

Gyakorló feladatok

1. a) Bizonyítsuk be, hogy ha $(a, b) = 1$, és a és b is osztója c -nek, akkor ab is osztója c -nek.
 b) Bizonyítsuk be, hogy a, b pozitív egészekre $\frac{ab}{(a,b)}$ az a és b kitüntetett közös többszöröse, azaz többszöröse a -nak és b -nek, és minden más közös többszörösüknek osztója.

Megoldás: a) Mivel a osztója c -nek, $c = ac_1$ valamely $c_1 \in \mathbb{Z}$ -re. De akkor $b \mid ac_1$ és $(b, a) = 1$ miatt $b \mid c_1$, azaz $c_1 = bc_2$ alkalmas $c_2 \in \mathbb{Z}$ -re, tehát $c = ac_1 = abc_2$.

b) Legyen $d = (a, b)$ és $m = \frac{ab}{d}$ (az utóbbi nyilván egész, mivel $\frac{a}{d}$ és $\frac{b}{d}$ is az). Az $m = \frac{ab}{d} = a \frac{b}{d} = \frac{a}{d} b$ felbontások mutatják, hogy m közös többszöröse a -nak és b -nek. Másrészt, ha valamely c is közös többszörös, akkor $a \mid c$ és $b \mid c$ leosztásával azt kapjuk, hogy $\frac{a}{d} \mid \frac{c}{d}$ és $\frac{b}{d} \mid \frac{c}{d}$, továbbá tudjuk, hogy $(\frac{a}{d}, \frac{b}{d}) = 1$, tehát az a) rész miatt $\frac{ab}{d^2} \mid \frac{c}{d}$, és ezt felszorozva $\frac{ab}{d} \mid c$.

2. Mutassuk meg, hogy

a) $4k + 1$ alakú számok szorzata $4k + 1$ alakú;

b) végtelen sok $4k + 3$ alakú prímszám van! (Útmutatás: Milyen prímosztói lehetnek a $4n! - 1$ számnak?)

Megoldás: a) Elég belátni, hogy két $4k + 1$ alakú szám szorzata $4k + 1$ alakú, abból már teljes indukcióval következik tetszőlegesen sok tényezősszorzatra is az állítás. $(4k + 1)(4\ell + 1) = 16k\ell + 4k + 4\ell + 1 = 4(4k\ell + k + \ell) + 1$.

b) $4n! - 1$ páratlan, ezért csak páratlan prímosztói vannak, másrészt az a) rész miatt nem lehet mindegyik prímosztója $4k + 1$ alakú. Tehát van olyan $4k + 3$ alakú prím, ami osztója $4n! - 1$ -nek. Viszont minden n alatti pozitív egész osztja $4n!$ -t, így nem osztja $4n! - 1$ -et, és ezért $p > n$. Ezzel beláttuk, hogy minden n -nél van nagyobb $4k + 3$ alakú prím, következésképpen az ilyen alakú prímek száma végtelen.

3. A páros számok körében definiált oszthatóságra nézve mely számok írhatók fel lényegében egyértelműen felbonthatatlanok szorzataként?

Megoldás: $2\mathbb{Z}$ helyett elég $2\mathbb{N}^+$ -ban vizsgálni a kérdést, mert az oszthatóság, ahogy \mathbb{Z} -ben, $2\mathbb{Z}$ -ben sem függ az előjeltől (és a 0 nem felbonthatatlan, és nem is bontható felbonthatatlanokra). A "lényegében egyértelmű" $2\mathbb{N}^+$ -ban azt fogja jelenteni, hogy sorrendtől eltekintve egyértelmű ($2\mathbb{Z}$ -ben azt, hogy sorrendtől és előjeltől eltekintve egyértelmű). $2\mathbb{N}^+$ -ban nincs egységelem, de még olyan szám sem, amit ilyen esetben egységnek hívhatnánk, azaz amelyik minden más számnak osztója, ugyanis semelyik $2\mathbb{N}^+$ -beli szám nem osztója (nem párosadrésze) sajátmagának. Tehát a felbonthatatlan számok azok, amelyek semmilyen módon nem bonthatók fel két páros szám szorzatára, azaz amelyek 2-vel oszthatók, de 4-gyel nem. Ilyen számok szorzatára mindegyik $2\mathbb{N}^+$ -beli szám felbontható, de nem feltétlenül egyértelműen. Legyen $n = 2^k m \in 2\mathbb{N}^+$, ahol $m \geq 1$ páratlan és $k \geq 1$. Ha $k = 1$, akkor n felbonthatatlan, ha $k \geq 2$, és $m = 1$ vagy $m \in \mathbb{N}^+$ -ban prím, akkor n csak $2m \cdot 2 \cdots 2$ alakban bontható fel felbonthatatlanok szorzatára. Viszont ha $k \geq 2$ és m összetett szám \mathbb{N}^+ -ban: $m = m_1 m_2$, ahol $m_1, m_2 > 1$, akkor $2m \cdot 2 \cdots 2$ és $2m_1 \cdot 2m_2 \cdots 2$ két lényegesen különböző felbontás. Tehát pontosan azoknak a számoknak van $2\mathbb{N}^+$ -ban egyértelmű irreducibilisekre való felbontásuk, amelyek nem oszthatók négyel (ezek maguk irreducibilisek), 2-hatványok, vagy 2-hatványok páratlan (\mathbb{N}^+ -beli) prímszám-szorosai.

4. a) Mi a 2 kitevője 17! kanonikus alakjában?
b) Hány nullára végződik a 100! szám?

Megoldás:

a) $\lfloor \frac{17}{2} \rfloor + \lfloor \frac{17}{4} \rfloor + \lfloor \frac{17}{8} \rfloor + \lfloor \frac{17}{16} \rfloor = 8 + 4 + 2 + 1 = 15.$

b) Egy n szám pontosan k nullára végződik, ha 10^k osztója az adott számnak, de 10^{k+1} nem. Mivel $10^k = 2^k \cdot 5^k$ relatív prím prímszorzatok szorzata, ehhez az kell, hogy $([n]_p$ -vel jelölve p kitevőjét n kanonikus alakjában) $[n]_2$ és $[n]_5$ mindegyike legalább k , de az egyik pontosan k . Az $n = 100!$ esetben $[100!]_2 = \lfloor \frac{100}{2} \rfloor + \lfloor \frac{100}{2^2} \rfloor + \dots$ nyilván legalább akkora, mint $[100!]_5 = \lfloor \frac{100}{5} \rfloor + \lfloor \frac{100}{5^2} \rfloor + 0 + 0 + \dots = 24$, tehát 100! pontosan 24 darab 0-ra végződik.

5. Bizonyítsuk be, hogy $n, a, b \in \mathbb{N}^+$ -ra $\left[\frac{n}{ab} \right] = \left[\frac{\left[\frac{n}{a} \right]}{b} \right]$.

Megoldás: Beláthatjuk általánosabban, hogy ha $x \in \mathbb{R}$, és $b \in \mathbb{N}^+$, akkor $\left[\frac{x}{b} \right] = \left[\frac{\left[x \right]}{b} \right]$.

Legyen $\left[\frac{x}{b} \right] = q \in \mathbb{Z}$. Ekkor $q \leq \frac{x}{b} < q + 1 \Rightarrow qb \leq x < qb + b$. Mivel az első és harmadik szám egész, ebből $qb \leq [x] < qb + b$, azaz $q \leq \frac{[x]}{b} < q + 1$ következik, így $\left[\frac{[x]}{b} \right] = q$.

6. Határozzuk meg az alábbi számok legnagyobb közös osztóját és legkisebb közös többszörösét!
a) $2^{23}3^{10}7^{13}, 2^{15}7^{10}13^5$
b) $2^{23}3^{10}7^{13}, 2^{15}7^{10}13^5, 3^{15}7^{20}11^2$.

Megoldás: a) A lko $2^{15}7^{10}$, a lkkt $2^{23}3^{10}7^{13}13^5$.

b) A lko 7^{10} , a lkkt $2^{23}3^{15}7^{20}11^213^5$.

7. Határozzuk meg $2^{67} \pmod{71}$ értékét!

Megoldás: A 67 2-es számrendszerben való felírásának segítségével állítsuk elő 67-et 2-hatványok összegeként: $67 = 64 + 2 + 1$. Így elég a hatványalap 2-hatványadik hatványait kiszámítani modulo 71 többszörös négyzetre emeléssel, és ezek (modulo 71) szorzatát venni.

$$2^1 \equiv 2 \pmod{71}$$

$$2^2 \equiv 4 \pmod{71}$$

$$2^4 \equiv 16 \pmod{71}$$

$$2^8 \equiv 256 \equiv -28 \pmod{71}$$

$$2^{16} \equiv 784 \equiv 3 \pmod{71}$$

$$2^{32} \equiv 9 \pmod{71}$$

$$2^{64} \equiv 81 \equiv 10 \pmod{71}$$

$$2^{67} \equiv 2 \cdot 4 \cdot 10 \equiv 9 \pmod{71}$$

2. megoldás: Amikor a hatványalap relatív prím a modulushoz, érdemes a hatványalapot és a kitevőt is redukálni (az előbit modulo m , az utóbbit modulo $\varphi(m)$) az Euler–Fermat-tétel felhasználásával. Itt viszont $67 < 70 = \varphi(71)$, tehát a kitevő nem lesz kisebb, ha modulo $\varphi(71)$ vesszük. Viszont az Euler–Fermat-tételből következik, hogy $x = 2^{67}$ -re

$8x = 2^{70} \equiv 1 \pmod{71}$, így elég csak ezt a kongruenciát megoldani a 8. feladatban látható módon. Pl. a $8x \equiv 1 \equiv 72 \pmod{71}$ kongruencia egyszerűsítésével azt kapjuk, hogy $x \equiv 9 \pmod{71}$.

8. Oldjuk meg a következő lineáris kongruenciákat!

a) $12x \equiv 15 \pmod{21}$

b) $12x \equiv 4 \pmod{6}$

c) $12x \equiv 4 \pmod{2}$

d) $30x \equiv 4 \pmod{37}$

Megoldás:

a) $12x \equiv 15 \pmod{21}$

$4x \equiv 5 \pmod{7}$

$4x \equiv 12 \pmod{7}$

$x \equiv 3 \pmod{7}$

$x \equiv 3, 10 \text{ vagy } 17 \pmod{21}$

b) Nincs megoldása, mert $(12, 6) = 6$ nem osztója 4-nek.

c) $12x \equiv 4 \pmod{2} \Leftrightarrow 0x \equiv 0 \pmod{2}$, és ezt minden x kielégíti, azaz $x \equiv 0, 1 \pmod{2}$.

d) Ekvivalensen: $-7x \equiv 4 \pmod{37} \equiv -70 \pmod{37}$, és ezt -7 -tel lehet egyszerűsíteni: $x \equiv 10 \pmod{37}$.

Vagy a $30x + 37y = 4$ diofantoszi egyenletet kivívított euklideszi algoritmussal megoldva:

		30	37
	37	0	1
-1.	30	1	0
-4.	7	-1	1
-3.	2	5	-4
-2.	1	-16	13
	0		

Itt a 2 előállításának kétszereséből megkapjuk, hogy $x = 10$ megoldás, másrészt ennek a kongruenciának $(30, 37) = 1$ miatt egyetlen megoldása van, tehát a megoldás $x \equiv 10 \pmod{37}$.

(a 37 oszlopát nem is feltétlenül kell kitölteni, mert csak az x értékét akarjuk megtudni.)

9. a) Határozzuk meg $5^{-1} \pmod{26}$ értékét!

b) Invertálható-e 4 modulo 26?

Megoldás: a) Az $5x \equiv 1 \equiv -25 \pmod{26}$ egyszerűsítésével $x \equiv -5 \equiv 21 \pmod{26}$, tehát $5^{-1} \pmod{26} = 21$.

b) Nem invertálható, ugyanis a 4 nem relatív prím a modulusához (másképpen, a $4x \equiv 1 \pmod{26}$ kongruencia nem oldható meg, mivel $(4, 26) = 2$ nem osztója 1-nek).