Gyakorló feladatok

1. *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.

2. *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.

3. *Határozzuk meg* $2^{67} \bmod 71$ *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.

$$\begin{aligned}
2^1 &\equiv 2 \pmod{71}\\
2^2 &\equiv 4 \pmod{71}\\
2^4 &\equiv 16 \pmod{71}\\
2^8 &\equiv 256 \equiv -28 \pmod{71}\\
2^{16} &\equiv 784 \equiv 3 \pmod{71}\\
2^{32} &\equiv 9 \pmod{71}\\
2^{64} &\equiv 81 \equiv 10 \pmod{71}\\
2^{67} &\equiv 2\cdot 4\cdot 10 \equiv 9 \pmod{71}
\end{aligned}$$

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 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 az 5. vagy 6. feladatban látható módon. Pl. a $8x \equiv 1 \equiv 72 \pmod{71}$ kongruencia egyszerűsítésével azt kapjuk, hogy $x \equiv 9 \pmod{71}$.

4. *Határozzuk meg azokat az n pozitív egészeket, amelyekre $\varphi(n) = 6$.*

Megoldás: A $\varphi(p_1^{a_1}\cdots p_r^{a_r}) = (p_1-1)p_1^{a_1-1}\cdots(p_r-1)p_r^{a_r-1}$ formulából nyilvánvaló, hogy n-nek nem lehet 7-nél nagyobb prímosztója.
Ha $7 \mid n$, akkor 7 kitevője csak 1, mert $7 \nmid 6$, tehát $n = 7m$, ahol $(7, m) = 1 \Rightarrow \varphi(n) = 6\cdot\varphi(m) \Rightarrow \varphi(m) = 1 \Rightarrow m = 1$ vagy 2 (ui. $n \geq 3$-ra 1 és $n-1$ is relatív prímek n-hez), azaz $n = 7$ vagy 14.
5 nem lehet osztója n-nek, mert $4 \nmid 6 = \varphi(n)$. Marad, hogy n prímosztói csak 2 és 3, és ebből a 3 pontosan a 2. hatványon szerepel, mivel $3 \mid \varphi(n)$, de $3^2 \nmid \varphi(n)$. Tehát $n = 2^k 3^2$ $\Rightarrow \varphi(n) = \varphi(2^k)\varphi(9) = \varphi(2^k)\cdot 6 \Rightarrow k = 0, 1 \Rightarrow n = 9, 18$.
Összefoglalva: $n = 7, 14, 9, 18$.

5. *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:

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

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.)

6. *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).

7. *Bizonyítsuk be Wilson tételét: $(p-1)! \equiv -1 \pmod p$ minden p prímre.*

Megoldás: $p = 2$-ra $1! = 1 \equiv -1 \pmod 2$.
$p \geq 2$-re párosítsuk az $1, 2, \ldots, p-1$ számokat a mod p inverzükkel. Lesz olyan szám, aminek sajátmaga az inverze:

$$x \equiv x^{-1}\ (p) \ \Leftrightarrow\ x^2 \equiv 1\ (p) \ \Leftrightarrow\ p \mid (x^2 - 1) = (x-1)(x+1),$$

és ez utóbbi ekvivalens azzal, hogy $p \mid x - 1$ vagy $p \mid x + 1$, mivel p prím. Tehát 1-nek és $p-1$-nek önmaga az inverze, a többieknek nem. Ezért megfelelően csoportosítva a $(p-1)!$ tényezőit,

$$1 \cdot 2 \cdot (p-1) \equiv 1^{(p-3/2)} \cdot 1 \cdot (-1) \equiv -1 \pmod p.$$

8. *Oldjuk meg az alábbi kongruenciarendszert!*

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 8 \\ x &\equiv -4 \pmod{11} \end{aligned}$$

Megoldás:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 8 \\ x &\equiv -4 \pmod{11} \end{aligned}$$

m_i	3	8	11
M_i	88	33	24
$x_i \equiv M_i^{-1}(m_i)$	1	1	6
a_i	2	3	-4

$x \equiv 88 \cdot 1 \cdot 2 + 33 \cdot 1 \cdot 3 + 24 \cdot 6 \cdot (-4) = 176 + 99 - 576 = -301 \equiv -37 \pmod{264}$.

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

$$2 + 3y \equiv 3\ (8) \ \Leftrightarrow\ 3y \equiv 1 \equiv 9\ (8) \ \Leftrightarrow\ y \equiv 3\ (8).$$

Az utóbbi azzal ekvivalens, hogy $y = 3 + 8z$ valamely $z \in \mathbb{Z}$-re, vagyis $x = 2 + 3(3 + 8z) = 11 + 24z$. Ezt behelyettesítve a harmadikba:

$$11 + 24z \equiv -4\ (11) \ \Leftrightarrow\ 24z \equiv -15\ (11) \ \Leftrightarrow\ 2z \equiv -4\ (11) \ \Leftrightarrow\ z \equiv -2\ (11).$$

Tehát $z = -2 + 11u$ valamely $u \in \mathbb{Z}$-re, amiből $x = 11 + 24(-2 + 11u) = -37 + 264u$, vagyis $x \equiv -37 \pmod{264}$.

9. $14^{20} \bmod 440 = ?$

Megoldás: A hatványalap nem relatív prím a modulushoz: $(14, 440) = 2$, ráadásul a modulus meglehetősen nagy összetett szám, ezért a kongruenciát szétbontjuk a kínai maradéktétel szerint vele ekvivalens relatív prím modulusú kongruenciákból álló kongruencia-rendszerre. Azt az x-et keressük, amelyre

$$\begin{aligned} x &\equiv 14^{20} \quad (8) \\ x &\equiv 14^{20} \quad (5) \\ x &\equiv 14^{20} \quad (11) \end{aligned}$$

Az elsőnek a megoldása $x \equiv 0\ (8)$, mert $2 \mid 14$, tehát már a harmadik hatványa is osztható 8-cal. A másik kettőben a hatványalap relatív prím a modulushoz, így a hatványalap mod m redukálása mellett, szükség esetén redukálhatjuk a kitevőt is $\varphi(m)$ szerint ($\varphi(5) = 4$ és $\varphi(11) = 10$):

$$14^{20} \equiv (-1)^{20} \equiv 1\ (5) \text{ és } 14^{20} \equiv 3^0 \equiv 1\ (11).$$

Ezután a kínai maradéktétel megoldási módszerével, de ebben az esetben akár fejben is, összerakhatjuk a megoldást.

$$\begin{aligned} x &\equiv 0 \quad (8) \\ x &\equiv 1 \quad (5) \\ x &\equiv 1 \quad (11) \end{aligned}$$

A 2. és 3. kongruenciából $55 \mid (x - 1)$, azaz $x \equiv 56\ (55)$, és $8 \mid 56$, tehát

$$14^{20} \equiv x \equiv 56 \pmod{440}$$

megoldása a teljes rendszernek is.