.1-3.

$$960 = 2^6 \cdot 3 \cdot 5$$

és

$$a(a^2 - 1)(a^2 - 4) = a(a-1)(a+1)(a-2)(a+2) \tag{1}$$

3 és 5 osztója (1)-nek, mert öt egymás utáni szám szorzata osztható 3-mal és 5-tel is. Tudjuk, hogy a 4-gyel nem osztható páros szám, ezért $a-2$ és $a+2$ 4-gyel osztható páros számok, sőt egyikük 8-cal is osztható. Ezek szerint (1) osztható 2^6-nal. Mivel az osztók mind relatív prímek, a szorzatuk is osztója (1)-nek. ■

4.1-4.

$$(a-1)^3 + a^3 + (a+1)^3 =$$

$$= a^3 - 3a^2 + 3a - 1 + a^3 + a^3 + 3a^2 + 3a + 1 = 3a^3 + 6a = 3a(a^2 + 2) \tag{1}$$

a. Az átalakításból látszik, hogy $3a$ osztója (1)-nek.

b. Ha $3|a$, akkor $9|3a$. Ha $3 \nmid a$, akkor a^2 3-mal osztva 1-et ad maradékul, így $3|a^2 + 2$ és $9|3(a^2 + 2)$, tehát 9 mindkét esetben osztója (1)-nek. ■

4.1-5.

Legyen a háromjegyű szám abc. A kapott új szám:

$$abcabc = a10^5 + b10^4 + c10^3 + a10^2 + b10 + c = 1001(a10^2 + b10 + c),$$

és $1001 = 7 \cdot 11 \cdot 13$, ami bizonyítja az állításunkat. ■

4.1-6.

Ha n páros, akkor $4|n^2$, s így $4 \nmid n^2 + 2$. Ha n páratlan, akkor $n = 2k + 1$,

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1,$$

és így szintén $4 \nmid n^2 + 2 = 4k^2 + 4k + 3$. ■

4.1-7.

a. $n^2 - n = n(n-1)$, n és $n-1$ közül az egyik páros, így a szorzatuk osztható 2-vel.

b. $n^3 - n = n(n^2-1) = n(n-1)(n+1)$. A három egymás utáni szám szorzata osztható 2-vel és 3-mal, így osztható 6-tal is.

c.

$$A = n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = \tag{1}$$

$$= n(n-1)(n+1)(n^2+1) \tag{2}$$

(2)-ből látható, hogy A felbontásában három egymás utáni szám szerepel, emiatt $2|A$ és $3|A$. Négyzetszám 5-tel osztva 0, 1 vagy -1 maradékot ad (2.1-1. példa), ezért $5|n$ vagy $5|n^2-1$ vagy $5|n^2+1$, amiből (1) alapján $5|A$. 2, 3 és 5 relatív prímek, így a szorzatuk, 30 is osztója A-nak. ■

4.1-8.

$$n = 2k+1, \quad n^2 - 1 = 4k^2 + 4k = 4k(k+1)$$

Mivel k vagy $k+1$ páros, a kifejezés osztható $4 \cdot 2 = 8$-cal. ■

4.1-9.

$$x = 2k+1, \quad y = 2l+1$$
$$x^2 + y^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4(k^2 + k + l^2 + l) + 2.$$

■

4.1-10.

Legyen a négy szám a, $a+1$, $a+2$, $a+3$. Ha bármelyik kettőnek van közös osztója, az csak 2 vagy 3 lehet, mert a közös osztó a különbséget is osztja. A két páratlan közül legfeljebb az egyik osztható 3-mal. A másik páratlan sem 2-vel, sem 3-mal nem osztható, így a többi számhoz relatív prím. ■

4.1-11.

A hat egymást követő természetes szám közül három páratlan. Ezek közül csak az egyik osztható 3-mal, és legfeljebb az egyik osztható 5-tel. Marad egy, amelyik sem 3-mal, sem 5-tel nem osztható. Ez relatív prím a többi öt számhoz. Ha ugyanis nem lenne valamelyikhez relatív prím, akkor a két szám közös osztója 2, 3, 4, 5 közül kerülne ki, hiszen a közös osztó két szám különbségét is osztja. ■

4.1-12.

$$4^{90}+1=(4^2)^{45}+1=16^{45}+1 \tag{1}$$

$a^{2k+1}+b^{2k+1}$ osztható $a+b$-vel, hiszen

$$a^{2k+1}+b^{2k+1}=(a+b)(a^{2k}-a^{2k-1}b+\ldots-ab^{2k-1}+b^{2k}),$$

ezért (1) osztható $16+1=17$-tel. ■

4.1-13.

Belátjuk, hogy $10|n^5-n$. Nézzük a következő átalakítást.

$$n^5-n=n(n^4-1)=n(n^2-1)(n^2+1) \tag{1}$$

2 osztója az (1) kifejezésnek, mert n és n^4-1 közül az egyik páros. 5 is osztója az (1) kifejezésnek, mert vagy $5|n$, vagy pedig n^2-1, illetve n^2+1 osztható 5-tel, hiszen négyzetszámok 5-tel osztva 0, 1, illetve -1 maradékot adhatnak. (Lásd 2.1-1. példa.) Mivel 2 és 5 relatív prímek, ezért a szorzatuk is osztója (1)-nek.

■

4.1-14.

$3\nmid m$, mert $3|m^2-m+1$. Hasonlóan $3\nmid n$, mert $3|2n^2+n-1$. Használjuk a következő jelölést: $a=m^2-m+1$, $\quad b=2n^2+n-1$, és nézzük $a+b$-t. $a+b$ szintén osztható 3-mal. Másrészt $a+b=m^2+2n^2-(m-n)$. m^2 és

n^2 3-mal való osztási maradéka 1, így $m^2 + 2n^2$ osztható 3-mal, tehát $m - n$ is osztható vele.

■

4.1-15.

$$n^4 - 18n^2 + 17 = n^2(n^2 - 17) - (n^2 - 17) = (n^2 - 17)(n - 1)(n + 1) \quad (1)$$

$$n^2 - 17 = n^2 - 1 - 16 = (n - 1)(n + 1) - 16 \quad (2)$$

$(n - 1)$ és $(n + 1)$ két egymás utáni páros szám, az egyikük 4-gyel is osztható, a szorzatuk osztható 8-cal, emiatt (2) is osztható 8-cal. Ezekből pedig következik, hogy (1) osztható $8 \cdot 8 = 64$-gyel. ■

4.1-16.

a. $(x, y) = (x, 100 - x) = (x, 100)$, de $3 \nmid 100$.

b. Legyen például $x = 100n + 5, \quad y = 95 - 100n, \quad n = 1,\ 2,\ 3,\ \ldots$ ■

4.1-17.

a. A 4-gyel osztható számok nem négyzetmentesek. Két szomszédos 4-gyel osztható szám között három másik helyezkedik el. Ezek lehetnek négyzetmentesek (pl. 5,6,7), lehetnek nem négyzetmentesek. A válasz tehát az, hogy legfeljebb három egymás utáni négyzetmentes szám lehet.

b. A 8-cal osztható számok nem köbmentesek. Két szomszédos 8-cal osztható szám között hét másik helyezkedik el. Ezek lehetnek köbmentesek (pl. 9, 10, 11, 12, 13, 14, 15), lehetnek nem köbmentesek. A válasz tehát az, hogy legfeljebb hét egymás utáni köbmentes szám lehet.

■

4.1-18.

Tudjuk, hogy négyzetszám 3-mal osztva csak 0 vagy 1 maradékot adhat (2.1-1. példa). Mivel x és y is relatív prím 3-hoz, x^2 és y^2 3-mal való osztási maradéka 1, $x^2 + y^2$-é 2, tehát $x^2 + y^2$ nem lehet négyzetszám. ■

4.1-19.

Nézzük, milyen számra végződnek a 2 hatványai:

n	1	2	3	4	5	6	7	8	...
2 n-edik hatványának utolsó jegye	2	4	8	6	2	4	8	6	...

$2^{400} = (2^4)^{100}$, és látható, hogy a negyedik hatvány és annak hatványai 6-ra végződnek, így 2^{400} utolsó számjegye 6. ∎

4.1-20.

1. *megoldás.*

Teljes indukcióval bizonyítunk.

I. $n = 1$ esetén
$$2^{3n+3} - 7n + 41 = 98 = 2 \cdot 49,$$
s így igaz az állítás.

II. Legyen most $n > 1$, és tegyük fel, hogy $49 | 2^{3n+3} - 7n + 41$.

$n + 1$ esetén:
$$2^{3(n+1)+3} - 7(n+1) + 41 = 2^{3n+3} - 7n + 41 + 7(2^{3n+3} - 1) =$$
$$= 2^{3n+3} - 7n + 41 + 7(8^{n+1} - 1)$$

$7 | 8^{n+1} - 1$ és így 49 osztója a kifejezésnek.

Mivel $n = 1$ esetén teljesül az állítás, és II.-ben beláttuk az öröklődést is, ezért az állítás minden n természetes szám esetén igaz.

2. *megoldás.*

Felhasználjuk, hogy $8^n - 1 = 7(8^{n-1} + 8^{n-2} + \ldots + 1)$.
$$2^{3n+3} - 7n + 41 = 8(8^n - 1) - 7n + 49 =$$
$$= 8 \cdot 7(8^{n-1} + 8^{n-2} + \ldots + 1) - 7n + 49 =$$
$$= 7(8^n + 8^{n-1} + \ldots + 8 - n) + 49 =$$
$$= 7((8^n - 1) + (8^{n-1} - 1) + \ldots + (8 - 1)) + 49$$

∎

4.1-21.
Legyen a két természetes szám m és n. Ekkor

$$\begin{aligned} m \cdot n + m + n &= 34 \\ (m+1)(n+1) &= 35 \end{aligned}$$

$m,\ n \geq 1$, így $m+1 = 5$ és $n+1 = 7$, vagy fordítva. A két szám tehát 4 és 6. ■

4.1-22.
A keresett szám legyen a. Ekkor $1000 \leq a \leq 9999$.

$25\ 855 = a \cdot q_1 + 37$	és	$33\ 835 = a \cdot q_2 + 73$
$25\ 818 = a \cdot q_1$	és	$33\ 762 = a \cdot q_2$
$25\ 818 = 2 \cdot 3 \cdot 13 \cdot 331$	és	$33\ 762 = 2 \cdot 3 \cdot 17 \cdot 331$

Az egyetlen négyjegyű közös osztó $2 \cdot 3 \cdot 331 = 1\ 968$, s így ez az egyetlen megoldás. ■

4.1-23.

A számok minden k közös osztója osztja a számok lineáris kombinációját is, így $k | 7(45n + 76) - 9(35n + 57) = 19$. Így $k = 1$ vagy $k = 19$. A legnagyobb közös osztó is az 1, illetve a 19 lehet. Például $n = 0$ esetén a legnagyobb közös osztó 19, $n = 1$ esetén pedig 1. ■

4.1-24.
Legyen $n = 8k \pm r$, ahol $k \in \mathbb{Z}$ és $r = 0,\ 1,\ 2,\ 3$ vagy 4. Ekkor

$$n^2 = 64k^2 \pm 16kr + r^2$$

r^2 lehetséges értékei $0,\ 1,\ 4,\ 9$ vagy 16, s így a maradék valóban négyzetszám. ■

4.1-25.
Ha egy m szám nem osztható 3-mal, akkor $m = 3k \pm 1$ alakú. Ekkor a köbe

$$m^3 = 27k^3 \pm 27k^2 + 9k \pm 1,$$

9-cel osztva a maradék ± 1. Ha egyik szám sem lenne osztható 3-mal, akkor a három köbszám maradékának összege 1, -1, 3, illetve -3 lehetne, tehát semmiképpen nem lenne a 9-cel történő osztás maradéka 0. ∎

4.1-26.

Jelöljük a számot n-nel. Ha n páratlan szám, $n = 2k + 1$, akkor k és $k + 1$ a két relatív prím összetevő. Ha n páros szám, $n = 2k$, akkor két esetet kell megkülönböztetnünk. Legyen először k páros szám. Ekkor a két relatív prím összetevő $k - 1$ és $k + 1$. Ezek valóban relatív prímek, mert közös osztójuk legfeljebb akkora lehet, mint a különbségük, ami 2. Ez azonban nem közös osztó, mert a számok páratlanok. Legyen most k páratlan szám. A megfelelő relatív prím összetevők $k-2$ és $k+2$. Az előzőhöz hasonlóan belátható, hogy valóban relatív prímek. ∎

4.1-27.

$77 = 7 \cdot 11$. Egyrészt

$$7|22^n - 15^n + 70^n,$$

mert $7|70$ és

$$7|22^n - 15^n = (22 - 15)(22^{n-1} + 22^{n-2} \cdot 15 + \ldots + 15^{n-1}) =$$

$$= 7(22^{n-1} + 22^{n-2} \cdot 15 + \ldots + 15^{n-1}).$$

Másrészt

$$11|22^n - 15^n + 70^n,$$

mert $11|22^n$ és

$$11|70^n - 15^n = (70 - 15)(70^{n-1} + 70^{n-2} \cdot 15 + \ldots + 15^{n-1}) =$$

$$= 55(70^{n-1} + 70^{n-2} \cdot 15 + \ldots + 15^{n-1}).$$

7 és 11 relatív prímek, így

$$77|22^n - 15^n + 70^n$$

is teljesül. ∎

4.2. Osztók száma, a τ függvény

4.2-1.

a. $\tau(900) = \tau(2^2 \cdot 5^2 \cdot 3^2) = 3 \cdot 3 \cdot 3 = 27$

b. $\tau(6!) = \tau(2^4 \cdot 3^2 \cdot 5) = 5 \cdot 3 \cdot 2 = 30$ ■

4.2-2.

a.	$27\ 000 = 2^3 \cdot 3^3 \cdot 5^3$	$\tau(27\ 000) = 4 \cdot 4 \cdot 4 = 64$
b.	$2\ 100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$	$\tau(2\ 100) = 3 \cdot 2 \cdot 3 \cdot 2 = 36$
c.	$55\ 125 = 3^2 \cdot 5^3 \cdot 7^2$	$\tau(55\ 125) = 3 \cdot 4 \cdot 3 = 36$
b.	$41\ 250 = 2 \cdot 3 \cdot 5^4 \cdot 11$	$\tau(41\ 250) = 2 \cdot 2 \cdot 5 \cdot 2 = 40$

■

4.2-3.
A következő egyenletet kell megoldanunk:

$$\tau(8n) = \tau(9n) \tag{1}$$

Legyen

$$n = 2^\alpha \cdot 3^\beta \cdot y, \text{ ahol } (y, 6) = 1. \tag{2}$$

Ekkor

$$\tau(8n) = \tau(2^{\alpha+3}) \cdot \tau(3^\beta) \cdot \tau(y)$$

$$\tau(9n) = \tau(2^\alpha) \cdot \tau(3^{\beta+2}) \cdot \tau(y)$$

Ezeket (1)-be behelyettesítjük, $\tau(y)$-nal egyszerüsítünk és kifejtjük.

$$(\alpha + 4)(\beta + 1) = (\alpha + 1)(\beta + 3)$$

Ebből

$$3\beta = 2\alpha - 1. \tag{3}$$

Ezt az egyszerű diofantoszi egyenletet oldjuk meg a következő módon. (Más megoldási lehetőségeket láthatunk a diofantikus egyenletek, valamint a kongruenciák megoldásával foglalkozó fejezetekben.)

$$2\alpha = 3\beta + 1$$

$$\alpha = \frac{3\beta + 1}{2} = \beta + \frac{\beta + 1}{2} \tag{4}$$

$\frac{\beta+1}{2}$ egész szám kell legyen, jelöljük k-val. Ekkor $\beta = 2k-1$. Ezt helyettesítsük (4)-be. $\alpha = 3k-1$-et kapunk. α és β nem negatív egész számok, így k pozitív egész kell legyen.

Tehát az $\alpha = 3k-1, \quad \beta = 2k-1 \quad k \in \mathbb{N}$ kitevőpárokkal képezett (2) alakú n számok alkotják a feladat megoldását. A 2-vel és 3-mal nem osztható y tényező tetszőlegesen választható. ■

4.2-4.

Legyen $n = 4k+1$ alakú prím. Ilyen végtelen sok van. (Lásd a 2.3-3. példát)

Ekkor $\tau(n) = 2$ és

$\tau(n+1) = \tau(4k+2) = \tau(2(2k+1)) = \tau(2)\tau(2k+1) \geq 2 \cdot 2 = 4.$ ■

4.2-5.

Állítsuk rendezett párba az n osztóit a következő módon. Az n olyan d osztójához, amelyikre $1 \leq d \leq \sqrt{n}$, rendeljük hozzá az $\frac{n}{d}$ komplementer osztót. Így az összes osztót párba rendeztük, és legfeljebb $\sqrt{n}$ párt kaptunk. A párok elemei különbözőek, kivéve azt az esetet, amikor $\sqrt{n}$ is osztó. Ekkor ugyanis

$$\frac{n}{\sqrt{n}} = \sqrt{n},$$

tehát $\sqrt{n}$ saját maga párja. Az osztók száma kevesebb, mint $2\sqrt{n}$, mert vagy $\sqrt{n}$ kimarad az osztók közül, és a párok száma kevesebb $\sqrt{n}$-nél, vagy $\sqrt{n}$ is szerepel az osztók között, de mivel önmagával van párban, az osztók száma kisebb, mint a párok számának a kétszerese, vagyis mint $2\sqrt{n}$.

■

4.2-6.

Keressük meg a szám kanonikus alakját.

$$n = 249\ 072\ 255\ 432 = 2^3 \cdot 3^2 \cdot 7 \cdot 11^3 \cdot 13^5$$

A 42-vel nem osztható osztók számát megkaphatjuk, ha az összes osztók számából kivonjuk a 42-vel osztható osztók számát, azaz $\frac{n}{42}$ osztóinak a számát:

$$\tau(n) - \tau\left(\frac{n}{42}\right) = \tau(2^3 \cdot 3^2 \cdot 7 \cdot 11^3 \cdot 13^5) - \tau(2^2 \cdot 3 \cdot 11^3 \cdot 13^5) =$$

$$= 4 \cdot 3 \cdot 2 \cdot 4 \cdot 6 - 3 \cdot 2 \cdot 4 \cdot 6 = 576 - 144 = 432$$

■

4.3. Prímszámok

4.3-1.
Osszuk el p-t maradékosan 30-cal.

$$p = 30n + r, \quad 1 \leq r < 30 \tag{1}$$

Belátjuk, hogy $r = 1$ vagy r prím. $30 = 2 \cdot 3 \cdot 5$ és $(2 \cdot 3 \cdot 5, r) = 1$, mert p prím. Az 1 és 30 közötti számok mindegyike vagy osztható $2,\ 3,\ 5$ valamelyikével, vagy az

$$1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$$

számok közül kerül ki, amelyek azonban mind prímek. ■

4.3-2.
$2p + 1 = a^3$, amiből $2p = a^3 - 1 = (a-1)(a^2 + a + 1)$. Ha $a - 1 = 2$ és $a^2 + a + 1 = p$, akkor $a = 3$ és $p = 13$. Ha pedig $a^2 + a + 1 = 2$ és $a - 1 = p$, akkor $a^2 + a - 1 = 0$. Ebből

$$a_{1,2} = \frac{-1 \pm \sqrt{5}}{2},$$

vagyis a nem egész szám, ami esetünkben nem megoldás. Az egyetlen megoldás $p = 13$. ■

4.3-3.

Csak $p = 3$ esetén. Ugyanis ha $p \neq 3$, akkor p^2 3-mal osztva 1 maradékot ad (lásd a 2.1-1. példát), tehát $p^2 + 2$ osztható 3-mal, ugyanakkor nagyobb 3-nál, így nem lehet prím. Ha azonban $p = 3$, akkor $p^2 + 2 = 11$, ami prím. ■

4.3-4.

$$n^4+4 = (n^2+2)^2-(2n)^2 = (n^2+2n+2)(n^2-2n+2) = ((n+1)^2+1)((n-1)^2+1)$$

Ebből leolvashatjuk, hogy legfeljebb $n = 1$, illetve $n = -1$ lehet a megoldás. Behelyettesítéssel meggyőződhetünk róla, hogy mindkét esetben 5 a kifejezés értéke, ami prímszám. ■

4.3-5.

a. Tegyük fel, hogy k összetett szám, tehát $k = a \cdot b$, ahol $1 < a < k$ és $1 < b < k$. Ekkor $2^a - 1 | 2^k - 1 = (2^a)^b - 1^b$, és $1 < 2^a - 1 < 2^k - 1$, tehát $2^k - 1$ nem prím.

b. $23 | 2^{11} - 1$ ■

4.3-6.

Tegyük fel, hogy $k = 2^n \cdot b$, ahol $b > 1$ páratlan szám, n nem negatív egész. Ekkor $2^{2^n} + 1 | (2^{2^n})^b + 1^b = 2^k + 1$. Másrészt $2^{2^n} + 1 \geq 2^{2^0} + 1 = 3$ miatt $1 < 2^{2^n} + 1 < 2^k + 1$, $2^{2^n} + 1$ valódi osztója $2^k + 1$-nek, tehát $2^k + 1$ nem prím. ■

4.3-7.

$2p - 1$, $2p$ és $2p + 1$ egyike osztható 3-mal. $2p$ pontosan akkor osztható 3-mal, ha p. A 3-mal osztható szám akkor lesz prím, ha értéke ± 3. A következő lehetőségeket kell megvizsgálnunk:

$2p-1$	p	$2p+1$
5	3	7
-7	-3	-5
1	1	3
-5	-2	-3
3	2	5
-3	-1	-1

$p = -3,\ -2,\ 2,\ 3$ esetén lesz mindhárom szám prím. ∎

4.3-8.

$$\begin{aligned} n^2+4 &= n^2-1+5 \\ n^2+16 &= n^2+1+15 \end{aligned}$$

Ha $5 \nmid n$, akkor $n^2 = 5k \pm 1$. A fenti két szám közül az egyik osztható 5-tel, s mivel prímszám kell legyen, csak 5 lehet az értéke. Ha $n^2+4 = 5$, akkor $n = 1$ és $n^2+16 = 17$. $n^2+16 = 5$ nem lehet. Az egyetlen megoldáspár az 5, 17.

∎

4.4. Euklideszi algoritmus

4.4-1. $a = 675$, $b = 471$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$675 = 471 \cdot 1 + 204$	$204 = 675 \cdot 1 + 471 \cdot (-1)$
$471 = 204 \cdot 2 + 63$	$63 = 675 \cdot (-2) + 471 \cdot 3$
$204 = 63 \cdot 3 + 15$	$15 = 675 \cdot 7 + 471 \cdot (-10)$
$63 = 15 \cdot 4 + 3$	$3 = 675 \cdot (-30) + 471 \cdot 43$
$15 = 3 \cdot 5 + 0$	$0 = 675 \cdot 157 + 471 \cdot (-225)$

lnko$(675, 471) = 3$, a lineáris kombinációs együtthatók: $x = -30$ és $y = 43$.

■

4.4-2. $a = 432$, $b = 300$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$432 = 300 \cdot 1 + 132$	$132 = 432 \cdot 1 + 300 \cdot (-1)$
$300 = 132 \cdot 2 + 36$	$36 = 432 \cdot (-2) + 300 \cdot 3$
$132 = 36 \cdot 3 + 24$	$24 = 432 \cdot 7 + 300 \cdot (-10)$
$36 = 24 \cdot 1 + 12$	$12 = 432 \cdot (-9) + 300 \cdot 13$
$24 = 12 \cdot 2 + 0$	$0 = 432 \cdot 25 + 300 \cdot (-36)$

lnko$(432, 300) = 12$, a lineáris kombinációs együtthatók: $x = -9$ és $y = 13$.

■

4.4-3. $a = 756$, $b = 333$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$756 = 333 \cdot 2 + 90$	$90 = 756 \cdot 1 + 333 \cdot (-2)$
$333 = 90 \cdot 3 + 63$	$63 = 756 \cdot (-3) + 333 \cdot 7$
$90 = 63 \cdot 1 + 27$	$27 = 756 \cdot 4 + 333 \cdot (-9)$
$63 = 27 \cdot 2 + 9$	$9 = 756 \cdot (-11) + 333 \cdot 25$
$27 = 9 \cdot 3 + 0$	$0 = 756 \cdot 37 + 333 \cdot (-84)$

lnko$(756, 333) = 9$, a lineáris kombinációs együtthatók: $x = -11$ és $y = 25$.

■

4.4-4. $a = 504$, $b = 150$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$504 = 150 \cdot 3 + 54$	$54 = 504 \cdot 1 + 150 \cdot (-3)$
$150 = 54 \cdot 2 + 42$	$42 = 504 \cdot (-2) + 150 \cdot 7$
$54 = 42 \cdot 1 + 12$	$12 = 504 \cdot 3 + 150 \cdot (-10)$
$42 = 12 \cdot 3 + 6$	$6 = 504 \cdot (-11) + 150 \cdot 37$
$12 = 6 \cdot 2 + 0$	$0 = 504 \cdot 25 + 150 \cdot (-84)$

$\text{lnko}(504, 150) = 6$, a lineáris kombinációs együtthatók: $x = -11$ és $y = 37$.

■

4.4-5. $a = 420$, $b = 154$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$420 = 154 \cdot 2 + 112$	$112 = 420 \cdot 1 + 154 \cdot (-2)$
$154 = 112 \cdot 1 + 42$	$42 = 420 \cdot (-1) + 154 \cdot 3$
$112 = 42 \cdot 2 + 28$	$28 = 420 \cdot 3 + 154 \cdot (-8)$
$42 = 28 \cdot 1 + 14$	$14 = 420 \cdot (-4) + 154 \cdot 11$
$28 = 14 \cdot 2 + 0$	$0 = 420 \cdot 11 + 154 \cdot (-30)$

$\text{lnko}(420, 154) = 14$, a lineáris kombinációs együtthatók: $x = -4$ és $y = 11$.

■

4.4-6. $a = 1080$, $b = 285$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$1080 = 285 \cdot 3 + 225$	$225 = 1080 \cdot 1 + 285 \cdot (-3)$
$285 = 225 \cdot 1 + 60$	$60 = 1080 \cdot (-1) + 285 \cdot 4$
$225 = 60 \cdot 3 + 45$	$45 = 1080 \cdot 4 + 285 \cdot (-15)$
$60 = 45 \cdot 1 + 15$	$15 = 1080 \cdot (-5) + 285 \cdot 19$
$45 = 15 \cdot 3 + 0$	$0 = 1080 \cdot 19 + 285 \cdot (-72)$

$\text{lnko}(1080, 285) = 15$, a lineáris kombinációs együtthatók: $x = -5$ és $y = 19$. ■

4.4-7. $a = 2016$, $b = 880$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$2016 = 880 \cdot 2 + 256$	$256 = 2016 \cdot 1 + 880 \cdot (-2)$
$880 = 256 \cdot 3 + 112$	$112 = 2016 \cdot (-3) + 880 \cdot 7$
$256 = 112 \cdot 2 + 32$	$32 = 2016 \cdot 7 + 880 \cdot (-16)$
$112 = 32 \cdot 3 + 16$	$16 = 2016 \cdot (-24) + 880 \cdot 55$
$32 = 16 \cdot 2 + 0$	$0 = 2016 \cdot 55 + 880 \cdot (-126)$

$\text{lnko}(2016, 880) = 16$, a lineáris kombinációs együtthatók: $x = -24$ és $y = 55$. ■

4.4-8. $a = 30$, $b = 22$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$30 = 22 \cdot 1 + 8$	$8 = 30 \cdot 1 + 22 \cdot (-1)$
$22 = 8 \cdot 2 + 6$	$6 = 30 \cdot (-2) + 22 \cdot 3$
$8 = 6 \cdot 1 + 2$	$2 = 30 \cdot 3 + 22 \cdot (-4)$
$6 = 2 \cdot 3 + 0$	$0 = 30 \cdot (-11) + 22 \cdot 15$

$\text{lnko}(30, 22) = 2$, a lineáris kombinációs együtthatók: $x = 3$ és $y = -4$. ■

4.4-9. $a = 430$, $b = 300$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$430 = 300 \cdot 1 + 130$	$130 = 430 \cdot 1 + 300 \cdot (-1)$
$300 = 130 \cdot 2 + 40$	$40 = 430 \cdot (-2) + 300 \cdot 3$
$130 = 40 \cdot 3 + 10$	$10 = 430 \cdot 7 + 300 \cdot (-10)$
$40 = 10 \cdot 4 + 0$	$0 = 430 \cdot (-30) + 300 \cdot 43$

lnko$(430, 300) = 10$, a lineáris kombinációs együtthatók: $x = 7$ és $y = -10$.

■

4.4-10. $a = 2355$, $b = 450$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$2355 = 450 \cdot 5 + 105$	$105 = 2355 \cdot 1 + 450 \cdot (-5)$
$450 = 105 \cdot 4 + 30$	$30 = 2355 \cdot (-4) + 450 \cdot 21$
$105 = 30 \cdot 3 + 15$	$15 = 2355 \cdot 13 + 450 \cdot (-68)$
$30 = 15 \cdot 2 + 0$	$0 = 2355 \cdot (-30) + 450 \cdot 157$

lnko$(2355, 450) = 15$, a lineáris kombinációs együtthatók: $x = 13$ és $y = -68$.

■

4.4-11. $a = 300$, $b = 132$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$300 = 132 \cdot 2 + 36$	$36 = 300 \cdot 1 + 132 \cdot (-2)$
$132 = 36 \cdot 3 + 24$	$24 = 300 \cdot (-3) + 132 \cdot 7$
$36 = 24 \cdot 1 + 12$	$12 = 300 \cdot 4 + 132 \cdot (-9)$
$24 = 12 \cdot 2 + 0$	$0 = 300 \cdot (-11) + 132 \cdot 25$

lnko$(300, 132) = 12$, a lineáris kombinációs együtthatók: $x = 4$ és $y = -9$. ■

4.4-12. $a = 518$, $b = 154$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$518 = 154 \cdot 3 + 56$	$56 = 518 \cdot 1 + 154 \cdot (-3)$
$154 = 56 \cdot 2 + 42$	$42 = 518 \cdot (-2) + 154 \cdot 7$
$56 = 42 \cdot 1 + 14$	$14 = 518 \cdot 3 + 154 \cdot (-10)$
$42 = 14 \cdot 3 + 0$	$0 = 518 \cdot (-11) + 154 \cdot 37$

lnko$(518, 154) = 14$, a lineáris kombinációs együtthatók: $x = 3$ és $y = -10$.

■

4.4-13. $a = 198$, $b = 72$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$198 = 72 \cdot 2 + 54$	$54 = 198 \cdot 1 + 72 \cdot (-2)$
$72 = 54 \cdot 1 + 18$	$18 = 198 \cdot (-1) + 72 \cdot 3$
$54 = 18 \cdot 3 + 0$	$0 = 198 \cdot 4 + 72 \cdot (-11)$

$\mathrm{lnko}(198, 72) = 18$, a lineáris kombinációs együtthatók: $x = -1$ és $y = 3$. ■

4.4-14. $a = 1100$, $b = 480$.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$1100 = 480 \cdot 2 + 140$	$140 = 1100 \cdot 1 + 480 \cdot (-2)$
$480 = 140 \cdot 3 + 60$	$60 = 1100 \cdot (-3) + 480 \cdot 7$
$140 = 60 \cdot 2 + 20$	$20 = 1100 \cdot 7 + 480 \cdot (-16)$
$60 = 20 \cdot 3 + 0$	$0 = 1100 \cdot (-24) + 480 \cdot 55$

$\mathrm{lnko}(1100, 480) = 20$, a lineáris kombinációs együtthatók: $x = 7$ és $y = -16$.

■

4.5. Kétváltozós lineáris diofantikus egyenletek

4.5-1. $60x + 16y = 60$
Az euklideszi algoritmussal számítsuk ki 60 és 16 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$60 = 16 \cdot 3 + 12$	$12 = 60 \cdot 1 + 16 \cdot (-3)$
$16 = 12 \cdot 1 + 4$	$4 = 60 \cdot (-1) + 16 \cdot 4$
$12 = 4 \cdot 3 + 0$	$0 = 60 \cdot 4 + 16 \cdot (-15)$

lnko$(60, 16) = 4$, a lineáris kombinációs együtthatók: $x' = -1$ és $y' = 4$.

Mivel $4|60$, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = (-1) \cdot 15 = -15 \qquad y_0 = y'\frac{c}{d} = 4 \cdot 15 = 60$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = -15 + 4t \qquad y_t = y_0 - t\frac{a}{(a,b)} = 60 - 15t \quad t \in \mathbb{Z}$$

■

4.5-2. $115x + 50y = 1100$

Az euklideszi algoritmussal számítsuk ki 115 és 50 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$115 = 50 \cdot 2 + 15$	$15 = 115 \cdot 1 + 50 \cdot (-2)$
$50 = 15 \cdot 3 + 5$	$5 = 115 \cdot (-3) + 50 \cdot 7$
$15 = 5 \cdot 3 + 0$	$0 = 115 \cdot 10 + 50 \cdot (-23)$

lnko$(115, 50) = 5$, a lineáris kombinációs együtthatók: $x' = -3$ és $y' = 7$.

Mivel $5|1100$, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = (-3) \cdot 220 = -660 \qquad y_0 = y'\frac{c}{d} = 7 \cdot 220 = 1540$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = -660 + 10t \qquad y_t = y_0 - t\frac{a}{(a,b)} = 1540 - 23t \quad t \in \mathbb{Z}$$

■

4.5-3. $374x + 99y = 297$

Az euklideszi algoritmussal számítsuk ki 374 és 99 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$374 = 99 \cdot 3 + 77$	$77 = 374 \cdot 1 + 99 \cdot (-3)$
$99 = 77 \cdot 1 + 22$	$22 = 374 \cdot (-1) + 99 \cdot 4$
$77 = 22 \cdot 3 + 11$	$11 = 374 \cdot 4 + 99 \cdot (-15)$
$22 = 11 \cdot 2 + 0$	$0 = 374 \cdot (-9) + 99 \cdot 34$

$\text{lnko}(374, 99) = 11$, a lineáris kombinációs együtthatók: $x' = 4$ és $y' = -15$.

Mivel $11|297$, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = 4 \cdot 27 = 108 \qquad y_0 = y'\frac{c}{d} = (-15) \cdot 27 = -405$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = 108 + 9t \qquad y_t = y_0 - t\frac{a}{(a,b)} = -405 - 34t \quad t \in \mathbb{Z}$$

■

4.5-4. $432x + 160y = 208$

Az euklideszi algoritmussal számítsuk ki 432 és 160 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$432 = 160 \cdot 2 + 112$	$112 = 432 \cdot 1 + 160 \cdot (-2)$
$160 = 112 \cdot 1 + 48$	$48 = 432 \cdot (-1) + 160 \cdot 3$
$112 = 48 \cdot 2 + 16$	$16 = 432 \cdot 3 + 160 \cdot (-8)$
$48 = 16 \cdot 3 + 0$	$0 = 432 \cdot (-10) + 160 \cdot 27$

$\text{lnko}(432, 160) = 16$, a lineáris kombinációs együtthatók: $x' = 3$ és $y' = -8$.

Mivel $16|208$, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = 3 \cdot 13 = 39 \qquad y_0 = y'\frac{c}{d} = (-8) \cdot 13 = -104$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = 39 + 10t \qquad y_t = y_0 - t\frac{a}{(a,b)} = -104 - 27t \quad t \in \mathbb{Z}$$

■

4.5-5. $117x + 81y = 891$
Az euklideszi algoritmussal számítsuk ki 117 és 81 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$117 = 81 \cdot 1 + 36$	$36 = 117 \cdot 1 + 81 \cdot (-1)$
$81 = 36 \cdot 2 + 9$	$9 = 117 \cdot (-2) + 81 \cdot 3$
$36 = 9 \cdot 4 + 0$	$0 = 117 \cdot 9 + 81 \cdot (-13)$

$\mathrm{lnko}(117, 81) = 9$, a lineáris kombinációs együtthatók: $x' = -2$ és $y' = 3$.
Mivel $9|891$, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = (-2) \cdot 99 = -198 \qquad y_0 = y'\frac{c}{d} = 3 \cdot 99 = 297$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = -198 + 9t \qquad y_t = y_0 - t\frac{a}{(a,b)} = 297 - 13t \quad t \in \mathbb{Z}$$

■

4.5-6. $323x + 85y = 323$
Az euklideszi algoritmussal számítsuk ki 323 és 85 legnagyobb közös osztóját, valamint a $d = ax + by$ lineáris kombinációs előállításhoz az x és y együtthatókat.

$r_n = r_{n+1}q_{n+1} + r_{n+2}$	$r_n = ax_n + by_n$
$323 = 85 \cdot 3 + 68$	$68 = 323 \cdot 1 + 85 \cdot (-3)$
$85 = 68 \cdot 1 + 17$	$17 = 323 \cdot (-1) + 85 \cdot 4$
$68 = 17 \cdot 4 + 0$	$0 = 323 \cdot 5 + 85 \cdot (-19)$

lnko$(323, 85) = 17$, a lineáris kombinációs együtthatók: $x' = -1$ és $y' = 4$.

Mivel $17|323$, megoldható az egyenlet, egy megoldáspár:

$$x_0 = x'\frac{c}{d} = (-1) \cdot 19 = -19 \qquad y_0 = y'\frac{c}{d} = 4 \cdot 19 = 76$$

Az összes megoldás:

$$x_t = x_0 + t\frac{b}{(a,b)} = -19 + 5t \qquad y_t = y_0 - t\frac{a}{(a,b)} = 76 - 19t \quad t \in \mathbb{Z}$$

■

4.6. Euler-féle φ függvény

4.6-1.

$m|n$ miatt $n = m \cdot s$. Ugyanakkor (X) alapján

$$\varphi(m) = m\prod_{p|m}\left(1 - \frac{1}{p}\right)$$

$$\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right) = m \cdot s \prod_{p|m\cdot s}\left(1 - \frac{1}{p}\right) =$$

$$= m \cdot s\prod_{p|m}\left(1 - \frac{1}{p}\right)\prod_{p|n,\, p\nmid m}\left(1 - \frac{1}{p}\right) =$$

$$= m\prod_{p|m}\left(1 - \frac{1}{p}\right) s \prod_{p|s,\, p\nmid m}\left(\frac{p-1}{p}\right),$$

ami igazolja az állítást. ■

4.6-2.
Felhasználjuk, hogy

$$\varphi(x) = x\prod_{p|x}\left(1-\frac{1}{p}\right).$$

Ez alapján:

$$2x\prod_{p|x}\left(1-\frac{1}{p}\right) = x,$$

$$2\prod_{p|x}\left(1-\frac{1}{p}\right) = 1.$$

Ez csak akkor lehetséges, ha x-nek egyetlen prímosztója van, és ez a 2. Az eredeti egyenletet az $x = 2^\alpha,\ \alpha \in \mathbb{N}$ számok elégítik ki. ∎

4.6-3.
Tegyük fel, hogy $n = 5^\alpha \cdot 7^\beta \cdot \gamma$, ahol $(\gamma, 5\cdot 7) = 1$. Legyen először $\alpha \geq 1$ és $\beta \geq 1$. Ekkor:

$$\begin{aligned}
\varphi(5n) &= \varphi(7n)\\
\varphi(5^{\alpha+1}\cdot 7^\beta\cdot\gamma) &= \varphi(5^\alpha\cdot 7^{\beta+1}\cdot\gamma)\\
\varphi(5^{\alpha+1})\cdot\varphi(7^\beta)\cdot\varphi(\gamma) &= \varphi(5^\alpha)\cdot\varphi(7^{\beta+1})\cdot\varphi(\gamma)\\
\varphi(5^{\alpha+1})\cdot\varphi(7^\beta) &= \varphi(5^\alpha)\cdot\varphi(7^{\beta+1})\\
5\cdot(5^\alpha-5^{\alpha-1})\cdot(7^\beta-7^{\beta-1}) &= (5^\alpha-5^{\alpha-1})\cdot 7\cdot(7^\beta-7^{\beta-1})
\end{aligned}$$

Az egyenletből egyszerűsítés után azt kapjuk, hogy $5 = 7$, ami ellentmondás.

Ha $\alpha \geq 1$ és $\beta = 0$, akkor az egyenlet a következőképpen alakul: $5 = 7-1$, ez megint csak ellentmondás. Ha $\alpha = 0$ és $\beta \geq 1$, akkor is ellentmondást kapunk, $5-1 = 7$. Végül ha $\alpha = 0$ és $\beta = 0$, akkor az $5-1 = 7-1$ ellentmondásra jutunk.

Az egyenletnek nincs megoldása. ∎

4.6-4.
1. *megoldás.*

$$105 = 3\cdot 5\cdot 7$$

A 105-nél nem nagyobb, 105-höz relatív prímek száma:

$$\varphi(105) = \varphi(3) \cdot \varphi(5) \cdot \varphi(7) = 2 \cdot 4 \cdot 6 = 48$$

A 210-nél nem nagyobb, 210-hez relatív prímek száma:

$$\varphi(210) = \varphi(2) \cdot \varphi(3) \cdot \varphi(5) \cdot \varphi(7) = 48 \tag{1}$$

Ez utóbbi számok fele esik az (1..105) tartományba, mert az 1. tételben beláttuk, hogy k és $m - k$ egyszerre relatív prímek m-hez. Tehát (1) alapján $\frac{48}{2} = 24$ olyan páratlan szám van 1 és 105 között, amelyek 105-höz relatív prímek. A 105-nél nem nagyobb, páros, 105-höz relatív prímek száma tehát

$$48 - \frac{48}{2} = 24.$$

2. *megoldás.* Az 1. tételben beláttuk, hogy k és $m-k$ egyszerre relatív prímek m-hez. Mivel $m = 105$ páratlan, ezért k és $105 - k$ egyike páros, a másika pedig páratlan. Tehát a 105-nél nem nagyobb páros i természetes számok száma éppen $\frac{\varphi(105)}{2} = 24$.

∎

4.6-5.

1. *megoldás.*

$$385 = 5 \cdot 7 \cdot 11$$

A 385-nél nem nagyobb, 385-höz relatív prímek száma:

$$\varphi(385) = \varphi(5) \cdot \varphi(7) \cdot \varphi(11) = 4 \cdot 6 \cdot 10 = 240$$

A 770-nél nem nagyobb, 770-hez relatív prímek száma:

$$\varphi(770) = \varphi(2) \cdot \varphi(5) \cdot \varphi(7) \cdot \varphi(11) = 240 \tag{1}$$

Ez utóbbi számok fele esik az (1..385) tartományba, mert az 1. tételben beláttuk, hogy k és $m - k$ egyszerre relatív prímek m-hez. Tehát (1) alapján $\frac{240}{2} = 120$ olyan páratlan szám van 1 és 385 között, amelyek 385-höz relatív prímek. A 385-nél nem nagyobb, páros, 385-höz relatív prímek száma tehát

$$240 - \frac{240}{2} = 120.$$

2. *megoldás.* Az 1. tételben beláttuk, hogy k és $m-k$ egyszerre relatív prímek m-hez. Mivel $m = 385$ páratlan, ezért k és $385 - k$ egyike páros, a másika pedig páratlan. Tehát a 385-nél nem nagyobb páros i természetes számok száma éppen $\frac{\varphi(385)}{2} = 120$. ■

4.6-6.

Például $n = m^k,\ k \in \mathbb{N}, k \geq 2$ esetén $m|\varphi(n)$. ■

4.6-7.

$$3600 = 2^4 \cdot 3^2 \cdot 5^2$$

A 3600-nál nem nagyobb, 3600-hoz relatív prím pozitív egészek száma:

$$\varphi(3600) = (2^4 - 2^3) \cdot (3^2 - 3) \cdot (5^2 - 5) = 8 \cdot 6 \cdot 20 = 960$$

A 3600-nál nem nagyobb, 3600-hoz nem relatív prím pozitív egészek száma:

$$3600 - \varphi(3600) = 3600 - 960 = 2640$$

■

4.6-8.

A 3600 és 7200 közötti, 3600-hoz relatív prímek száma megegyezik az 1 és 3600 közöttiek számával, ugyanis $(x, 3600) = 1$ pontosan akkor teljesül, amikor $(x + 3600, 3600) = 1$.

$\varphi(3600) = 960$. Mivel $7200 = 2 \cdot 3600$, ezért a megoldás $2 \cdot 960 = 1920$. ■

4.6-9.

$$25\ 200 = 7 \cdot 3600 \qquad \varphi(3600) = 960 \qquad 7 \cdot 960 = 6\ 720$$

■

4.6-10.

Legyen $n = 2^\alpha \cdot y, \quad (2, y) = 1$.
Ha $\alpha > 0$, akkor

$$\varphi(2n) = (2^{\alpha+1} - 2^\alpha)\varphi(y) = 2(2^\alpha - 2^{\alpha-1})\varphi(y)$$

$$\varphi(n) = (2^\alpha - 2^{\alpha-1})\varphi(y),$$

amiből $\varphi(2n) > \varphi(n)$.

Ha pedig $\alpha = 0$, akkor

$$\varphi(2n) = (2-1)\varphi(y)$$
$$\varphi(n) = \varphi(y)$$

ebből $\varphi(2n) = \varphi(n)$.

Így a megoldás a következő: **a.** n páratlan; **b.** n páros. ■

4.6-11.

Például $n = 5^k \quad k = 1,\ 2,\ \ldots$ esetén $\varphi(n) = 5^{k-1}\cdot 4$. ■

4.6-12.

Az egyenlet az alábbi alakban írható:

$$3^x(1-\frac{1}{3}) = 486$$

Ebből $\quad 2\cdot 3^{x-1} = 2\cdot 3^5, \quad x-1 = 5, \quad x = 6.$ ■

4.6-13.

$$\varphi(x) = x(1-\frac{1}{p})(1-\frac{1}{q}) = p^2q^2\cdot\frac{p-1}{p}\cdot\frac{q-1}{q} = pq(p-1)(q-1) \qquad (1)$$

$$\varphi(x) = 17\ 160 = 2^3\cdot 3\cdot 5\cdot 11\cdot 13$$

Tegyük fel, hogy $p < q$. Ekkor (1)-ben a $p,\ p-1,\ q-1$ tényezők mindegyike, s így a prímosztói is kisebbek q-nál. $\varphi(x)$ legnagyobb prímtényezője 13, tehát $q = 13$. Másrészt (1)-ből

$$p(p-1) = \frac{\varphi(x)}{q(q-1)} = \frac{2^3\cdot 3\cdot 5\cdot 11\cdot 13}{13\cdot 12} = 2\cdot 5\cdot 11.$$

A bal oldalon a legnagyobb prímosztó p, a jobb oldalon 11, amiből $p = 11$. A megoldás: $x = p^2q^2 = 11^2\cdot 13^2 = 121\cdot 169 = 20\ 449$ ■

4.6-14.

$$\varphi(x) = x(1 - \frac{1}{p})(1 - \frac{1}{q}) = p^2q^2 \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} = pq(p-1)(q-1) \qquad (1)$$

$$\varphi(x) = 2200 = 2^3 \cdot 5^2 \cdot 11$$

Tegyük fel, hogy $p < q$. Ekkor (1)-ben a $p,\ p-1,\ q-1$ tényezők mindegyike, s így a prímosztói is kisebbek q-nál. $\varphi(x)$ legnagyobb prímtényezője 11, tehát $q = 11$. Másrészt (1)-ből

$$p(p-1) = \frac{\varphi(x)}{q(q-1)} = \frac{2^3 \cdot 5^2 \cdot 11}{11 \cdot 10} = 2^2 \cdot 5.$$

A bal oldalon a legnagyobb prímosztó p, a jobb oldalon 5, amiből $p = 5$. A megoldás:

$$x = p^2q^2 = 5^2 \cdot 11^2 = 25 \cdot 121 = 3025$$

■

4.6-15.

$$\varphi(x) = x(1 - \frac{1}{p})(1 - \frac{1}{q}) = p^2q^2 \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} = pq(p-1)(q-1) \qquad (1)$$

$$\varphi(x) = 120 = 2^3 \cdot 3 \cdot 5$$

Tegyük fel, hogy $p < q$. Ekkor (1)-ben a $p,\ p-1,\ q-1$ tényezők mindegyike, s így a prímosztói is kisebbek q-nál. $\varphi(x)$ legnagyobb prímtényezője 5, tehát $q = 5$. Másrészt (1)-ből

$$p(p-1) = \frac{\varphi(x)}{q(q-1)} = \frac{2^3 \cdot 3 \cdot 5}{5 \cdot 4} = 3 \cdot 2.$$

A bal oldalon a legnagyobb prímosztó p, a jobb oldalon 3, amiből $p = 3$. A megoldás: $x = p^2q^2 = 3^2 \cdot 5^2 = 9 \cdot 25 = 225$ ■

4.6-16.

$$\varphi(x) = x(1-\frac{1}{p})(1-\frac{1}{q}) = p^2q^2 \cdot \frac{p-1}{p} \cdot \frac{q-1}{q} = pq(p-1)(q-1) \qquad (1)$$

$$\varphi(x) = 840 = 2^3 \cdot 3 \cdot 5 \cdot 7$$

Tegyük fel, hogy $p < q$. Ekkor (1)-ben a p, $p-1$, $q-1$ tényezők mindegyike, s így a prímosztói is kisebbek q-nál. $\varphi(x)$ legnagyobb prímtényezője 7, tehát $q = 7$. Másrészt (1)-ből

$$p(p-1) = \frac{\varphi(x)}{q(q-1)} = \frac{2^3 \cdot 3 \cdot 5 \cdot 7}{7 \cdot 6} = 2^2 \cdot 5.$$

A bal oldalon a legnagyobb prímosztó p, a jobb oldalon 5, amiből $p = 5$. A megoldás:

$$x = p^2q^2 = 5^2 \cdot 7^2 = 25 \cdot 49 = 1225$$

■

4.6-17.

$$\varphi(mn) = mn \prod_{p|mn} \left(1 - \frac{1}{p}\right) \qquad (1)$$

$$\varphi(m)\varphi(n) = m \prod_{p|m} \left(1 - \frac{1}{p}\right) n \prod_{p|n} \left(1 - \frac{1}{p}\right) \qquad (2)$$

(1) tényezői megtalálhatók (2)-ben, (2)-ben ezen kívül még előfordul a

$$\prod_{p|m \wedge p|n} \left(1 - \frac{1}{p}\right)$$

tényező. Ez utóbbi kisebb 1-nél, és így (1) értéke nagyobb vagy egyenlő, mint (2) értéke. Ebből az is következik, hogy egyenlőség akkor és csak akkor áll fenn, ha m és n relatív prímek. ■

4.6-18.

150 kanonikus alakja $150 = 2 \cdot 3 \cdot 5^2$. Azokat a 2005-nél nem nagyobb számokat keressük, amelyek $2, 3, 5$ egyikével sem oszthatók. A logikai szita formulát alkalmazzuk. A szóba jöhető 2005 egész szám közül el kell venni azokat, amelyek 2, 3, illetve 5 valamelyikével oszthatóak.

A 2-vel osztható számok száma $[\frac{2005}{2}] = 1002$, hiszen minden második szám ilyen. A 3-mal oszthatóak száma $[\frac{2005}{3}] = 668$, 5-tel osztható pedig $[\frac{2005}{5}] = 401$ van. Ha ezeket az értékeket kivonjuk 2005-ből, lesznek olyan számok, amelyeket kétszer vettünk el, mégpedig a 2-vel és 3-mal is oszthatóakat (ezek száma $[\frac{2005}{2 \cdot 3}]$), a 2-vel és 5-tel, valamint a 3-mal és 5-tel oszthatóakat. Ezek számát tehát vissza kell adni az eddig kapott értékhez. A 2, 3 és 5-tel is oszthatók száma viszont 3-szor lett kivonva, 3-szor visszaadtuk, tehát újra le kell vonnunk. Így a következő képlethez jutunk:

$$2005 - \left[\frac{2005}{2}\right] - \left[\frac{2005}{3}\right] - \left[\frac{2005}{5}\right] + \left[\frac{2005}{2 \cdot 3}\right] + \left[\frac{2005}{2 \cdot 5}\right] + \left[\frac{2005}{3 \cdot 5}\right] - \left[\frac{2005}{2 \cdot 3 \cdot 5}\right] =$$

$$= 2005 - 1002 - 668 - 401 + 334 + 133 + 200 - 66 = 535$$

■

4.7. Kongruenciák, maradékrendszerek, Euler–Fermat-tétel

4.7.1. Kongruenciák, maradékrendszerek

4.7-1.

1. $$\left.\begin{array}{l} a \equiv b \pmod m \\ c \equiv d \pmod m \end{array}\right\} \rightarrow \quad a + c \equiv b + d \pmod m$$

2. $$\left.\begin{array}{l} a \equiv b \pmod m \\ c \equiv d \pmod m \end{array}\right\} \rightarrow \quad ac \equiv bd \pmod m$$

3. $$ac \equiv bc \pmod m \quad \Leftrightarrow \quad a \equiv b \pmod{\tfrac{m}{(m,c)}}$$

I. Ha

$$a \equiv b \pmod m \text{ és } c \equiv d \pmod m \tag{1}$$

teljesül, akkor

$$m|a-b \text{ és } m|c-d, \tag{2}$$

de akkor $m|a-b+c-d=(a+c)-(b+d)$ is igaz, ami azt jelenti, hogy $a+c\equiv b+d \pmod{m}$, tehát 1.-et beláttuk.

Másrészt (1)-ből az is következik, hogy $m|c(a-b)+b(c-d)=ac-bd$, vagyis $ac\equiv bd \pmod{m}$, tehát 2. is teljesül.

II. a. Legyen először $ac\equiv bc \pmod{m}$, vagyis $m|c(a-b)$. Létezik tehát olyan q egész, amellyel $mq=c(a-b)$. Ebből:

$$\frac{m}{(m,c)}q=\frac{c}{(m,c)}(a-b) \qquad \frac{m}{(m,c)}\,\bigg|\,\frac{c}{(m,c)}(a-b)$$

Mivel nyilvánvalóan

$$\left(\frac{m}{(m,c)},\frac{c}{(m,c)}\right)=1 \qquad \frac{m}{(m,c)}\,\bigg|\,(a-b)$$

is igaz, ez pedig az $a\equiv b \pmod{\frac{m}{(m,c)}}$ kongruencia tejesülését jelenti.

b. Tegyük fel most, hogy

$$a\equiv b \pmod{\frac{m}{(m,c)}}, \quad \text{ami azt jelenti, hogy} \quad \frac{m}{(m,c)}\,\bigg|\,a-b.$$

Létezik tehát q egész, melyre $\frac{m}{(m,c)}q=a-b$. c-vel beszorozva az egyenletet $m\frac{c}{(m,c)}q=ac-bc$, és mivel $\frac{c}{(m,c)}$ is egész, $m|ac-bc$, vagyis $ac\equiv bc \pmod{m}$.

■

4.7-2. $a_1,\ a_2,\ \ldots,\ a_m$ teljes maradékrendszer, $b_1,\ b_2,\ \ldots,\ b_{\varphi(m)}$ redukált maradékrendszer modulo m

1. $(a,m)=1 \quad\rightarrow\quad aa_1+c,\ aa_2+c,\ \ldots,\ aa_m+c$ teljes maradékrendszer modulo m

2. $(a,m)=1 \quad\rightarrow\quad ab_1,\ ab_2,\ \ldots,\ ab_{\varphi(m)}$ redukált maradékrendszer modulo m

Az 1. sorozat elemszáma nyilván m, másrészt inkongruensek az elemek, hiszen ha $aa_i+c\equiv aa_j+c \pmod{m}$, akkor $aa_i\equiv aa_j \pmod{m}$ és $(a,m)=1$ miatt

$a_i \equiv a_j \pmod m$ teljesül. Így az első sorozat elemei teljes maradékrendszert alkotnak.

Most igazoljuk a 2. állítást. Az elméleti összefoglalóban felsorolt három ismérv közül az első, tudniillik az, hogy az elemszám $\varphi(m)$, nyilván teljesül. Bármely két különböző elem inkongruens is, hiszen ha $ab_i \equiv ab_j \pmod m$, akkor $(a, m) = 1$ miatt megint $b_i \equiv b_j \pmod m$. Az is igaz, hogy az elemek m-hez relatív prímek, tehát 2. elemei redukált maradékrendszert alkotnak. ■

4.7-3.

Egyrészt
$$641 = 625 + 16 = 5^4 + 2^4,$$
másrészt
$$641 = 640 + 1 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1,$$
amiből
$$5 \cdot 2^7 \equiv -1 \pmod{641},$$
s így
$$5^4 \cdot 2^{28} \equiv 1 \pmod{641}.$$
Ehhez hozzáadva a
$$2^{32} \equiv 2^{32} \pmod{641}$$
kongruenciát a
$$2^{28}(5^4 + 2^4) \equiv 1 + 2^{32} \pmod{641}$$
kongruenciát kapjuk, amiből
$$2^{28} \cdot 641 \equiv 2^{32} + 1 \equiv 0 \pmod{641},$$

s így valóban $641 | 2^{32} + 1$, tehát az F_5 Fermat-szám nem prím. ■

4.7-4.

A halmaz elemeinek száma m és páronként inkongruensek. Ez utóbbi abból következik, hogy $2i \equiv 2j \pmod m$ esetén $i \equiv j \pmod m$, tehát $i = j$. ■

4.7-5.

Nézzük meg, hogy vannak-e közöttük kongruensek. $x^2 \equiv y^2 \pmod{m}$ esetén $m|x^2-y^2 = (x-y)(x+y)$. Ha $m = x+y$ és $x \neq y$, akkor x^2 és y^2 kongruensek egymással. Lássuk például modulo 5 és modulo 6 ezeket a számokat:

x		1	2	3	4	5
x^2	(mod 5)	1	4	4	1	0

x		1	2	3	4	5	6
x^2	(mod 6)	1	4	3	4	1	0

■

4.7-6.

Legyen a teljes maradékrendszer $a_1,\ a_2,\ \ldots,\ a_m$. Ekkor

$$\sum_{i=1}^{m} a_i \equiv \sum_{i=1}^{m} i \pmod{m},$$

$$\sum_{i=1}^{m} i = m\frac{m+1}{2}.$$

Ez az érték pontosan akkor kongruens nullával modulo m, ha $m+1$ osztható 2-vel, tehát ha m páratlan. ■

4.7-7.

a. modulo 6: $\{1,\ 5\}$

b. modulo 7: $\{1,\ 2,\ 3,\ 4,\ 5,\ 6\}$

c. modulo 12: $\{1,\ 5,\ 7,\ 11\}$

d. modulo 18: $\{1,\ 5,\ 7,\ 11,\ 13,\ 17\}$

e. modulo 20: $\{1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19\}$ ■

4.7-8.
Legyen $p > 2$ prím, valamint a modulo p redukált maradékrendszer

$$a_1,\ a_2,\ \dots,\ a_{\varphi(p)}.$$

$\varphi(p) = p - 1$, és így

$$\sum_{i=1}^{p-1} a_i \equiv \sum_{i=1}^{p-1} i \pmod{p},$$

$$\sum_{i=1}^{p-1} i = \frac{p-1}{2} \cdot p.$$

$\frac{p-1}{2}$ egész szám, tehát a redukált maradékrendszer elemeinek összege osztható p-vel. ■

4.7-9.
Legyen a redukált maradékrendszer $a_1,\ a_2,\ \dots,\ a_{\varphi(m)}$, és $m > 2$. Ekkor

$$\sum_{i=1}^{\varphi(m)} a_i \equiv \sum_{\substack{1 \le i \le \varphi(m) \\ (i,m)=1}} i \pmod{m}.$$

Az utóbbi szummában szereplő számok olyan párokká alakíthatók, amelyek összege m – lásd az Euler-féle φ függvényre vonatkozó 2.6.1 tételt –, így a teljes összeg kongruens nullával modulo m. ■

4.7-10.
a.

$$\sum_{i=1}^{2004} i = \frac{2004 \cdot 2005}{2} = 2\,009\,010$$

b.

$$2004 = 2^2 \cdot 3 \cdot 167 \text{ és } \varphi(2004) = 2 \cdot 2 \cdot 166 = 664$$

Így a keresett összeg – felhasználva a 2.6-4. példa eredményét –:

$$\varphi(2004) \cdot \frac{2004}{2} = 664 \cdot 1002 = 665\,328$$

■

4.7-11.

a.

$$\sum_{i=1}^{2005} i = \frac{2005 \cdot 2006}{2} = 2\,011\,015$$

b.

$$2005 = 5 \cdot 401 \text{ és } \varphi(2005) = 4 \cdot 400 = 1600$$

Így a keresett összeg – a 2.6-4. példa eredményét felhasználva –:

$$\frac{\varphi(2005) \cdot 2005}{2} = \frac{1600 \cdot 2005}{2} = 1\,604\,000$$

■

4.7-12.

Nem, mert nem mindegyik pár inkongruens. Például:

$$1 \cdot 2 \equiv (p-2) \cdot (p-1) \pmod p$$

■

4.7-13.

Vizsgáljuk meg, hogy két szám mikor lesz kongruens modulo nk.

$$\begin{aligned} a_i + nb_j &\equiv a_r + nb_s \pmod{nk} \\ a_i + nb_j &\equiv a_r + nb_s \pmod{n} \\ a_i &\equiv a_r \pmod{n} \\ i &= r \end{aligned}$$

Másrészt:

$$\begin{aligned} a_i + nb_j &\equiv a_i + nb_s \pmod{nk} \\ nb_j &\equiv nb_s \pmod{nk} \\ b_j &\equiv b_s \pmod{k} \\ j &= s \end{aligned}$$

Tehát a két szám csak akkor lehet kongruens modulo nk, ha megegyeznek. Mivel számuk nk, így teljes maradékrendszert alkotnak modulo nk. ∎

4.7-14.

a. Tegyük fel, hogy (1) redukált maradékrendszer. Mivel (2) elemszáma $\varphi(m)$, és $(a_i^3, m) = 1$-ből következik $(a_i, m) = 1$, csak azt kell megvizsgálnunk, hogy (2) elemei inkongruensek-e egymással. Ha $a_i \equiv a_j \pmod{m}$, akkor $a_i^3 \equiv a_j^3 \pmod{m}$, tehát (2) elemei inkongruensek, és így ha (1) redukált maradékrendszer, akkor (2) is az.

b. Tegyük fel most, hogy (2) redukált maradékrendszer. (1) elemeinek a száma $\varphi(m)$, és ha $(a_i, m) = 1$, akkor $(a_i^3, m) = 1$. Elég tehát megnézni, hogy (1) elemei inkongruensek-e egymással. Tegyük fel, hogy

$$a_i^3 \equiv a_j^3 \pmod{m}. \tag{3}$$

Ekkor

$$a_i^{3k} \equiv a_j^{3k} \pmod{m}. \tag{4}$$

Másrészt

$$a_i^{\varphi(m)} \equiv a_j^{\varphi(m)} \equiv 1 \pmod{m},$$

és így

$$a_i^{3k+2} \equiv a_j^{3k+2} \pmod{m}. \tag{5}$$

(4) és (5)-ből pedig, mivel $(a_i, m) = 1$,

$$a_i^2 \equiv a_j^2 \pmod{m}, \tag{6}$$

majd (3) és (6) alapján, támaszkodva arra, hogy $(a_i, m) = 1$,

$$a_i \equiv a_j \pmod{m}$$

következik. Beláttuk, hogy ha (2) redukált maradékrendszer, akkor (1) is az.

∎

4.7-15.

Az a_i és b_j, valamint az $a_i \cdot b_j$ számok helyett tekinthetjük a velük modulo p kongruens 1 és $p - 1$ közé eső számokat. Nézzük a szorzótáblát modulo p. Minden sorban és minden oszlopban minden elem pontosan egyszer fordul elő. Menjünk végig az $1, \ldots, p-1$ elemeken, és válasszunk nekik szorzópárt lehetőleg úgy, hogy a szorzat ne szerepeljen az eddig kapottak között.

Megmutatjuk, hogy előbb-utóbb elakadunk. Ha soronként haladunk, és egy párt már lerögzítettünk, akkor a továbbiakban nem választhatunk ebből az oszlopból, valamint nem választhatjuk ezt az értéket sem, ami a többi oszlopban más-más sorban fordul elő. Legkésőbb az utolsó választásunknál olyan érték marad az egyetlen lehetséges oszlopban, ami korábban már előfordult. Nézzük például a modulo 7 tekintett szorzótáblát:

modulo 7	1	2	3	4	5	6
1	1	2	3	4	5	$\underline{6}$
2	2	4	6	1	$\underline{3}$	5
3	3	6	2	$\underline{5}$	1	4
4	4	$\underline{1}$	5	2	6	3
5	$\underline{5}$	3	1	6	4	2
6	6	5	$\underline{4}$	3	2	1

Egy lehetséges választás az alábbi, amely az $a_i = 5$ esetén akadt el:

a_i	1	2	3	4	5	6
b_j	6	5	4	2	1	3
$a_i \cdot b_j$	6	3	5	1	5	4

■

4.7-16.

Mindegyik számhoz található egy másik, amellyel való szorzatuk 1-gyel kongruens modulo p, hiszen az $ax \equiv 1 \pmod{p}$ egyenletnek pontosan akkor van megoldása, ha $a \nmid p$ (lásd a lineáris kongruenciák megoldását a 2.8. fejezetben). Másrészt csak az $\overline{1}$ és $\overline{-1}$ maradékosztályokhoz tartozó elemek inverze önmaga. Ha ugyanis

$$a^2 \equiv 1 \pmod{p},$$

akkor

$$a^2 - 1 \equiv 0 \pmod{p},$$

amiből $(a-1)(a+1) \equiv 0 \pmod{p}$, tehát $p|(a-1)(a+1)$. Mivel p prím, csak $p|a-1$, illetve $p|a+1$ lehet, tehát $a \equiv 1 \pmod{p}$ vagy $a \equiv -1 \pmod{p}$.

Párosítsuk össze tehát a számokat úgy, hogy szorzatuk 1-et adjon. A párosításból csak az 1 és -1 marad ki, amivel az eddigi szorzatot – az 1-et – még meg kell szoroznunk. A végeredmény tehát -1. ■

4.7.2. Euler–Fermat-tétel

4.7-17.

a. $(n, 7) = 1$ miatt a Fermat-tétel első alakja alkalmazható. $n^6 \equiv 1 \pmod 7$, ez pedig éppen az állítás.

b. $(n, 7) = 1$ miatt a Fermat-tétel első alakja alkalmazható. $n^6 \equiv 1 \pmod 7$, amiből négyzetre emeléssel $n^{12} \equiv 1 \pmod 7$, s ez éppen az állítás.

c. $(n, 7) = 1$ miatt a Fermat-tétel első alakja alkalmazható. $n^6 \equiv 1 \pmod 7$, amit k-adik hatványra emelve $n^{6k} \equiv 1 \pmod 7$. Ez éppen az állítás. ∎

4.7-18.

Mivel $42 = 2 \cdot 3 \cdot 7$, nézzük meg, hogy a kongruencia fennáll-e modulo 2, 3 és 7.

$$x^7 \equiv x \pmod 7 \tag{1}$$

a Fermat-tétel második alakjának felírása.

$$x^2 \equiv 1 \pmod 3$$

a Fermat-tétel első alakjának alkalmazása, amiből

$$x^6 \equiv 1 \pmod 3$$

következik. Ha pedig beszorozzuk a kongruenciát x-szel, akkor

$$x^7 \equiv x \pmod 3. \tag{2}$$

Nyilván fennáll

$$x^7 \equiv x \pmod 2, \tag{3}$$

hiszen x^7 pontosan akkor páros, amikor x. Mivel 2, 3 és 7 páronként relatív prímek, így (1), (2) és (3) alapján

$$x^7 \equiv x \pmod{42}$$

is fennáll. ∎

4.7-19.

Olyan x értéket keresünk, amelyre $x \equiv 3^{1003} \pmod{1000}$. Mivel $1000 = 8 \cdot 125$, megoldjuk a kongruenciát modulo 8 és modulo 125 is. $\varphi(8) = 4$ és az Euler-tétel miatt $3^4 \equiv 1 \pmod 8$, 250-edik hatványra emelve $3^{1000} \equiv 1 \pmod 8$, így $x \equiv 3^{1003} \equiv 3^3 \pmod 8$. $\varphi(125) = 100$ és az Euler-tétel miatt $3^{100} \equiv 1 \pmod{125}$, 10-edik hatványra emelve $3^{1000} \equiv 1 \pmod{125}$, így $x \equiv 3^{1003} \equiv 3^3 \pmod{125}$. Mivel a kongruencia fennáll modulo 8 és modulo 125 is, és $(8, 125) = 1$, így fennáll modulo 1000 is, s a keresett érték $3^3 = 27$.

■

4.7-20.

Egyrészt $\varphi(17) = 16$, és mivel $(3, 17) = 1$, a Fermat-tételre támaszkodva $3^{16} \equiv 1 \pmod{17}$. Másrészt $173 \equiv 3 \pmod{17}$. Ezeket felhasználva:

$$173^{163} \equiv 3^{163} = 3^{16 \cdot 10+3} = (3^{16})^{10} \cdot 3^3 \equiv 3^3 = 27 \equiv 10 \pmod{17}$$

Az osztási maradék 10. ■

4.7-21.

Olyan x értéket keresünk, amelyre

$$x \equiv 143^{143} \pmod{27}.$$

$$143^{143} \equiv 8^{143} \pmod{27}$$

$(8, 27) = 1$, valamint $\varphi(27) = 3^3 - 3^2 = 18$, az Euler-tételt alkalmazva $8^{18} \equiv 1 \pmod{27}$. Ezt felhasználva kongruenciánk így alakul:

$$8^{143} = 8^{18 \cdot 7+17} = (8^{18})^7 \cdot 8^{17} \equiv 8^{17} = (64)^8 \cdot 8 \equiv 10^8 \cdot 8 \equiv 100^4 \cdot 8 \equiv$$

$$\equiv 19^4 \cdot 8 \equiv (-8)^4 \cdot 8 = 64^2 \cdot 8 \equiv 10^2 \cdot 8 \equiv 19 \cdot 8 = 152 \equiv 17 \pmod{27}$$

A tízes számrendszerben kiszámított 17 a hármas számrendszerben felírva 122.

■

4.7-22.

$$x \equiv 205^{206^{207}} \equiv (-1)^{206^{207}} \equiv 1 \pmod{103}$$

■

4.7-23.
Olyan x értéket keresünk, amelyre

$$x \equiv 37^{39^{42}} \pmod{100}.$$

Mivel $\varphi(100) = \varphi(4 \cdot 25) = 2 \cdot 20 = 40$, valamint $(37, 100) = 1$, az Euler-tételt alkalmazva azt kapjuk, hogy $37^{40} \equiv 1 \pmod{100}$. Így a 39^{42} kitevő 40-nel való osztási maradékát keressük.

$$y \equiv 39^{42} \equiv (-1)^{42} \equiv 1 \pmod{40}$$

A kitevő osztási maradéka 1, így $37^{39^{42}} \equiv 37 \pmod{100}$, tehát a $37^{39^{42}}$ szám utolsó két számjegye 37. ■

4.7-24.
A keresett x értékre a következő teljesül: $x \equiv 403^{402} \pmod{1000}$. Mivel $\varphi(1000) = 400$ és $(403, 1000) = 1$, így az Euler-tétel alkalmazható, $403^{400} \equiv 1 \pmod{1000}$.

$$403^{402} \equiv 403^2 = (4 \cdot 10^2 + 3)^2 = 16 \cdot 10^4 + 24 \cdot 10^2 + 9 \equiv 409 \pmod{1000}.$$

Az utolsó három számjegy 409. ■

4.7-25.
Az alábbi kongruencia megoldását keressük:

$$x \equiv 519^{6803} \pmod{100}$$

$$519^{6803} \equiv 19^{6803} \pmod{100}$$

$(19, 100) = 1$, és $\varphi(100) = 40$. Az Euler-tétel szerint $19^{40} \equiv 1 \pmod{100}$. Ezt felhasználva:

$$19^{6803} \equiv 19^3 = 661 \cdot 19 \equiv 61 \cdot 19 = 1159 \equiv 59 \pmod{100}$$

Az utolsó két számjegy 59. ■

4.7-26.

Az $x \equiv 3^{400} \pmod{10}$ kongruencia megoldását keressük. $(3,10)=1$, $\varphi(10)=4$ és így $3^4 \equiv 1 \pmod{10}$. Ezt 100-adik hatványra emelve $3^{400} \equiv 1 \pmod{10}$, tehát az utolsó számjegy az 1-es. ■

4.7-27.

Az $x \equiv 3^{404} \pmod{100}$ kongruencia megoldását keressük. $(3,100)=1$, $\varphi(100)=40$ és így $3^{40} \equiv 1 \pmod{100}$. Ezt 10-edik hatványra emelve $3^{400} \equiv 1 \pmod{100}$. Ebből $3^{404} \equiv 3^4 = 81 \pmod{100}$. Az utolsó két számjegy 81. ■

4.7-28.

Az $x \equiv 17^{3^{1997}} \pmod{64}$ kongruencia megoldása a feladat.

$(17,64)=1$, és $\varphi(64)=\varphi(2^6)=2^6-2^5=32$, s így az Euler-tételt alkalmazhatjuk. $17^{32} \equiv 1 \pmod{64}$. A kitevő 32-vel való osztási maradékát kell kiszámítanunk. $y \equiv 3^{1997} \pmod{32}$. $(3,32)=1$, és $\varphi(32)=16$, s újra az Euler-tételt alkalmazva $3^{16} \equiv 1 \pmod{32}$.

$$3^{1997} = 3^{16\cdot 124+13} = (3^{16})^{124}\cdot 3^{13} \equiv 3^{13} = (3^4)^3\cdot 3 = (81)^3 \cdot 3 \equiv 17^3\cdot 3 =$$

$$= 289\cdot 17\cdot 3 \equiv 17\cdot 3 = 51 \equiv 19 \pmod{32}$$

Visszatérve az eredeti kongruenciához:

$$17^{3^{1997}} \equiv 17^{19} = (17^2)^9\cdot 17 \equiv (33^2)^4\cdot 33\cdot 17 =$$

$$= 1089^4\cdot 33\cdot 17 \equiv 33\cdot 17 \equiv 49 \pmod{64}$$

A kapott 49 nyolcas számrendszerben felírva 61. ■

4.7-29.

a. Az $x \equiv 323^{149} \pmod{63}$ kongruenciát kell megoldanunk.

$$323^{149} \equiv 8^{149} \pmod{63}$$

$(8,63)=1$ és $\varphi(63)=\varphi(3^2\cdot 7)=6\cdot 6=36$. Az Euler-tétel alkalmazzuk:

$$8^{36} \equiv 1 \pmod{63}$$

Ez alapján

$$8^{149} = 8^{36\cdot 4+5} = (8^{36})^4 \cdot 8^5 \equiv 8^5 = (8^2)^2 \cdot 8 = 64^2 \cdot 8 \equiv 8 \pmod{63}.$$

A keresett osztási maradék 8.
b. Az $x \equiv 423^{173} \pmod{52}$ kongruenciát kell megoldanunk.

$$423^{173} \equiv 7^{173} \pmod{52}$$

$(7,52) = 1$ és $\varphi(52) = \varphi(2^2 \cdot 13) = 2 \cdot 12 = 24$. Az Euler-tétel alkalmazzuk:

$$7^{24} \equiv 1 \pmod{52}$$

Ez alapján

$$7^{173} = 7^{24\cdot 7+5} = (7^{24})^7 \cdot 7^5 \equiv 7^5 = (7^2)^2 \cdot 7 \equiv (-3)^2 \cdot 7 =$$

$$= 9 \cdot 7 = 63 \equiv 11 \pmod{52}.$$

A keresett osztási maradék 11.
c. Az $x \equiv 495^{173} \pmod{98}$ kongruenciát kell megoldanunk.

$$495^{173} \equiv 5^{173} \pmod{98}$$

$(5,98) = 1$ és $\varphi(98) = \varphi(2 \cdot 7^2) = 42$. Az Euler-tétel alkalmazzuk:

$$5^{42} \equiv 1 \pmod{98}$$

Ez alapján

$$5^{173} = 5^{42\cdot 4+5} = (5^{42})^4 \cdot 5^5 \equiv 5^5 = 5^4 \cdot 5 = 625 \cdot 5 \equiv$$

$$\equiv 37 \cdot 5 = 185 \equiv 87 \pmod{98}.$$

A keresett osztási maradék 87.
d. Az $x \equiv 457^{101} \pmod{90}$ kongruenciát kell megoldanunk.

$$457^{101} \equiv 7^{101} \pmod{90}$$

$(7,90) = 1$ és $\varphi(90) = \varphi(2 \cdot 3^2 \cdot 5) = 6 \cdot 4 = 24$. Az Euler-tétel alkalmazzuk:

$$7^{24} \equiv 1 \pmod{90}$$

Ez alapján

$$7^{101} = 7^{24\cdot 4+5} = (7^{24})^4 \cdot 7^5 \equiv 7^5 = 7^3 \cdot 7^2 = 343 \cdot 7^2 \equiv 73 \cdot 49 \equiv$$

$$\equiv (-17) \cdot 49 = -833 \equiv 67 \pmod{90}.$$

A keresett osztási maradék 67. ∎

4.7-30.
A következő kongruencia megoldását keressük:

$$x \equiv 11^{1999^{26}} \pmod{100} \tag{1}$$

Az Euler-tételt alkalmazva $11^{40} \equiv 1 \pmod{100}$. Az (1)-ben szereplő kitevő 40-nel való osztási maradékát keressük.

$$y \equiv 1999^{26} \equiv (-1)^{26} = 1 \pmod{40}$$

Eszerint (1) így alakul:

$$11^{1999^{26}} \equiv 11 \pmod{100}$$

A keresett két jegy 11. ∎

4.7-31.
a. $n^{13} - n$ osztható 2-vel, mert n^{13} és n ugyanakkor páros, illetve páratlan.
b. 1. *megoldás.* Ha $3|n$, akkor $3|n^{13}$ is, így $3|n^{13} - n$. Tegyük fel, hogy $3 \nmid n$. $\varphi(3) = 2$, és így $n^2 \equiv 1 \pmod 3$, amit 6-odik hatványra emelve $n^{12} \equiv 1 \pmod 3$, ezt pedig n-nel beszorozva $n^{13} \equiv n \pmod 3$. Ez azt jelenti, hogy $n^{13} - n$ osztható 3-mal.
2. *megoldás.* A Fermat-tétel 2. alakja szerint $n^3 \equiv n \pmod 3$. Ezt alkalmazzuk az alábbi átalakításban:

$$n^{13} \equiv (n^3)^4 \cdot n \equiv n^4 \cdot n = n^5 = n^3 \cdot n^2 \equiv n \cdot n^2 = n^3 \equiv n \pmod 3$$

Ez pedig azt jelenti, hogy $n^{13} - n$ osztható 3-mal.
c. 1. *megoldás.* Ha $5|n$, akkor $5|n^{13}$ is, így $5|n^{13} - n$. Tegyük fel, hogy $5 \nmid n$. $\varphi(5) = 4$, és így $n^4 \equiv 1 \pmod 5$, amit harmadik hatványra emelve $n^{12} \equiv 1 \pmod 5$, ezt pedig n-nel beszorozva $n^{13} \equiv n \pmod 5$. Ebből következik az oszthatóság.
2. *megoldás.* A Fermat-tétel 2. alakja szerint $n^5 \equiv n \pmod 5$. Ezt alkalmazzuk az alábbi átalakításban:

$$n^{13} \equiv (n^5)^2 \cdot n^3 \equiv n^2 \cdot n^3 = n^5 \equiv n \pmod 5$$

Ez azt jelenti, hogy $n^{13} - n$ osztható 5-tel.
d. 1. *megoldás.* Ha $7|n$, akkor $7|n^{13}$ is, így $7|n^{13} - n$. Tegyük fel, hogy $7 \nmid n$.

$\varphi(7) = 6$, és így $n^6 \equiv 1 \pmod 7$, amit négyzetre emelve $n^{12} \equiv 1 \pmod 7$, ezt pedig n-nel beszorozva $n^{13} \equiv n \pmod 7$. Tehát $n^{13} - n$ osztható 7-tel.
2. *megoldás.* A Fermat-tétel 2. alakja szerint $n^7 \equiv n \pmod 7$. Ezt alkalmazzuk az alábbi átalakításban:

$$n^{13} = (n^7) \cdot n^6 \equiv n \cdot n^6 = n^7 \equiv n \pmod 7$$

Ez éppen azt jelenti, hogy $n^{13} - n$ osztható 7-tel.

e. A Fermat-tétel 2. alakja szerint $n^{13} \equiv n \pmod{13}$. Ez azt jelenti, hogy $n^{13} - n$ osztható 13-mal. ■

4.7-32.

a. Belátjuk, hogy $13 | m \cdot n(m^{60} - n^{60})$. Ha $13 | m \cdot n$, akkor teljesül az oszthatóság. Különben $(13, m \cdot n) = 1$, és mivel $\varphi(13) = 12$, $m^{12} \equiv 1 \pmod{13}$, amiből $m^{60} \equiv 1 \pmod{13}$. Hasonlóan $n^{60} \equiv 1 \pmod{13}$, s így $m^{60} - n^{60} \equiv 0 \pmod{13}$, ami azt jelenti, hogy $13 | m^{60} - n^{60}$, tehát $13 | m \cdot n(m^{60} - n^{60})$.
b. Most megmutatjuk, hogy $31 | m \cdot n(m^{60} - n^{60})$. Ha $31 | m \cdot n$, akkor teljesül az oszthatóság. Különben $(31, m \cdot n) = 1$, és mivel $\varphi(31) = 30$, $m^{30} \equiv 1 \pmod{31}$, amiből $m^{60} \equiv 1 \pmod{31}$. Hasonlóan $n^{60} \equiv 1 \pmod{31}$, s így $m^{60} - n^{60} \equiv 0 \pmod{31}$, ami azt jelenti, hogy $31 | m^{60} - n^{60}$.
c. Nézzük végül a 61-gyel való oszthatóságot. Ha $61 | m \cdot n$, akkor teljesül az oszthatóság. Különben $(61, m \cdot n) = 1$, és mivel $\varphi(61) = 60$, $m^{60} \equiv 1 \pmod{61}$. Hasonlóan $n^{60} \equiv 1 \pmod{61}$, s így $m^{60} - n^{60} \equiv 0 \pmod{61}$, ami azt jelenti, hogy $61 | m^{60} - n^{60}$.

13, 31, 61 páronként relatív prímek, ezért ha mindegyik osztója egy számnak, akkor a szorzatuk is osztója. ■

4.7-33.

Először belátjuk, hogy ha p olyan prím, amelyre $p - 1 | 60$, akkor $p | m \cdot n(m^{60} - n^{60})$. Ha $p | m \cdot n$, akkor teljesül az oszthatóság. Ha pedig $p \nmid m \cdot n$, akkor $m^{p-1} \equiv 1 \pmod p$, és $n^{p-1} \equiv 1 \pmod p$ miatt $m^{p-1} \equiv n^{p-1} \pmod p$, amiből $m^{60} \equiv n^{60} \pmod p$, tehát $p | m^{60} - n^{60}$. A 2, 3, 5, 7, 11, 13, 31, 61 prímek mind kielégítik a feltételt, s így a szorzatuk is osztója az $m \cdot n(m^{60} - n^{60})$ kifejezésnek. Be lehet látni, hogy csak ezek a prímek felelnek meg a feladat feltételeinek. ■

4.7-34.

Mivel 341 nem prím, a Fermat-tételre nem támaszkodhatunk. $341 = 11 \cdot 31$, valamint $(11, 31) = 1$, így ha belátjuk modulo 11 és modulo 31 a kongruencia fennállását, ebből következik, hogy modulo 341 is fennáll. Egyrészt $\varphi(11) = 10$ és a Fermat-tétel alapján $2^{10} \equiv 1 \pmod{11}$. Így $2^{341} = (2^{10})^{34} \cdot 2 \equiv 2 \pmod{11}$. Másrészt $\varphi(31) = 30$ és a Fermat-tétel alapján $2^{30} \equiv 1 \pmod{31}$. Emiatt $2^{341} = (2^{30})^{11} \cdot 2^{11} \equiv 2^{11} \equiv (2^5)^2 \cdot 2 \equiv (32)^2 \cdot 2 \equiv 2 \pmod{31}$. ■

4.7-35.
$1729 = 7 \cdot 13 \cdot 19$. Megmutatjuk, hogy a kongruencia fennáll modulo 7, modulo 13 és modulo 19. Mivel $7, 13$ és 19 relatív prímek, ebből következik, hogy modulo 1729 is fennáll a kongruencia. Szükségünk lesz a következőre: $1728 = 2^6 \cdot 3^3$.

a. Ha $7|a$, akkor nyilván $a^{1729} \equiv a \pmod{7}$. Legyen most $7 \nmid a$. Ekkor $\varphi(7) = 6$, és így $a^6 \equiv 1 \pmod{7}$. $\frac{1728}{6}$ egész szám, így az utolsó kongruenciát $\frac{1728}{6}$-odik hatványra emelve $a^{1728} \equiv 1 \pmod{7}$, és így $a^{1729} \equiv a \pmod{7}$.

b. Ha $13|a$, akkor $a^{1729} \equiv a \pmod{13}$. Tegyük fel, hogy $13 \nmid a$. $\varphi(13) = 12$, és így $a^{12} \equiv 1 \pmod{13}$, amit $\frac{1728}{12}$-edik hatványra emelve $a^{1728} \equiv 1 \pmod{13}$, ezt pedig a-val beszorozva $a^{1729} \equiv a \pmod{13}$.

c. Ha $19|a$, akkor nyilván $a^{1729} \equiv a \pmod{19}$. Legyen most $19 \nmid a$. $\varphi(19) = 18$, és így $a^{18} \equiv 1 \pmod{19}$, ezt $\frac{1728}{18}$-odik hatványra emelve $a^{1728} \equiv 1 \pmod{19}$, és így $a^{1729} \equiv a \pmod{19}$. ■

4.7-36.
a. $561 = 3 \cdot 11 \cdot 17$. Megmutatjuk, hogy a kongruencia fennáll modulo 3, modulo 11 és modulo 17.
1. A Fermat-tétel második alakja szerint $a^3 \equiv a \pmod{3}$. Ezt alkalmazzuk a következőkben többször is.

$$a^{561} = (a^3)^{11\cdot 17} \equiv a^{11\cdot 17} = ((a^3)^3 \cdot a^2)^{17} \equiv (a^3 \cdot a^2)^{17} \equiv (a \cdot a^2)^{17} \equiv a^{17} =$$

$$= (a^3)^5 \cdot a^2 \equiv a^5 \cdot a^2 = a^7 = (a^3)^2 \cdot a \equiv a^2 \cdot a = a^3 \equiv a \pmod{3}$$

2. Felhasználjuk, hogy $a^{11} \equiv a \pmod{11}$.

$$a^{561} = (a^{11})^{3 \cdot 17} \equiv a^{51} = (a^{11})^4 \cdot a^7 \equiv a^4 \cdot a^7 = a^{11} \equiv a \pmod{11}$$

3. Alkalmazzuk az $a^{17} \equiv a \pmod{17}$ összefüggést.

$$a^{561} = (a^{17})^{3 \cdot 11} \equiv a^{33} = a^{17} \cdot a^{16} \equiv a \cdot a^{16} = a^{17} \equiv a \pmod{17}$$

Mivel modulo 3, modulo 11 és modulo 17 fennáll a kongruencia, és 3, 11, 17 páronként relatív prímek, ezért modulo 561 is teljesül a kongruencia.
b. $1105 = 5 \cdot 13 \cdot 17$. Be kell látni, hogy a kongruencia fennáll modulo 5, modulo 13 és modulo 17, amiből következik az állítás. Ez az a. feladatban látható módon történhet.

c. $2465 = 5 \cdot 17 \cdot 29$. Be kell látni, hogy a kongruencia fennáll modulo 5, modulo 17 és modulo 29, amiből következik az állítás. Ez az a. feladatban látható módon történhet. ■

4.7-37.
$(1997, 10\ 000) = 1$, így alkalmazva az Euler-tételt:

$$1997^{\varphi(10\ 000)} \equiv 1 \pmod{10\ 000}$$

Ebből bármilyen $k \in \mathbb{N}$ esetén:

$$1997^{k\varphi(10\ 000)+1} \equiv 1997 \pmod{10\ 000}$$

Ezek a számok tehát mindnyájan 1997-re végződnek. ■

4.7-38.
Mivel $(p, 10) = 1$, $10^{p-1} \equiv 1 \pmod{p}$. Ezt k-adik hatványra emelve, ahol $k \in \mathbb{N}$ tetszőleges, $10^{k(p-1)} \equiv 1 \pmod{p}$. Ez azt jelenti, hogy $p | 10^{k(p-1)} - 1$, ami csupa 9-esből álló szám.

Ha $p \neq 3$, akkor az előbbi csupa 9-esből álló számot 9-cel osztva csupa 1-esből álló számot kapunk, amelyik szintén osztható p-vel. ■

4.8. Lineáris kongruenciák

4.8-1.

a. 5; **b.** 0; **c.** 5. ∎

4.8-2. $21x \equiv 57 \pmod{78}$
$(21, 78) = 3|57$

$$7x \equiv 19 \pmod{26}$$
$$7x \equiv 19 - 26 = -7 \pmod{26}$$
$$x \equiv -1 \equiv 25 \pmod{26}$$

A $\overline{25}, \overline{51}, \overline{77} \pmod{78}$ maradékosztályok alkotják a megoldást. ∎

4.8-3.
a.

$$26x \equiv 12 \pmod{22} \quad (26, 22) = 2|12$$

$$13x \equiv 6 \pmod{11}$$
$$13x \equiv 39 \pmod{11}$$
$$x \equiv 3 \pmod{11}$$

A $\overline{3}, \overline{14} \pmod{22}$ maradékosztályok alkotják a megoldást.

b. $20x \equiv 19 \pmod{22}$ nem megoldható, mert $(20, 22) = 2 \nmid 19$. ∎

4.8-4.
$(16, 28) = 4|36$
$16x \equiv 36 \pmod{28}$ $4x \equiv 9 \pmod{7}$ $4x \equiv 16 \pmod{7}$ $x \equiv 4 \pmod{7}$

A $\overline{4}, \overline{11}, \overline{18}, \overline{25} \pmod{28}$ maradékosztályok alkotják a megoldást. ∎

4.8-5.

$(126, 99) = 9|45$

$126x \equiv 45 \pmod{99}$ $14x \equiv 5 \pmod{11}$ $3x \equiv 5 \pmod{11}$

$3x \equiv 27 \pmod{11}$ $x \equiv 9 \pmod{11}$

A $\overline{9}, \overline{20}, \overline{31}, \overline{42}, \overline{53}, \overline{64}, \overline{75}, \overline{86}, \overline{97} \pmod{99}$ maradékosztályok alkotják a megoldást. ■

4.8-6.

$126x \equiv 46 \pmod{99}$ $\quad (126, 99) = 9 \nmid 46$, és így nincs megoldás. ■

4.8-7.

$35x \equiv -15 \pmod{30}$ $\quad (35, 30) = 5 | -15$

$7x \equiv -3 \pmod 6$ $\quad x \equiv -3 \pmod 6$ $\quad x \equiv 3 \pmod 6$

A $\overline{3}, \overline{9}, \overline{15}, \overline{21}, \overline{27},$ (mod 30) maradékosztályok alkotják a megoldást. ■

4.8-8.
a. $20x \equiv 4 \pmod{30}$, nincs megoldás, $(20, 30) = 10 \nmid 4$.
b. $20x \equiv 30 \pmod 4$, nincs megoldás, $(20, 4) = 4 \nmid 30$.
c. $353x \equiv 254 \pmod{40}$ $\quad (353, 40) = 1 | 254$
$-7x \equiv 14 \pmod{40}$ $\quad x \equiv -2 \pmod{40}$ $\quad x \equiv 38 \pmod{40}$

A megoldás a $\overline{38} \pmod{40}$ maradékosztály. ■

4.8-9.
a. $30x \equiv 40 \pmod{15}$ $\quad (30, 15) = 15 \nmid 40$, nincs megoldása a kongruenciának.
b. $40x \equiv 25 \pmod{15}$ $\quad (40, 15) = 5 | 25$
$8x \equiv 5 \pmod 3$ $\quad 2x \equiv 5 \pmod 3$ $\quad 2x \equiv 2 \pmod 3$ $\quad x \equiv 1 \pmod 3$

Az $\overline{1}, \overline{4}, \overline{7}, \overline{10}, \overline{13} \pmod{15}$ maradékosztályok alkotják a megoldást. ■

4.8-10.
$27x + 49y = 3$ $\quad (27, 49) = 1 | 3$
$49y \equiv 3 \pmod{27}$ $\quad -5y \equiv 3 \pmod{27}$ $\quad -5y \equiv 30 \pmod{27}$
$-y \equiv 6 \pmod{27}$ $\quad y \equiv -6 \equiv 21 \pmod{27}$

$y = 21 + 27t,\ t \in \mathbb{Z}, \quad x = \frac{3-49y}{27} = \frac{3-49(21+27t)}{27} = -38 - 49t$

Az $x = -38 - 49t, y = 21 + 27t,\ t \in \mathbb{Z}$ számpárok a megoldásai a diofantikus egyenletnek. ■

4.8-11.
$33x + 23y = 2 \quad (33, 23) = 1|2$
$33x \equiv 2 \pmod{23} \quad 10x \equiv 2 \pmod{23} \quad 5x \equiv 1 \pmod{23}$
$5x \equiv -45 \pmod{23} \quad x \equiv -9 \pmod{23} \quad x \equiv 14 \pmod{23}$

$x = 14 + 23t,\ t \in \mathbb{Z} \quad y = \frac{2-33x}{23} = \frac{2-33(14+23t)}{23} = -20 - 33t$

Az $x = 14 + 23t, y = -20 - 33t,\ t \in \mathbb{Z}$ számpárok a megoldásai a diofantikus egyenletnek. ■

4.8-12.

$$\begin{aligned} 33x + 23y &= 3 \\ 33x &\equiv 3 \pmod{23} \\ 10x &\equiv 3 \pmod{23} \\ 10x &\equiv -20 \pmod{23} \\ x &\equiv -2 \pmod{23} \\ x &\equiv 21 \pmod{23} \end{aligned}$$

$x = 21 + 23k,\ k \in \mathbb{Z} \quad y = \frac{3-33x}{23} = \frac{3-33(21+23k)}{23} = -30 - 33k.$

Az $x = 21 + 23k, y = -30 - 33k,\ t \in \mathbb{Z}$ számpárok a megoldásai a diofantikus egyenletnek. ■

4.8-13.
A következő A értéket keressük. $A = 28x+3 = 19y+4$, amiből $28x-1 = 19y$.

$$\begin{aligned} 28x &\equiv 1 \pmod{19} \\ 9x &\equiv 1 \pmod{19} \\ 9x &\equiv -18 \pmod{19} \\ x &\equiv -2 \pmod{19} \\ x &\equiv 17 \pmod{19} \end{aligned}$$

$x = 17 + 19k,\ k \in \mathbb{Z}.$ Ebből $x = 17$ adja a legkisebb A értéket.

$$A = 28 \cdot 17 + 3 = 479$$

■

4.8-14.
Legyen a szám x. Hetes számrendszerben írjuk fel $23x$-et.

$$23x = a_0+7a_1+7^2a_2+7^3a_3+\ldots = 5+7\cdot 2+7^2\cdot(a_2+7a_3+\ldots) = 5+2\cdot 7+7^2\cdot y$$

$$\begin{aligned} 23x &= 19 + 49y \\ 49y &\equiv -19 \pmod{23} \\ 3y &\equiv 4 \pmod{23} \\ 3y &\equiv 27 \pmod{23} \\ y &\equiv 9 \pmod{23} \end{aligned}$$

$y = 9+23t,\ x = \frac{49\cdot(9+23t)+19}{23} = 20+49t$. Ebből 20 és 69 felel meg a feltételnek.

■

4.8-15.
$a \equiv b \pmod{p^n}$ azt jelenti, hogy $p^n|a-b$, tehát $a = b + tp^n$, ahol $t \in \mathbb{Z}$.

$$a^p = b^p + \binom{p}{1} b^{p-1}tp^n + \binom{p}{2} b^{p-2}t^2p^{2n} + \ldots$$

$$\ldots + \binom{p}{p-1} bt^{p-1}(p^n)^{p-1} + \binom{p}{p} t^p(p^n)^p \qquad (1)$$

Felhasználjuk azt, hogy $p|\binom{p}{i} = \frac{p!}{i!(p-i)!}$, ha $1 \le i \le p-1$. (1) jobb oldalának a második tagtól kezdve mindegyik tagja osztható p^{n+1}-gyel, így

$$p^{n+1}|a^p - b^p,$$

ez pedig ekvivalens az állítással. ■

4.9. Lineáris kongruencia-rendszerek, a kínai maradéktétel

4.9-1.

$$\begin{aligned} 7x &\equiv 11 \pmod{12} \\ 13x &\equiv 17 \pmod{21} \end{aligned}$$

Mivel $(m_1, m_2) = 3|c_1 - c_2 = 6$, a kongruencia-rendszernek van megoldása.

1. *megoldás.*

Oldjuk meg először az első kongruenciát.

$$\begin{aligned} 7x &\equiv 11 \pmod{12} \\ 7x &\equiv 35 \pmod{12} \\ x &\equiv 5 \pmod{12} \end{aligned}$$

A kongruenciát az

$$x = 5 + 12r \quad r \in \mathbb{Z} \tag{1}$$

számok elégítik ki. Ezt helyettesítsük be a második kongruenciába.

$$\begin{aligned} 13(5 + 12r) &\equiv 17 \pmod{21} \\ 156r &\equiv -48 \pmod{21} \\ 9r &\equiv -48 \pmod{21} \\ 3r &\equiv -16 \pmod{7} \\ 3r &\equiv -9 \pmod{7} \\ r &\equiv -3 \pmod{7} \\ r &\equiv 4 \pmod{7} \end{aligned}$$

A megoldást az $r = 4 + 7s, \quad s \in \mathbb{Z}$ számok alkotják. Ezt behelyettesítjük (1)-be. $x = 5 + 12r = 5 + 12(4 + 7s) = 53 + 84s, \quad s \in \mathbb{Z}$. A kongruencia-rendszer megoldása tehát $\overline{53} \pmod{84}$. Figyeljük meg, hogy $84 = \mathrm{lkkt}(12, 21)$.

2. *megoldás.*

A kínai maradéktétel alkalmazásával is megoldhatjuk a kongruencia-rendszert. A $7x \equiv 11 \pmod{12}$ kongruencia ekvivalens a következő kongruencia-rendszerrel:

$$\begin{aligned} 7x &\equiv 11 \pmod{3} \\ 7x &\equiv 11 \pmod{4} \end{aligned}$$

A $13x \equiv 17 \pmod{21}$ kongruencia pedig a következő kongruencia-rendszerrel ekvivalens:

$$\begin{aligned} 13x &\equiv 17 \pmod 3 \\ 13x &\equiv 17 \pmod 7 \end{aligned}$$

Oldjuk meg először külön-külön a kongruenciákat.

$$7x \equiv 11 \pmod 3 \quad \text{megoldása} \quad x \equiv 2 \pmod 3;$$

$$7x \equiv 11 \pmod 4 \quad \text{megoldása} \quad x \equiv 1 \pmod 4;$$

$$13x \equiv 17 \pmod 3 \quad \text{megoldása} \quad x \equiv 2 \pmod 3;$$

$$13x \equiv 17 \pmod 7 \quad \text{megoldása} \quad x \equiv 4 \pmod 7.$$

Tehát a következő három kongruenciából álló rendszert kell megoldanunk:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 4 \pmod 7 \end{aligned}$$

Erre teljesülnek a kínai maradéktétel feltételei.

$$m = 3 \cdot 4 \cdot 7 = 84 \qquad M_1 = 28 \qquad M_2 = 21 \qquad M_3 = 12$$

Az alábbi kongruenciákat egyenként oldjuk meg.

$$\begin{array}{rclllrclllrcll}
28y & \equiv & 1 & \pmod 3 & \quad & 21y & \equiv & 1 & \pmod 4 & \quad & 12y & \equiv & 1 & \pmod 7 \\
y & \equiv & 1 & \pmod 3 & & y & \equiv & 1 & \pmod 4 & & -2y & \equiv & 8 & \pmod 7 \\
 & & & & & & & & & & -y & \equiv & 4 & \pmod 7 \\
 & & & & & & & & & & y & \equiv & -4 & \pmod 7 \\
 & & & & & & & & & & y & \equiv & 3 & \pmod 7 \\
y_1 & = & 1 & & & y_2 & = & 1 & & & y_3 & = & 3 &
\end{array}$$

Az x_0 megoldást modulo 84 nézzük.

$$x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 \equiv 28 \cdot 1 \cdot 2 + 21 \cdot 1 \cdot 1 + 12 \cdot 3 \cdot 4 \equiv$$

$$\equiv 56 + 21 + 144 \equiv 53 \pmod{84}$$

A feladat megoldása $\overline{53} \pmod{84}$. ■

4.9-2.
Legyen a keresett szám x. A következő kongruencia-rendszert kell megoldanunk:

$$x \equiv 46 \pmod{72}$$
$$x \equiv 97 \pmod{127}$$

Az első kongruenciát az

$$x = 46 + 72s \quad s \in \mathbb{Z} \tag{1}$$

számok elégítik ki. Ezt helyettesítsük a második kongruenciába.

$$\begin{aligned}
46 + 72s &\equiv 97 \pmod{127}\\
72s &\equiv 51 \pmod{127}\\
24s &\equiv 17 \pmod{127}\\
24s &\equiv 144 \pmod{127}\\
s &\equiv 6 \pmod{127}
\end{aligned}$$

A második kongruencia megoldása $s = 6 + 127r, \quad r \in \mathbb{Z}$. Ezt helyettesítsük (1)-be. $x = 46 + 72(6 + 127r) = 478 + 9144r$. Ezek közül a számok közül csak $r = 1$ esetén lesz négyjegyű. A megoldás tehát $478 + 9144 = 9622$. ■

4.9-3.

$$x \equiv 1 \pmod{3}$$
$$x \equiv 1 \pmod{5}$$
$$x \equiv 1 \pmod{7}$$

A kínai maradéktétel feltételei teljesülnek, így alkalmazhatjuk a módszert.

$$m = 3 \cdot 5 \cdot 7 = 105 \qquad M_1 = 35 \qquad M_2 = 21 \qquad M_3 = 15$$

Az alábbi kongruenciákat egyenként oldjuk meg:

$$\begin{array}{rcll rcll rcll}
35y & \equiv & 1 & \pmod{3} & 21y & \equiv & 1 & \pmod{5} & 15y & \equiv & 1 & \pmod{7}\\
-y & \equiv & 1 & \pmod{3} & y & \equiv & 1 & \pmod{5} & y & \equiv & 1 & \pmod{7}\\
y & \equiv & 2 & \pmod{3} & & & & & & & &\\
y_1 & = & 2 & & y_2 & = & 1 & & y_3 & = & 1 &
\end{array}$$

A kapott y_i értékek segítségével előállítandó x_0 megoldást modulo 105 vesszük.

$$x_0 \equiv M_1y_1c_1+M_2y_2c_2+M_3y_3c_3 \equiv 35\cdot2\cdot1+21\cdot1\cdot1+15\cdot1\cdot1 \equiv 106 \pmod{105}$$

A feladat megoldása 106. ∎

4.9-4.

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 5 \pmod 2 \end{aligned}$$

A kínai maradéktétel feltételei teljesülnek, így alkalmazhatjuk a módszert.

$$m = 3\cdot5\cdot2 = 30 \qquad M_1 = 10 \qquad M_2 = 6 \qquad M_3 = 15$$

Az alábbi kongruenciákat egyenként oldjuk meg:

$$\begin{array}{rcll} 10y & \equiv & 1 & \pmod 3 \\ y & \equiv & 1 & \pmod 3 \\ y_1 & = & 1 & \end{array} \qquad \begin{array}{rcll} 6y & \equiv & 1 & \pmod 5 \\ y & \equiv & 1 & \pmod 5 \\ y_2 & = & 1 & \end{array} \qquad \begin{array}{rcll} 15y & \equiv & 1 & \pmod 2 \\ y & \equiv & 1 & \pmod 2 \\ y_3 & = & 1 & \end{array}$$

Az x_0 megoldást modulo 30 vesszük.

$$x_0 \equiv M_1y_1c_1 + M_2y_2c_2 + M_3y_3c_3 \equiv 10\cdot1\cdot2 + 6\cdot1\cdot3 + 15\cdot1\cdot5 \equiv$$

$$\equiv 20 + 18 + 75 \equiv 113 \equiv 23 \pmod{30}$$

A feladatnak megfelelő egész számok: $23 + 30j \quad j \in \mathbb{Z}$. ∎

4.9-5.

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 5 \pmod 7 \end{aligned}$$

A kínai maradéktétel feltételei teljesülnek, így alkalmazhatjuk a módszert.

$$m = 4\cdot3\cdot7 = 84 \qquad M_1 = 21 \qquad M_2 = 28 \qquad M_3 = 12$$

Az alábbi kongruenciákat egyenként oldjuk meg:

$$\begin{array}{rcll} 21y & \equiv & 1 & \pmod 4 \\ y & \equiv & 1 & \pmod 4 \\ \\ y_1 & = & 1 & \end{array} \qquad \begin{array}{rcll} 28y & \equiv & 1 & \pmod 3 \\ y & \equiv & 1 & \pmod 3 \\ \\ y_2 & = & 1 & \end{array} \qquad \begin{array}{rcll} 12y & \equiv & 1 & \pmod 7 \\ -2y & \equiv & -6 & \pmod 7 \\ y & \equiv & 3 & \pmod 7 \\ y_3 & = & 3 & \end{array}$$

Az x_0 megoldást modulo 84 tekintjük.

$$x_0 \equiv M_1y_1c_1 + M_2y_2c_2 + M_3y_3c_3 \equiv 21 \cdot 1 \cdot 1 + 28 \cdot 1 \cdot 0 + 12 \cdot 3 \cdot 5 \equiv$$

$$\equiv 21 + 180 \equiv 201 \equiv 33 \pmod{84}$$

A feladat megoldása $\overline{33}$ (mod 84). ■

4.9-6.

A következő kongruencia-rendszert kell megoldani:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

A kínai maradéktétel feltételei teljesülnek, így alkalmazhatjuk a módszert.

$$m = 3 \cdot 4 \cdot 5 = 60 \qquad M_1 = 20 \qquad M_2 = 15 \qquad M_3 = 12$$

Az alábbi kongruenciákat egyenként oldjuk meg:

$$\begin{array}{rcll} 20y & \equiv & 1 & \pmod 3 \\ -y & \equiv & 1 & \pmod 3 \\ y & \equiv & 2 & \pmod 3 \\ y_1 & = & 2 & \end{array} \qquad \begin{array}{rcll} 15y & \equiv & 1 & \pmod 4 \\ -y & \equiv & 1 & \pmod 4 \\ y & \equiv & 3 & \pmod 4 \\ y_2 & = & 3 & \end{array} \qquad \begin{array}{rcll} 12y & \equiv & 1 & \pmod 5 \\ 2y & \equiv & 6 & \pmod 5 \\ y & \equiv & 3 & \pmod 5 \\ y_3 & = & 3 & \end{array}$$

Az x_0 megoldást modulo 60 vesszük.

$$x_0 \equiv M_1y_1c_1 + M_2y_2c_2 + M_3y_3c_3 \equiv 20 \cdot 2 \cdot 1 + 15 \cdot 3 \cdot 2 + 12 \cdot 3 \cdot 3 \equiv$$

$$\equiv 40 + 90 + 108 \equiv 238 \equiv -2 \pmod{60}$$

A feladatnak megfelelő egész számok: $60j - 2 \quad j \in \mathbb{Z}$. ■

4.9-7.
$m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. Keressük meg 23 és 37 számjegyeit maradékszám-rendszerben, tehát a modulo p_i maradékokat.

$$29 = (1,\ 2,\ 4,\ 1,\ 7) \qquad 36 = (0,\ 0,\ 1,\ 1,\ 3)$$

Végezzük el a szorzást a maradékokkal.

$$29 \cdot 36 = (1 \cdot 0,\ 2 \cdot 0,\ 4 \cdot 1,\ 1 \cdot 1,\ 7 \cdot 3) = (0,\ 0,\ 4,\ 1,\ 10)$$

Oldjuk meg a következő szimultán kongruencia-rendszert:

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 0 \pmod 3 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 1 \pmod 7 \\ x &\equiv 10 \pmod{11} \end{aligned}$$

Az M_i értékek sorban 1155, 770, 462, 330 és 210. Az $M_i y \equiv 1 \pmod{p_i}$ kongruenciák közül csak a modulo 5, a modulo 7 és a modulo 11 kongruenciák megoldására van szükség, mert a többi értéke x_0-ban 0-val szorzódik.

$$y_3 = 3, \quad y_4 = 1, \quad y_5 = 1.$$

Ennek felhasználásával:

$$x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 + M_4 y_4 c_4 + M_5 y_5 c_5 \equiv$$

$$\equiv 1155 \cdot y_1 \cdot 0 + 770 \cdot y_2 \cdot 0 + 462 \cdot 3 \cdot 4 + 330 \cdot 1 \cdot 1 + 210 \cdot 1 \cdot 10 \equiv 1044 \pmod{2310}$$

A számolás eredménye $29 \cdot 36 = 1044$. ■

4.9-8.
$m = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$. Keressük meg 19 és 48 számjegyeit maradékszám-rendszerben, tehát a modulo p_i maradékokat.

$$19 = (1,\ 1,\ 4,\ 5,\ 8) \qquad 48 = (0,\ 0,\ 3,\ 6,\ 4)$$

Végezzük el a szorzást a maradékokkal.

$$19 \cdot 48 = (1 \cdot 0,\ 1 \cdot 0,\ 4 \cdot 3,\ 5 \cdot 6,\ 8 \cdot 4) = (0,\ 0,\ 2,\ 2,\ 10)$$

Oldjuk meg a következő szimultán kongruencia-rendszert:

$$
\begin{aligned}
x &\equiv 0 \pmod 2\\
x &\equiv 0 \pmod 3\\
x &\equiv 2 \pmod 5\\
x &\equiv 2 \pmod 7\\
x &\equiv 10 \pmod{11}
\end{aligned}
$$

Az M_i értékek sorban 1155, 770, 462, 330 és 210. Az $M_i y \equiv 1 \pmod{p_i}$ kongruenciák közül csak a modulo 5, a modulo 7 és a modulo 11 kongruenciák megoldására van szükség, mert a többi értéke x_0-ban 0-val szorzódik.

$$y_3 = 3, \quad y_4 = 1, \quad y_5 = 1.$$

Ennek felhasználásával:

$$x_0 \equiv M_1 y_1 c_1 + M_2 y_2 c_2 + M_3 y_3 c_3 + M_4 y_4 c_4 + M_5 y_5 c_5 \equiv$$

$$\equiv 1155 \cdot y_1 \cdot 0 + 770 \cdot y_2 \cdot 0 + 462 \cdot 3 \cdot 2 + 330 \cdot 1 \cdot 2 + 210 \cdot 1 \cdot 10 \equiv 912 \pmod{2310}$$

A számolás eredménye $19 \cdot 48 = 912$. ■

4.9-9.

Legyenek $p_1,\ p_2,\ \ldots,\ p_k$ páronként különböző prímek, és nézzük a következő kongruencia-rendszert:

$$
\begin{aligned}
x + 1 &\equiv p_1 \pmod{p_1^2}\\
x + 2 &\equiv p_2 \pmod{p_2^2}\\
&\vdots\\
x + k &\equiv p_k \pmod{p_k^2}
\end{aligned}
$$

Ez a kongruencia-rendszer a kínai maradéktétel szerint megoldható, a megoldások között vannak pozitív egész számok is. Legyen például x_0 egy ilyen megoldás. x_0+1 kanonikus alakjában például p_1 első hatványon szerepel, mert $p_1^2 | x_0+1-p_1$, s így $p_1 | x_0+1$, de $p_1^2 \nmid x_0+1$. Emiatt x_0+1 nem teljes hatvány. Hasonló mondható el az $x_0+s \quad s = 2, \ldots, k$ számokról is, tehát egyik sem teljes hatvány. ■

4.10. Lánctörtek, diofantikus approximációelmélet

4.10-1.

a.

$$\frac{41}{31} = //3,\ 1,\ 2,\ 1,\ 2//$$

b.

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	$-$	1	0	$-$
1	3	3	1	3
2	1	$1 \cdot 3 + 1 = 4$	$1 \cdot 1 + 0 = 1$	4
3	2	$2 \cdot 4 + 3 = 11$	$2 \cdot 1 + 1 = 3$	$\frac{11}{3}$
4	1	$1 \cdot 11 + 4 = 15$	$1 \cdot 3 + 1 = 4$	$\frac{15}{4}$
5	2	$2 \cdot 15 + 11 = 41$	$2 \cdot 4 + 3 = 11$	$\frac{41}{11}$

Az utolsó közelítő tört maga a lánctörtbe fejtett szám. ■

4.10-2.

a.

$$\frac{85}{37} = //2,\ 3,\ 2,\ 1,\ 3//$$

b.

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	$-$	1	0	$-$
1	2	2	1	2
2	3	$3 \cdot 2 + 1 = 7$	$3 \cdot 1 + 0 = 3$	$\frac{7}{3}$
3	2	$2 \cdot 7 + 2 = 16$	$2 \cdot 3 + 1 = 7$	$\frac{16}{7}$
4	1	$1 \cdot 16 + 7 = 23$	$1 \cdot 7 + 3 = 10$	$\frac{23}{10}$
5	3	$3 \cdot 23 + 16 = 85$	$3 \cdot 10 + 7 = 37$	$\frac{85}{37}$

Az utolsó közelítő tört maga a lánctörtbe fejtett szám. ■

4.10-3.

a.

$$\frac{83}{22} = //3,\ 1,\ 3,\ 2,\ 2//$$

b.

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	$-$	1	0	$-$
1	3	3	1	3
2	1	$1 \cdot 3 + 1 = 4$	$1 \cdot 1 + 0 = 1$	4
3	3	$3 \cdot 4 + 3 = 15$	$3 \cdot 1 + 1 = 4$	$\frac{15}{4}$
4	2	$2 \cdot 15 + 4 = 34$	$2 \cdot 4 + 1 = 9$	$\frac{34}{9}$
5	2	$2 \cdot 34 + 15 = 83$	$2 \cdot 9 + 4 = 22$	$\frac{83}{22}$

Az utolsó közelítő tört maga a lánctörtbe fejtett szám. ■

4.10-4.

a.

$$\frac{62}{23} = //2,\ 1,\ 2,\ 3,\ 2//$$

b.

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	2	2	1	2
2	1	$1 \cdot 2 + 1 = 3$	$1 \cdot 1 + 0 = 1$	3
3	2	$2 \cdot 3 + 2 = 8$	$2 \cdot 1 + 1 = 3$	$\frac{8}{3}$
4	3	$3 \cdot 8 + 3 = 27$	$3 \cdot 3 + 1 = 10$	$\frac{27}{10}$
5	2	$2 \cdot 27 + 8 = 62$	$2 \cdot 10 + 3 = 23$	$\frac{62}{23}$

Az utolsó közelítő tört maga a lánctörtbe fejtett szám. ■

4.10-5. $//1,\ 2,\ 3,\ 4,\ 5//$

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	1	1	1	1
2	2	$2 \cdot 1 + 1 = 3$	$2 \cdot 1 + 0 = 2$	$\frac{3}{2}$
3	3	$3 \cdot 3 + 1 = 10$	$3 \cdot 2 + 1 = 7$	$\frac{10}{7}$
4	4	$4 \cdot 10 + 3 = 43$	$4 \cdot 7 + 2 = 30$	$\frac{43}{30}$
5	5	$5 \cdot 43 + 10 = 225$	$5 \cdot 30 + 7 = 157$	$\frac{225}{157}$

A keresett alak $\frac{225}{157}$. ■

4.10-6. //5, 4, 3, 2, 1//

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	5	5	1	5
2	4	$4 \cdot 5 + 1 = 21$	$4 \cdot 1 + 0 = 4$	$\frac{21}{4}$
3	3	$3 \cdot 21 + 5 = 68$	$3 \cdot 4 + 1 = 13$	$\frac{68}{13}$
4	2	$2 \cdot 68 + 21 = 157$	$2 \cdot 13 + 4 = 30$	$\frac{157}{30}$
5	1	$1 \cdot 157 + 68 = 225$	$1 \cdot 30 + 13 = 43$	$\frac{225}{43}$

A keresett alak $\frac{225}{43}$. ■

4.10-7. //1, 2, 3, 1, 2//

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	1	1	1	1
2	2	$2 \cdot 1 + 1 = 3$	$2 \cdot 1 + 0 = 2$	$\frac{3}{2}$
3	3	$3 \cdot 3 + 1 = 10$	$3 \cdot 2 + 1 = 7$	$\frac{10}{7}$
4	1	$1 \cdot 10 + 3 = 13$	$1 \cdot 7 + 2 = 9$	$\frac{13}{9}$
5	2	$2 \cdot 13 + 10 = 36$	$2 \cdot 9 + 7 = 25$	$\frac{36}{25}$

A keresett alak $\frac{36}{25}$. ■

4.10-8. //2, 3, 1, 2, 3//

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	2	2	1	2
2	3	$3 \cdot 2 + 1 = 7$	$3 \cdot 1 + 0 = 3$	$\frac{7}{3}$
3	1	$1 \cdot 7 + 2 = 9$	$1 \cdot 3 + 1 = 4$	$\frac{9}{4}$
4	2	$2 \cdot 9 + 7 = 25$	$2 \cdot 4 + 3 = 11$	$\frac{25}{11}$
5	3	$3 \cdot 25 + 9 = 84$	$3 \cdot 11 + 4 = 37$	$\frac{84}{37}$

A keresett alak $\frac{84}{37}$. ∎

4.10-9. //3, 2, 1, 3, 2//

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	3	3	1	3
2	2	$2 \cdot 3 + 1 = 7$	$2 \cdot 1 + 0 = 2$	$\frac{7}{2}$
3	1	$1 \cdot 7 + 3 = 10$	$1 \cdot 2 + 1 = 3$	$\frac{10}{3}$
4	3	$3 \cdot 10 + 7 = 37$	$3 \cdot 3 + 2 = 11$	$\frac{37}{11}$
5	2	$2 \cdot 37 + 10 = 84$	$2 \cdot 11 + 3 = 25$	$\frac{84}{25}$

A keresett alak $\frac{84}{25}$. ∎

4.10-10. $//2,\ 1,\ 2,\ 1,\ 2//$

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	2	2	1	2
2	1	$1 \cdot 2 + 1 = 3$	$1 \cdot 1 + 0 = 1$	3
3	2	$2 \cdot 3 + 2 = 8$	$2 \cdot 1 + 1 = 3$	$\frac{8}{3}$
4	1	$1 \cdot 8 + 3 = 11$	$1 \cdot 3 + 1 = 4$	$\frac{11}{4}$
5	2	$2 \cdot 11 + 8 = 30$	$2 \cdot 4 + 3 = 11$	$\frac{30}{11}$

A keresett alak $\frac{30}{11}$. ■

4.10-11. $//3,\ 1,\ 3,\ 1,\ 3//$

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	3	3	1	3
2	1	$1 \cdot 3 + 1 = 4$	$1 \cdot 1 + 0 = 1$	4
3	3	$3 \cdot 4 + 3 = 15$	$3 \cdot 1 + 1 = 4$	$\frac{15}{4}$
4	1	$1 \cdot 15 + 4 = 19$	$1 \cdot 4 + 1 = 5$	$\frac{19}{5}$
5	3	$3 \cdot 19 + 15 = 72$	$3 \cdot 5 + 4 = 19$	$\frac{72}{19}$

A keresett alak $\frac{72}{19}$. ■

4.10-12. //2, 3, 2, 3, 2//

n	q_n	$P_0 = 1, \quad P_1 = q_1$ $P_k = q_k P_{k-1} + P_{k-2}$	$Q_0 = 0, \quad Q_1 = 1$ $Q_k = q_k Q_{k-1} + Q_{k-2}$	$\delta_n = \frac{P_n}{Q_n}$
0	–	1	0	–
1	2	2	1	2
2	3	$3 \cdot 2 + 1 = 7$	$3 \cdot 1 + 0 = 3$	$\frac{7}{3}$
3	2	$2 \cdot 7 + 2 = 16$	$2 \cdot 3 + 1 = 7$	$\frac{16}{7}$
4	3	$3 \cdot 16 + 7 = 55$	$3 \cdot 7 + 3 = 24$	$\frac{55}{24}$
5	2	$2 \cdot 55 + 16 = 126$	$2 \cdot 24 + 7 = 55$	$\frac{126}{55}$

A keresett alak $\frac{126}{55}$. ■

5. Ajánlott irodalom

Dringó László – Kátai Imre: *Bevezetés a matematikába.*
Tankönyvkiadó, Budapest, 1982.

Freud Róbert – Gyarmati Edit: *Számelmélet.*
Nemzeti Tankönyvkiadó, Budapest, 2000.

Fuchs László: *Bevezetés az algebrába és a számelméletbe.*
Tankönyvkiadó, Budapest, 1964.

Gyarmati Edit, Turán Pál előadásainak felhasználásával: *Számelmélet.*
Tankönyvkiadó, Budapest, 1991.

Járai Antal: *Bevezetés a matematikába.*
ELTE Eötvös Kiadó, 2005.

Láng Csabáné: *Bevezető fejezetek a matematikába I.*
ELTE Budapest, 1997.

Megyesi László: *Bevezetés a számelméletbe.*
Polygon, Szeged, 1997.

Niven, I. – Zuckerman, H. S.: *Bevezetés a számelméletbe.*
Műszaki Könyvkiadó, Budapest, 1978.

Ore, Oysten: *Bevezetés a számelmélet világába.*
Gondolat, Budapest, 1977.

Perron, O.: *Die Lehre von den Kettenbrüchen II.*
Stuttgart, 1954.

Sárközy András: *Számelmélet.*

Műszaki Könyvkiadó, Budapest, 1976.
Szalay Mihály: *Számelmélet.*
Tankönyvkiadó, Budapest, 1991.
Vinogradov, I. M.: *A számelmélet alapjai.*
Tankönyvkiadó, Budapest, 1968.

Tárgymutató