

1. **Határozzuk meg az Euklidészi algoritmussal $lnko(504, 372)$ -t! Határozzuk meg $lkkt(504, 372)$ -t! Hány osztója van 504-nek?**

$$\begin{aligned} 504 &= 1 \cdot 372 + 132 \\ 372 &= 2 \cdot 132 + 108 \\ 132 &= 1 \cdot 108 + 24 \\ 108 &= 4 \cdot 24 + \mathbf{12} \\ 24 &= 2 \cdot 12 + 0, \end{aligned}$$

tehát $lnko(504, 372) = 12$.

$lnko(x, y) \cdot lkkt(x, y) = x \cdot y$, ezért $lkkt(504, 372) = 504 \cdot 372 / 12 = 15624$. Másképp is lehet, a prímfelbontások alapján $504 = 2^3 \cdot 3^2 \cdot 7$, $372 = 2^2 \cdot 3 \cdot 31$, ezért $lkkt(504, 372) = 2^3 \cdot 3^2 \cdot 7 \cdot 31 = 15624$.

$504 = 2^3 \cdot 3^2 \cdot 7$, ezért $(3 + 1)(2 + 1)(1 + 1) = 24$ osztója van.

2. **A $\{0, 1, \dots, 14\} \pmod{15}$ teljes maradékrendszer mely elemeihez tartoznak a következő számok: 221, 152, 193, 46, 66, 209, 11980, 46628?**

11, 2, 13, 1, 6, 14, 10, 8, feltéve, hogy nem gépeltem el semmit.

3. **Bizonyítsuk be, hogy minden n természetes számra $n^7 - n$ osztható 42-vel!**

Azt kell belátni, hogy $n^7 - n$ osztható 2-vel, 3-mal és 7-tel. $n^7 - n = n(n^6 - 1) = n(n^3 - 1)(n^3 + 1)$. 2-vel oszthatóság triviális (n^7 és n paritása azonos, így különbségük páros). Héttel oszthatóság ekvivalens azzal, hogy $(\pmod{7}) 0$ az eredmény, kis-Fermat tétel alapján $n^7 - n \equiv n - n \equiv 0 \pmod{7}$. 3-mal oszthatóság: $n(n^3 - 1)(n^3 + 1) \equiv n(n - 1)(n + 1)$ kis-Fermat tétel alapján, azaz három egymást követő szám szorzata, amiből az egyik biztos osztható 3-mal.

4. **Bizonyítsuk be, hogy $39^{14} - 1$ osztható 5-tel!**

$$39^{14} - 1 \equiv (-1)^{14} - 1 \equiv 1 - 1 \equiv 0 \pmod{5}.$$

5. **Határozzuk meg x -et!**

(a) $5^{1997} \equiv x \pmod{17}$

$(5, 17) = 1$, tehát az Euler-Fermat tétel használatával:

$$\begin{aligned} 5^3 \cdot 5^{1997} &\equiv 5^3 \cdot x \pmod{17} \\ 5^{2000} &\equiv 6x \pmod{17} \\ (5^{16})^{125} &\equiv 6x \pmod{17} \\ 1^{125} &\equiv 6x \pmod{17} \\ 6x &\equiv 1 \pmod{17} \\ 6x &\equiv 18 \pmod{17} \\ x &\equiv 3 \pmod{17} \end{aligned}$$

(b) $108^{182} \equiv x \pmod{19}$

$(13, 19) = 1$, tehát az Euler-Fermat tétel használatával:

$$\begin{aligned}13^{182} &\equiv x \pmod{19} \\(13^{18})^{10} \cdot 13^2 &\equiv x \pmod{19} \\13^2 &\equiv x \pmod{19} \\169 &\equiv x \pmod{19} \\17 &\equiv x \pmod{19}\end{aligned}$$

(c) $205^{206^{207}} \equiv x \pmod{103}$
 $205^{206^{207}} \equiv (-1)^{206^{207}} \equiv 1 \equiv x \pmod{103}$

6. Mi az alábbi lineáris kongruenciák megoldása?

(a) $8x \equiv 3 \pmod{21}$

Mivel $(21, 8) = 1$, és $1 \mid 3$, ezért létezik megoldás, és pontosan 1 megoldás létezik.

$$\begin{aligned}8x &\equiv 24 \pmod{21} \\x &\equiv 3 \pmod{21}\end{aligned}$$

(b) $9x \equiv 24 \pmod{96}$

Mivel $(96, 9) = 3$, és $3 \mid 24$, ezért létezik megoldás, és pontosan 3 megoldás létezik.

$$\begin{aligned}3x &\equiv 8 \pmod{32} \\3x &\equiv 72 \pmod{32} \\x &\equiv 24 \pmod{32} \\x_1 &\equiv 24 \pmod{96} \\x_2 &\equiv 56 \pmod{96} \\x_3 &\equiv 88 \pmod{96}\end{aligned}$$

7. Ha 10839-et és 11863-at elosztjuk ugyanazzal a háromjegyű számmal, akkor ugyanazt a maradékot kapjuk. Mi ez a maradék? Ha ez a háromjegyű szám x , akkor a feladat szövege szerint $10839 \equiv 11863 \pmod{x}$. Definíció szerint ez azt jelenti, hogy $x \mid 11863 - 10839 = 1024$ -et. Vagyis x kizárólag 128, 256 vagy 512 lehet, így a keresett maradék 87.

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.

Fel fogjuk használni, hogy $\min(a, b) \max(a, b) = ab$, valamint $\min(a, b) + \max(a, b) = a + b$. n és m kanonikus alakjával fogunk dolgozni, $n = \prod_{i=1}^k p_i^{\alpha_i}$ és $m = \prod_{i=1}^k p_i^{\beta_i}$.

Bal oldal: $d(n)d(m) = \prod_{i=1}^k (\alpha_i + 1)(\beta_i + 1) = \prod_{i=1}^k (\alpha_i \beta_i + \alpha_i + \beta_i + 1)$

Jobb oldal: $d(\lnko(n, m))d(\lkkt(n, m)) = \prod_{i=1}^k (\min(\alpha_i, \beta_i) + 1)(\max(\alpha_i, \beta_i) + 1) = \prod_{i=1}^k (\min(\alpha_i, \beta_i) \max(\alpha_i, \beta_i) + \min(\alpha_i, \beta_i) + \max(\alpha_i, \beta_i) + 1) = \prod_{i=1}^k (\alpha_i \beta_i + \alpha_i + \beta_i + 1)$.

Azaz ekvivalens átalakításokkal ugyanarra jutottunk, tehát az állítás igaz.

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.

Tétel: $\lnko(n, m)\lkkt(n, m) = nm$. Ebből $nm = 10 \cdot 1000 = 10000$.

10. **a és b páratlan számok, $c = a^2 + b^2$. Mennyi c és 4 legnagyobb közös osztója?**
 Legyen $a = 2k + 1$ és $b = 2l + 1$, ekkor $c = (2k + 1)^2 + (2l + 1)^2 = 4(k^2 + l^2 + k + l) + 2$.
 Ekkor az Euklidészi algoritmussal

$$\begin{aligned} c &= (k^2 + l^2 + k + l) \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0, \end{aligned}$$

vagyis 2.

Persze az is jó (bár kevésbé elegáns) megoldás, hogy két páratlan szám összege páros lesz, így a 2-vel oszthatóság biztos, és mutatunk egy ellenpéldát, miszerint c nem osztható 4-gyel.

11. **Van-e olyan a és b szám, hogy $\text{lnko}(a, b) = 3$ és $a + b = 100$? És ha $\text{lnko}(a, b) = 5$?**
 Az első esetben 3 osztója mindkét számnak, azaz $a = 3k$ és $b = 3l$, ekkor $a + b = 3(k + l) = 100$, 100 viszont nem osztható hárommal, tehát nincs. A második esetben igen, pl. 55 és 45.

12. **Melyek azok a p prímszámok, amelyekre $p + 10$ és $p + 14$ is prím?**
 A 2 nem jó, a 3 jó. Nézzük meg a nagyobbakat! 10 3-mal osztva 1 maradékot, míg 14 pedig 2 maradékot ad. A $p > 3$ prímszám biztos nem osztható 3-mal, így 1 vagy 2 maradékot ad vele osztva. Első esetben $p + 14$, míg a másodikban $p + 10$ lesz osztható 3-mal, vagyis összetett. Tehát az egyetlen megoldás 3.

13. **Bizonyítsuk be, hogy tetszőleges p prímszámra: $(a + b)^p \equiv a^p + b^p \pmod{p}$**
 A kis Fermat-tétel segítségével triviális:

$$(a + b)^p \equiv a + b \equiv a^p + b^p \pmod{p}$$

14. **Bizonyítsuk be, hogy minden n természetes számra $n^{11} + 10n$ osztható 11-gyel!**
 A kis Fermat-tétel használatával (mivel 11 prím):

$$n^{11} + 10n \equiv n + 10n \equiv 11n \equiv 0 \pmod{11}$$

15. **Határozzuk meg x -et!**

(a) $49^{49} \equiv x \pmod{15}$

Felhasználva, hogy $(4, 15) = 1$ (Euler-Fermat tételhez), valamint $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$,

$$\begin{aligned} 49^{49} &\equiv 4^{49} \equiv x \pmod{15} \\ 4 \cdot 4^{48} &\equiv 4 \cdot (4^8)^6 \equiv x \pmod{15} \\ 4 &\equiv x \pmod{15} \end{aligned}$$

(b) $42^{600} \equiv x \pmod{13}$

Az előzőhöz hasonlóan

$$\begin{aligned} 42^{600} &\equiv 3^{600} \equiv x \pmod{13} \\ 3^{600} &\equiv 3^{12 \cdot 50} \equiv (3^{12})^{50} \equiv x \pmod{13} \\ 1 &\equiv x \pmod{13} \end{aligned}$$

(c) $x^{11999} \equiv 5 \pmod{13}$

x nem lehet 0, ezért biztos, hogy $(x, 13) = 1$ (13 prímsége miatt). Ezért szorozhatunk vele büntetlenül, és az Euler-Fermat tételt is használhatjuk.

$$\begin{aligned}x^{11999} \cdot x &\equiv 5x \pmod{13} \\x^{12 \cdot 1000} &\equiv (x^{12})^{1000} \equiv 5x \pmod{13} \\1 &\equiv 5x \pmod{13} \\40 &\equiv 5x \pmod{13} \\8 &\equiv x \pmod{13}\end{aligned}$$

(d) $1998! + 111^{1998} \equiv x \pmod{1999}$

Wilson-tétel és Euler-Fermat tétel használatával (a feltételek teljesülnek, 1999 prím):
 $1998! + 111^{1998} \equiv -1 + 1 \equiv 0 \equiv x \pmod{1999}$.

16. $15x \equiv 3 \pmod{18}$

Mivel $(15, 18) = 3$, és $3 \mid 3$, ezért létezik megoldás, és pontosan 3 megoldás létezik.

$$\begin{aligned}5x &\equiv 1 \pmod{6} \\5x &\equiv -5 \pmod{6} \\x &\equiv -1 \pmod{6} \\x &\equiv 5 \pmod{6}\end{aligned}$$

Tehát a 3 megoldás:

$$\begin{aligned}x_1 &\equiv 5 \pmod{18} \\x_2 &\equiv 11 \pmod{18} \\x_3 &\equiv 17 \pmod{18}\end{aligned}$$

17. **Létezik-e olyan háromjegyű szám, amely osztóinak száma osztható 11-gyel?**

Mivel 11 prímszám, ennek a keresett számnak a prímfelbontása így néz ki: $p_1^{\alpha_1} \cdot \dots \cdot p_i^{10} \cdot \dots \cdot p_k^{\alpha_k}$.
Ha csak a legkisebb prímszámot, 2-t engedjük meg a prímfelbontásban, akkor is már $2^{10} = 1024$ lenne az első ilyen szám, tehát háromjegyűvel biztos nem megoldható.

18. **Bizonyítsuk be, hogy a $\frac{21n+4}{14n+3}$ tört semmilyen n -re nem egyszerűsíthető!**

Keressük meg $lnko$ -t! Euklidészi algoritmussal:

$$\begin{aligned}21n + 4 &= 1 \cdot (14n + 3) + (7n + 1) \\14n + 3 &= 2 \cdot (7n + 1) + 1 \\7n + 1 &= 1 \cdot (7n + 1) + 0,\end{aligned}$$

vagyis a számláló és nevező relatív prím.

19. **Bizonyítsuk be, hogy ha az $n > 1$ számnak 2005 osztója van, akkor n nem lehet egy egész szám ötödik hatványa!**

Ha n egy egész szám ötödik hatványa, akkor a prímtényezős felírásban a kitevők így néznek ki: $5\alpha_1, \dots, 5\alpha_k$, tehát osztóinak száma $(5\alpha_1 + 1) \cdot \dots \cdot (5\alpha_k + 1)$. 2005 prímtényezős felbontása $5 \cdot 401$, viszont az osztók száma nem osztható 5-tel (minden tag $5\alpha_i + 1$ alakú).

20. Bizonyítsuk be, hogy tetszőleges p prímszámra:

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

$$\frac{(2p)!}{p!p!} \equiv 2 \pmod{p}$$

$$\frac{2p(2p-1)\dots(p+1)p!}{p(p-1)!p!} \equiv 2 \pmod{p}$$

A tört nevezőjében a szorzat minden eleme relatív prím p -hez (hiszen az prím), így $(p-1)!$ -sal bátran szorozhatunk.

$$2(2p-1)\dots(p+1) \equiv 2(p-1)! \pmod{p}$$

$$2(p-1)(p-2)\dots 2 \cdot 1 \equiv 2(p-1)! \pmod{p}$$

$$2(p-1)! \equiv 2(p-1)! \pmod{p}$$

És kész is vagyunk, persze a Wilson-tétel segítségével még szebbé tehetjük:

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

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 sahn 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?

Vegyük észre, hogy pontosan akkor lesz nyitva az i -edik cella, ha i osztóinak száma páratlan! Ez azért van, mert minden cella zárján az összes „osztója” fordít egyet. Azon számoknak van páratlan osztójuk, amiknek a prímtényező felbontásában csupa páros hatvány szerepel – ha lenne a kanonikus alakban $p_i^{2\alpha_i+1}$ tag, akkor ez az osztók számának számításakor $(2\alpha_i + 1) + 1 = 2(\alpha_i + 1)$ tagot jelentene, vagyis párossá tenné azt. Ha egy szám prímtényező felírásában minden kitevő páros, akkor négyzetszámról beszélünk. Tehát akkor és csak akkor szabadulhat ki egy rab, ha négyzetszám a cellájának sorszáma. 1 és 100 közötti négyzetszámok tehát: 1,4,9,16,25,36,49,64,81,100. Ők 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