Gyakorló feladatok

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

Megoldás:
a) $\left\lfloor \frac{17}{2} \right\rfloor + \left\lfloor \frac{17}{4} \right\rfloor + \left\lfloor \frac{17}{8} \right\rfloor + \left\lfloor \frac{17}{16} \right\rfloor = 8 + 4 + 2 + 1 = 15$.
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 prímhatványok 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 $[100!]_2 = \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{2^2} \right\rfloor + \dots$ nyilván legalább akkora, mint $[100!]_5 = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{5^2} \right\rfloor + 0 + 0 + \dots = 24$, tehát 100! pontosan 24 darab 0-ra végződik.

2. *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 lnko $2^{15}7^{10}$, a lkkt $2^{23}3^{10}7^{13}13^5$.
b) A lnko 7^{10}, a lkkt $2^{23}3^{10}7^{20}11^2 13^5$.

3. *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 tényezős szorzatra 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.

4. *Határozzuk meg* $2^{67} \bmod 71$ *értékét!*

Megoldás: A 67-et 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 kiszámítani.

$$2^1 \equiv 2 \pmod{71}$$
$$2^2 \equiv 4 \pmod{71}$$
$$2^4 \equiv 16 \pmod{71}$$
$$2^8 \equiv 256 \equiv 43 \pmod{71}$$
$$2^{16} \equiv 1849 \equiv 3 \pmod{71}$$
$$2^{32} \equiv 9 \pmod{71}$$
$$2^{64} \equiv 81 \equiv 10 \pmod{71}$$
$$2^{67} \equiv 2 \cdot 4 \cdot 10 \equiv 9 \pmod{71}$$

2. *megoldás:* Amikor a hatványalap relatív prím a modulushoz, érdemes a hatványalapot és a kitevőt is redukálni (az előbbit modulo m, az utóbbit modulo $\varphi(m)$) az Euler–Fermat-tétel felhasználásával. Itt viszont $67 < 70 = \varphi(71)$, tehát a kitevő sem 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 6. feladatban látható módon. Pl. a $8x \equiv 1 \equiv 72 \pmod{71}$ kongruencia egyszerűsítésével azt kapjuk, hogy $x \equiv 9 \pmod{71}$.

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

Megoldás: $2\mathbb{Z}$ helyett $2\mathbb{N}$-ben vizsgáljuk a kérdést, ahol a "lényegében egyértelmű" azt fogja jelenteni, hogy sorrendtől eltekintve egyértelmű. $2\mathbb{N}$-ben nincs egységelem, de még olyan szám sem, amit ilyen esetben egységnek hívhatnánk, azaz amelyik minden más számnak osztója, ugyanis semelyik $2\mathbb{N} \setminus \{0\}$-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 prím, akkor n csak $2m \cdot 2 \cdots 2$ alakban bontható fel felbonthatatlanok szorzatára. Viszont ha $k \geq 2$ és m összetett szám: $m = m_1 m_2$, 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 itt egyértelmű irreducibilisekre való felbontásuk, amelyek nem oszthatók néggyel (ezek maguk irreducibilisek), 2-hatványok, vagy 2-hatványok páratlan ($\mathbb{Z}$-beli) prímszámszorosai.

6. *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)
$$\begin{array}{rcll} 12x & \equiv & 15 & \pmod{21} \\ 4x & \equiv & 5 & \pmod{7} \\ 4x & \equiv & 12 & \pmod{7} \\ x & \equiv & 3 & \pmod{7} \\ x & \equiv & 3, 10 \text{ vagy } 17 & \pmod{21} \end{array}$$

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 kivővített euklideszi algoritmussal megoldva:

		30	37
	37	0	1
$-1\cdot$	30	1	0
$-4\cdot$	7	-1	1
$-3\cdot$	2	5	-4
$-2\cdot$	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.)*

7. *a) Határozzuk meg* $5^{-1} \bmod 26$ *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 modulushoz (másképpen, a $4x \equiv 1 \pmod{26}$ kongruencia nem oldható meg, mivel $(4, 16) = 2$ nem osztója 1-nek).

8. *Oldjuk meg az alábbi kongruenciarendszert!*

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

Megoldás:

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

m_i	3	5	11
M_i	55	33	15
$x_i \equiv M_i^{-1}(m_i)$	1	2	3
a_i	2	3	-4

$x \equiv 55 \cdot 1 \cdot 2 + 33 \cdot 2 \cdot 3 + 15 \cdot 3 \cdot (-4) \equiv 128 \equiv -37 \pmod{165}$.

2. *megoldás:* behelyettesítésekkel. Az első kongruencia ekvivalens azzal, hogy $x = 2 + 3y$ valamely $y \in \mathbb{Z}$-re.
Ezt behelyettestítve a másodikba:

$$2 + 3y \equiv 3 \pmod{5} \Leftrightarrow 3y \equiv 1 \equiv 6 \pmod{5} \Leftrightarrow y \equiv 2 \pmod{5}.$$

Az utóbbi azzal ekvivalens, hogy $y = 2 + 5z$ valamely $z \in \mathbb{Z}$-re, vagyis $x = 2 + 3(2 + 5z) = 8 + 15z$. Ezt behelyettesítve a harmadikba:

$$8 + 15z \equiv -4 \pmod{11} \Leftrightarrow 4z \equiv -12 \pmod{11} \Leftrightarrow z \equiv -3 \pmod{11}.$$

Tehát $z = -3 + 11u$ valamely $u \in \mathbb{Z}$-re, amiből $x = 8 + 15(-3 + 11u) = -37 + 165u$, vagyis $x \equiv -37 \pmod{165}$.