

Gyakorló feladatok

1. a) Mi a 2 kitevője $17!$ kanonikus alakjában?
b) Hány nullára végződik a $100!$ szám?
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) $2^{23}3^{10}7^{13}$, $2^{15}7^{10}13^5$, $3^{15}7^{20}11^2$.
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?)
4. Határozzuk meg $2^{67} \bmod 71$ értékét!
5. A páros számok körében definiált oszthatóságra nézve mely számok írhatók fel lényegében egyértelműen felbonthatatlanok szorzataként?
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) $30x \equiv 4 \pmod{37}$
7. a) Határozzuk meg $5^{-1} \bmod 26$ értékét!
b) Invertálható-e 4 modulo 26?
8. Oldjuk meg az alábbi kongruenciarendszert!

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

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

$$x \equiv -4 \pmod{11}$$

Házi feladatok

Beadási határidő: szeptember 30.

A feladatokra teljes, tömör és világos megoldást kérünk részletszámításokkal, indoklással, az eredmény leírása nem elegendő. A feladatok egy pontot érnek, a csillagos kettőt. A hétből hat feladat megoldását adjuk be, ezekből legalább 4 pontot el kell érni! Együtt gondolkozni szabad, de más megoldását lemásolni nem!

1. Hány 0-ra végződik az $1234!$ szám?
2. Bizonyítsuk be, hogy minden $a, b > 1$ egész számra

$$[a, b] \mid a + b \Leftrightarrow a = b.$$

3. Számítsuk ki $25^{101} \bmod 11$ értékét!
4. Oldjuk meg a következő lineáris kongruenciákat!
 - a) $4x \equiv 6 \pmod{14}$,
 - b) $4x \equiv 6 \pmod{16}$,
 - c) $4x \equiv 8 \pmod{16}$.
5. Számítsuk ki $3^{-1} \bmod 13$, $3^{-1} \bmod 26$ és $3^{-1} \bmod 52$ értékét!
6. Oldjuk meg az alábbi kongruenciarendszert!

$$x \equiv 1 \pmod{3}$$

$$x \equiv 1 \pmod{4}$$

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

- 7*. Adott $m \in \mathbb{N}^+$ -ra határozzuk meg az összes olyan b egész számot, amelyre

$$\{t_1 + b, t_2 + b, \dots, t_{\varphi(m)} + b\}$$

redukált maradékrendszer modulo m , ha $\{t_1, t_2, \dots, t_{\varphi(m)}\}$ redukált maradékrendszer modulo m !