

1. Határozzuk meg az Euklidészi algoritmussal  $\lnko(504, 372)$ -t! Határozzuk meg  $lkkt(504, 372)$ -t! Hány osztója van 504-nek?
2. A  $\{0, 1, \dots, 14\} \pmod{15}$  teljes maradékrendszer mely elemeihez tartoznak a következő számok: 221, 152, 193, 46, 66, 209, 11980, 46628?
3. Bizonyítsuk be, hogy minden  $n$  természetes számra  $n^7 - n$  osztható 42-vel!
4. Bizonyítsuk be, hogy  $39^{14} - 1$  osztható 5-tel!
5. Határozzuk meg  $x$ -et!
  - (a)  $5^{1997} \equiv x \pmod{17}$
  - (b)  $108^{182} \equiv x \pmod{19}$
  - (c)  $205^{206^{207}} \equiv x \pmod{103}$
6. Mi az alábbi lineáris kongruenciák megoldása?
  - (a)  $8x \equiv 3 \pmod{21}$
  - (b)  $9x \equiv 24 \pmod{96}$
7. Ha 10839-et és 11863-at elosztjuk ugyanazzal a háromjegyű számmal, akkor ugyanazt a maradékot kapjuk. Mi ez a maradék?

---

8. **[ZH 2008. november 17.]** Igazoljuk, hogy ha  $m$  és  $n$  pozitív egészek, akkor  $d(n)d(m) = d(\lnko(n, m))d(lkkt(n, m))$  teljesül, ahol  $d(k)$  a  $k$  pozitív osztóinak számát,  $\lnko(n, m)$  és  $lkkt(n, m)$  pedig rendre az  $n$  és  $m$  legnagyobb közös osztóját ill. legkisebb közös többszörösét jelölik.
9. **[PZH 2008. december 5.]** Tudjuk, hogy  $n$  és  $m$  olyan pozitív egészek, amikre  $\lnko(n, m) = 10$  és  $lkkt(n, m) = 1000$ , ahol  $\lnko(n, m)$  és  $lkkt(n, m)$  pedig rendre az  $n$  és  $m$  legnagyobb közös osztóját ill. legkisebb közös többszörösét jelölik. Határozzuk meg az  $nm$  szorzatot.
10.  $a$  és  $b$  páratlan számok,  $c = a^2 + b^2$ . Mennyi  $c$  és 4 legnagyobb közös osztója?
11. Van-e olyan  $a$  és  $b$  szám, hogy  $\lnko(a, b) = 3$  és  $a + b = 100$ ? És ha  $\lnko(a, b) = 5$ ?
12. Melyek azok a  $p$  prímszámok, amelyekre  $p + 10$  és  $p + 14$  is prím?
13. Bizonyítsuk be, hogy tetszőleges  $p$  prímszámra:  $(a + b)^p \equiv a^p + b^p \pmod{p}$
14. Bizonyítsuk be, hogy minden  $n$  természetes számra  $n^{11} + 10n$  osztható 11-gyel!
15. Határozzuk meg  $x$ -et!
  - (a)  $49^{49} \equiv x \pmod{15}$
  - (b)  $42^{600} \equiv x \pmod{13}$
  - (c)  $x^{11999} \equiv 5 \pmod{13}$
  - (d)  $1998! + 111^{1998} \equiv x \pmod{1999}$
16.  $15x \equiv 3 \pmod{18}$

17. Létezik-e olyan háromjegyű szám, amely osztóinak száma osztható 11-gyel?
18. Bizonyítsuk be, hogy a  $\frac{21n+4}{14n+3}$  tört semmilyen  $n$ -re nem egyszerűsíthető!
19. Bizonyítsuk be, hogy ha az  $n > 1$  számnak 2005 osztója van, akkor  $n$  nem lehet egy egész szám ötödik hatványa!
20. Bizonyítsuk be, hogy tetszőleges  $p$  prímszámra:

$$\binom{2p}{p} \equiv 2 \pmod{p}$$

21. Egy perzsa sahnak 100 felesége van, a börtönében is épp 100 rab sínylődik, 1-től 100-ig számozott cellákban. A börtöncellák zárjai „kétállásúak”: ha egyet fordítanak rajtuk, a bezárt ajtó kinyílik, a nyitott ajtó bezáródik. A sah születésnapján a 100 feleség végigvonul a börtönön és a zárossal játszanak. Az első feleség minden záron egyet fordít, a második feleség minden második ajtó zárján egyet fordít, stb., a  $k$ -edik feleség minden  $k$ -edik ajtó zárján egyet fordít, egészen a századik feleségig. Végül azok a rabok, akiknek az ajtaja nyitva van, kiszabadulnak. Milyen sorszámú cellában laknak a szerencsések?

### Hasznos tudnivalók

- Ha  $a \equiv b \pmod{m}$ , akkor
  - $a \pm c \equiv b \pm c \pmod{m}$
  - $a \cdot c \equiv b \cdot c \pmod{m}$
  - $\frac{a}{c} \equiv \frac{b}{c} \pmod{\frac{m}{c}}$ , ha  $c \mid a, b, m$
  - $\frac{a}{c} \equiv \frac{b}{c} \pmod{m}$ , ha  $(c, m) = 1$
  - $a \cdot c \equiv b \cdot d \pmod{m}$ , ha  $c \equiv d \pmod{m}$
- Euler-Fermat témakör
  - $\varphi(m)$ : 1 és  $m$  közötti  $m$ -hez relatív prímelek száma;  $\varphi(p) = p - 1$ , ha  $p$  prím
  - $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ , ha  $p$  prím
  - $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ , ha  $(a, b) = 1$
  - Ha  $(a, m) = 1$ , akkor  $a^{\varphi(m)} \equiv 1 \pmod{m}$
  - Ha  $p$  prím és  $p \nmid a$ , akkor  $a^{p-1} \equiv 1 \pmod{p}$
  - Ha  $p$  prím, akkor  $a \equiv a^p \pmod{p}$
- Wilson-tétel
 
$$(n-1)! \equiv \begin{cases} -1 \pmod{n} & \text{ha } n \text{ prím} \\ 2 \pmod{n} & \text{ha } n = 4 \\ 0 \pmod{n} & \text{ha } n > 4 \text{ összetett} \end{cases}$$
- $a \cdot x \equiv b \pmod{m}$  lineáris kongruenciának
  - $\exists$  megoldása  $\Leftrightarrow (a, m) \mid b$
  - $\exists$  megoldása  $\Leftrightarrow (a, m) \pmod{m}$  megoldása létezik