Bevezetés az algebrába 1

Egész számok

Wettl Ferenc diái alapján

Kongruenciák

Kongruenciák

Kongruenciák definíciója és műveletei

D **A mod művelet**

$a \in \mathbb{Z}$, $m \in \mathbb{N}^+$. Az a-nak m-mel való osztási maradékát $a \bmod m$ jelöli. (Itt mod egy bináris, azaz kétváltozós művelet.)

P $12 \bmod 5 = 2$, $(-12) \bmod 5 = 3$.

D **Kongruencia**

$a, b \in \mathbb{Z}$, $m \in \mathbb{N}^+$. Azt mondjuk, hogy a kongruens b-vel modulo m, ha $m \mid a - b$. (m a kongruencia modulusa.)
Jelölései: $a \equiv b \pmod{m}$, $a \equiv b \mod m$, $a \equiv b \ (m)$.

Á $a \equiv b \pmod{m} \iff a \bmod m = b \bmod m$

B Legyen $a = mq_1 + r_1$ és $b = mq_2 + r_2$ maradékos osztás m-mel. Ekkor $a \bmod m = r_1$ és $b \bmod m = r_2$.
($\Rightarrow$) $a - b = m(q_1 - q_2) + (r_1 - r_2)$, és $m \mid (a - b) \Rightarrow m \mid (r_1 - r_2)$. De $|r_1 - r_2| < m$, így $r_1 - r_2 = 0$, azaz $a \bmod m = r_1 = r_2 = b \bmod m$.
($\Leftarrow$) $r_1 = r_2 \Rightarrow a - b = m(q_1 - q_2)$ osztható m-mel.

P $12 \equiv 107 \ (5)$, mert $5 \mid 107 - 12$; $-6 \equiv 99 \ (5)$, mert $5 \mid 99 - (-6)$.

P $13 \not\equiv 23 \ (9)$, mert $9 \nmid 23 - 13$.

Á $a \equiv b \ (m) \iff$ van olyan k egész, hogy $a = b + km$.

T **A kongruencia ekvivalenciareláció**

Reflexív: $a \equiv a \pmod{m}$,

Szimmetrikus: $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$

Tranzitív: $a \equiv b \pmod{m}$, $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

B Az oszthatóság elemi tulajdonságaiból.

- A mod m kongruencia megad egy osztályozást $\mathbb{Z}$-n: egy osztályba kerülnek azok, amelyek kongruensek egymással.

P $\mathbb{Z} = \{\dots, -3, 0, 3, \dots\} \dot\cup \{\dots, -2, 1, 4, \dots\} \dot\cup \{\dots, -1, 2, 5, \dots\}$

D modulo m maradékosztályok:

az m szerint azonos maradékot adó, azaz egymással kongruens egészek osztályai (m darab)

T **Műveletek kongruenciákkal**

Ha $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}^+$, és $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$, akkor

(1) $a + c \equiv b + d \pmod{m}$ (spec. $a + c \equiv b + c \pmod{m}$)

(2) $a - c \equiv b - d \pmod{m}$ (spec. $a - c \equiv b - c \pmod{m}$)

(3) $ac \equiv bd \pmod{m}$ (spec. $ac \equiv bc \pmod{m}$)

B (1), (2): ✓

(3): Speciális: $m \mid a - b \Rightarrow m \mid c(a - b) = ac - bc$.

Általános a speciálisból: $ac \equiv bc \equiv bd \pmod{m}$

P $7 \equiv 33 \pmod{13} \rightsquigarrow 27 \equiv 53 \pmod{13}$ $[+20]$

P $7 \equiv 33 \pmod{13} \rightsquigarrow 70 \equiv 330 \pmod{13}$ $[\cdot 10]$

P $7 \equiv 33 \pmod{13}$, $4 \equiv 30 \pmod{13} \rightsquigarrow 28 \equiv 990 \pmod{13}$

T **Kongruenciák egyszerűsítése**

Legyen $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{N}^+$. Ekkor

$$ac \equiv bc \pmod{m} \iff a \equiv b \left(\mathrm{mod}\, \frac{m}{(m,c)}\right)$$

Következésképpen ha $(c, m) = 1$, akkor az $ac \equiv bc \pmod{m}$ kongruencia egyszerűsíthető c-vel, azaz ekkor $a \equiv b \pmod{m}$.

B Legyen $d = (m, c)$ Ekkor

$ac \equiv bc \pmod{m} \iff m \mid (a-b)c \iff \frac{m}{d} \mid (a-b)\frac{c}{d}$, de $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, így az utóbbi ekvivalens azzal, hogy $\frac{m}{d} \mid (a-b)$.

P $a \in \mathbb{Z}$-re $3a \equiv 15 \pmod{7} \iff a \equiv 5 \pmod{7}$, ui. $(3, 7) = 1$,

de $6a \equiv 18 \pmod{21} \iff a \equiv 3 \pmod{7} \iff a \equiv 3,\ 10$ v.17 $\pmod{21}$

T $a \equiv b \pmod{m}$, $n \in \mathbb{N}^+ \Rightarrow a^n \equiv b^n \pmod{m}$

B **1. biz.:** n-szer összeszorozva az $a \equiv b \pmod{m}$ kongruenciát;

2. biz.: az $a^n - b^n = (a-b)(a^{n-1} + \ldots + b^{n-1})$ összefüggésből.

T $a, n > 1$ egészek, és $a^n - 1$ prím $\Rightarrow a = 2$, és n prím.

B Az előző tételből $(a-1) \mid (a^n - 1)$.

- Ha $a > 2$, akkor $1 < a - 1 < a^n - 1 \Rightarrow (a-1)$ valódi osztó $\Rightarrow a^n - 1$ nem felbonthatatlan, azaz nem prím.
- Ha $a = 2$ és $n = pq$ valódi felbontás, akkor $a^{pq} - 1 = (a^p)^q - 1$ az előző szerint nem prím, mert $a^p > 2$.

D Mersenne-prímek: a $2^p - 1$ alakú prímek, ahol p prím. Pl. $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$ prímek, de $2^{11} - 1 = 2047 = 23 \cdot 89$ nem prím.

Kongruenciák

Számolás modulo m

P $7! \bmod 13 = ?$

m Az egymás utáni műveleteknél mindig vehetjük a maradékot, sőt, a legkisebb abszolút értékű maradékot.

$$\begin{array}{lcccccccccccl} 7! = 1 & \cdot & 2 & \cdot & 3 & \cdot & 4 & \cdot & 5 & \cdot & 6 & \cdot & 7 \\ & & 2 & & 6 & & -2 & & 3 & & 5 & & -4 & \equiv 9 \pmod{13} \end{array}$$

P $3^{32} \equiv ? \pmod{13}$

m Elég ötször négyzetre emelni:

mod 13

n	1	2	4	8	16	32
3^n	3	-4	3	-4	3	-4

$$\Rightarrow 3^{32} \equiv -4 \equiv 9 \pmod{13}$$

F Számítsuk ki a 91^{89} hatványt modulo 11 úgy, hogy először egyszerűbb alakra hozzuk a hatványalapot modulo 11, majd a 2-hatványadik hatványokból rakjuk össze a 89-ediket. ($89 = X_2$, $X = ?$)

m $91 \equiv 3 \pmod{11}$, $89 = 1011001_2 \Rightarrow$
$91^{89} \equiv 3^{89} = 3^{64} \cdot 3^{16} \cdot 3^8 \cdot 3^1 \equiv 4 \cdot 3 \cdot 5 \cdot 3 \equiv 4 \pmod{11}$

Kongruenciák

Maradékrendszerek

D **TMR**

Egészek egy halmaza teljes maradékrendszer modulo m (TMR mod m), ha minden egész szám ennek a halmaznak pontosan egy elemével kongruens mod m.

Ekv.: $0, 1, \ldots, m-1$ maradékot adnak valamilyen sorrendben.

P A $\{0, 1, \ldots, m-1\}$ halmaz TMR mod m.

P $\left\{-\lfloor \frac{m-1}{2} \rfloor, \ldots, 0, \ldots, \lfloor \frac{m}{2} \rfloor\right\}$ TMR modulo m (a legkisebb abszolút értékű maradékok):

pl. $\{-2, -1, 0, 1, 2\}$ TMR mod5, $\{-2, -1, 0, 1, 2, 3\}$ TMR mod6.

L **Lemma:**

$$H \subseteq \mathbb{Z} \text{ TMR mod } m \Leftrightarrow \begin{cases} |H| = m \\ \text{H elemei páronként inkongruensek} \end{cases}$$

(inkongruens = nem kongruens)

T Ha $\{t_1, t_2, \ldots, t_m\}$ TMR modulo m, és $(a, m) = 1$, $b \in Z$ tetszőleges, akkor $\{at_1 + b, at_2 + b, \ldots, at_m + b\}$ is TMR mod m.

B $at_i + b \equiv at_j + b \ (m) \iff at_i \equiv at_j \ (m) \overset{(a,m)=1}{\iff} t_i \equiv t_j \ (m)$ (mert $(a, m) = 1$) $\iff i = j$. Így ez is m darab inkongruens számból áll.

L $a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$

B $a - b = km \Rightarrow (a, m) = (b + km, m) = (b, m)$.

D Redukált maradékosztály modulo m: maradékosztály, amelynek elemei relatív prímek m-hez. (Ha egy elem relatív prím, akkor a lemma miatt az összes az.)

D **RMR**

Modulo m redukált maradékrendszernek (RMR) nevezzük egészek egy R halmazát, ha minden redukált maradékosztályból R pontosan egy elemet tartalmaz.

D **Euler-féle φ-függvény**

A redukált maradékosztályok számát $\varphi(m)$-mel jelöljük, és φ-t Euler-féle φ-függvénynek nevezzük.

- Másképpen: $\varphi(m)$ az $\{1, 2, \ldots, m\}$ halmazból az m-hez relatív prímek száma.

P $\{1, 5\}$ RMR mod 6 $\rightsquigarrow \varphi(6) = 2$.

P $\{1, 2, \ldots, p-1\}$ RMR mod p, ha p prím $\rightsquigarrow \varphi(p) = p - 1$ minden p prímre.

L $H \subseteq \mathbb{Z}$ RMR $\bmod m \Leftrightarrow \begin{cases} |H| = \varphi(m) \\ \text{H elemei páronként inkongruensek} \\ \text{H minden eleme relatív prím } m\text{-hez} \end{cases}$

T Ha $\{t_1, t_2, \ldots, t_m\}$ RMR modulo m, és $(a, m) = 1$, akkor $\{at_1, at_2, \ldots, at_m\}$ is RMR mod m.

B $\varphi(m)$ darab. ✓

$at_i \equiv at_j \ (m) \overset{(a,m)=1}{\iff} t_i \equiv t_j \ (m) \iff i = j.$

$(at_i, m) = (t_i, m) = 1$, mert $(a, m) = 1$.

Mj Nem adhatunk hozzá b-t, mint a TMR-nél, mert akkor nem maradnának relatív prímek m-hez. *(Van-e olyan eset, amikor mégis?)*

T A $\varphi : \mathbb{N}^+ \to \mathbb{N}^+$ számelméleti függvény multiplikatív, azaz $(m, n) = 1$ esetén $\varphi(mn) = \varphi(m)\varphi(n)$.

Mj Szükséges az $(m, n) = 1$ feltétel, pl.
$\varphi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6 \neq 2 \cdot 2 = \varphi(3) \cdot \varphi(3)$.

B Írjuk fel 1-től mn-ig a számokat egy táblázatba:

1	2	$\dots$	n
$n+1$	$n+2$	$\dots$	$2n$
$\vdots$	$\vdots$		$\vdots$
$(m-1)n+1$	$(m-1)n+2$	$\dots$	mn

Az első sor egy TMR $\bmod n$, és az alattuk levő számok velük kongruensek $\bmod n \rightsquigarrow$ pontosan $\varphi(m)$ oszlopnak az összes eleme relatív prím n-hez, a többi oszlop elemei nem.
Minden oszlop teljes TMR $\bmod m$ (mert $(m, n) = 1$) $\rightsquigarrow$ minden oszlopban pontosan $\varphi(m)$ elem relatív prím m-hez.
$\Rightarrow$ pontosan $\varphi(m)\varphi(n)$ elem van a táblázatban, amelyik m-hez és n-hez is rel. prím, azaz amely mn-hez rel. prím.

T **$\varphi(n)$ kanonikus alakja**

Ha $n \in \mathbb{N}^+$ kanonikus alakja $n = p_1^{a_1} \cdots p_r^{a_r}$, akkor

$$\varphi(n) = (p_1 - 1)p_1^{a_1-1} \cdots (p_r - 1)p_r^{a_r-1} = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

B $n = p^a$ prímhatványra a nem relatív prímek a p-vel oszthatók, így $\varphi(p^a) = p^a - \frac{p^a}{p} = p^a - p^{a-1} = (p-1)p^{a-1}$, tehát a φ multiplikativitása miatt

$$\varphi(n) = \varphi(p_1^{a_1}) \cdots \varphi(p_r^{a_r})$$

valóban a fenti formulával egyezik meg.Ha kiemeljük a tényezőkből $p_i^{a_i}$-t, akkor megkapjuk a második alakot.

P $\varphi(1200) = \varphi(2^4 3^1 5^2) = (2-1)2^3(3-1)(5-1)5^1 = 320.$

Euler–Fermat-tétel

T **Euler–Fermat-tétel**

Ha $m \in \mathbb{N}^+$, $a \in \mathbb{Z}$ és $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.

B Legyen $R_m = \{r_1, r_2, \ldots, r_{\varphi(m)}\}$ egy redukált maradékrendszer modulo m, és mivel $(a, m) = 1$, ezért $R'_m = \{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ is RMR modulo m.

$$r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)} \equiv (ar_1) \cdot (ar_2) \cdot \cdots \cdot (ar_{\varphi(m)}) \pmod{m},$$

egyszerűsítés után: $1 \equiv a^{\varphi(m)} \pmod{m}$.

K **Kis Fermat-tétel (első alak)**

Ha p prím, $a \in \mathbb{Z}$ és $p \nmid a$, akkor $a^{p-1} \equiv 1 \pmod{p}$.

B p prím $\rightsquigarrow$ $((a, p) = 1 \Leftrightarrow p \nmid a)$ és $\varphi(p) = p - 1$.

K **Kis Fermat-tétel (második alak)**

Ha p prím, akkor $a^p \equiv a \pmod{p}$.

K Ha $k \equiv \ell \pmod{\varphi(m)}$, $k, \ell \geq 0$, $(a, m) = 1 \Rightarrow a^k \equiv a^\ell \pmod{m}$

B Tfh. $k \geq \ell$. $k = \ell + q\varphi(m)$ $(q \geq 0)$. $\rightsquigarrow$
$a^k = a^\ell \cdot a^{q\varphi(m)} = a^\ell \cdot \left(a^{\varphi(m)}\right)^q \equiv a^\ell \cdot 1^q \equiv a^\ell \pmod{m}$.

K Köv.köv.: $(a, m) = 1$ esetén

$$a^n \equiv (a \bmod m)^{n \bmod \varphi(m)} \pmod{m}$$

m A moduláris hatványozás algoritmusához nincs szükség prímfaktorizálásra, de $\varphi(m)$ kiszámításához igen, amire nem ismerünk hatékony algoritmust.

P $18^{53} \bmod 13 = ?$

m $\varphi(13) = 12$ és $53 \equiv 5 \pmod{12} \rightsquigarrow 18^{53} \equiv 5^5 = 25 \cdot 25 \cdot 5 \equiv 5 \ (13)$

F $91^{89} \bmod 11 = ?$ a korábbinál egyszerűbben.

Kongruenciák

Lineáris kongruenciák

T **Lineáris kongruenciák megoldhatósága és a mo-k száma**

$a, b \in \mathbb{Z}$, $m \in \mathbb{N}^+$-re az $ax \equiv b \pmod{m}$ kongruencia pontosan akkor oldható meg, ha $(a, m) \mid b$. Ha megoldható, akkor pontosan (a, m) darab inkongruens megoldása van mod m.

B (Megoldhatóság) $ax \equiv b \pmod{m}$ megoldható $\iff$ $\exists y : ax + my = b \iff (a, m) \mid b$.

(Megoldások száma)

Ha $(a, m) = 1$, akkor a megoldás modulo m egyértelmű, ugyanis ekkor a kongruenciák egyszerűsítési szabálya szerint

$ax_1 \equiv ax_2 \pmod{m} \Rightarrow x_1 \equiv x_2 \pmod{m}$.

Ha $(a, m) = d \mid b$, akkor $ax \equiv b \pmod{m} \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$,

és az utóbbinak már egyértelmű a megoldása modulo $\mathbb{Z}_{m/d}$: x_0.

$\rightsquigarrow$ a megoldások modulo m: $x_0,\ x_0 + \frac{m}{d},\ \ldots,\ x_0 + (d-1) \cdot \frac{m}{d}$, vagyis d darab megoldás van.

P Oldjuk meg a $12x \equiv 15 \pmod{21}$ kongruenciát!

m A kongruencia megoldható, mert $(12, 21) = 3 \mid 15$.

x megoldás $\Leftrightarrow \exists y\colon\ 12x + 21y = 15$. A kongruenciát megoldhatjuk kibővített euklideszi algoritmussal. (Az y oszlopát nem is kell feltétlenül kitölteni.)

		12	21
	21	0	
-1	12	1	
-1	9	-1	
-3	3	2	

Jelentése:

$$\begin{aligned} 21 &\equiv 12 \cdot 0 \pmod{21} \\ 12 &\equiv 12 \cdot 1 \pmod{21} \\ 9 &\equiv 12 \cdot (-1) \pmod{21} \\ 3 &\equiv 12 \cdot 2 \pmod{21} \end{aligned}$$

$\rightsquigarrow 15 \equiv 12 \cdot 10 \pmod{21} \rightsquigarrow x_0 = 10$ megoldás, és ebből a $(12, 21) = 3$ darab különböző megoldás: $x \equiv 10, 17, 24 \pmod{21}$. ($\frac{m}{d} = \frac{21}{3} = 7$-eket kell hozzáadni az alapmegoldáshoz.)

m2 A kongruencia egyszerűsítésével:

$$\begin{aligned} 12x &\equiv 15 \pmod{21} \\ 4x &\equiv 5 \equiv 12 \pmod{7} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 3,\ 10,\ 17 \pmod{21} \end{aligned}$$

D Ha $a \in \mathbb{Z}$ és $(a, m) = 1$, akkor az $ax \equiv 1\ (m)$ kongruencia egy megoldását az *a elem moduláris inverzének* nevezzük mod m.

P Határozzuk meg az 5 moduláris inverzeit modulo 26.

m $(5, 26) = 1$, tehát az $5x \equiv 1\ (26)$ kongruencia megoldható.

$$\begin{aligned} 5x &\equiv 1 \equiv -25 \pmod{26} \\ x &\equiv -5 \pmod{26} \end{aligned}$$

tehát -5 egy inverze 5-nek modulo 26

(az összes: $x \equiv -5 \equiv 21\ (26)$, azaz $x = -5 + 26k$).

P Számítsuk ki még egyszerűbben a 91^{89} mod 11 értéket!

m $91 \equiv 3 \pmod{11}$, $\varphi(11) = 10$, így $91^{89} \equiv 3^{-1} \pmod{11}$, azaz a megoldás az az x, amelyre $3x \equiv 1 \equiv 12 \pmod{11}$, vagyis $x \equiv 4 \pmod{11}$

F $2^{67} \equiv ? \pmod{71}$

m $(2, 71) = 1$, $\varphi(71) = 70 \rightsquigarrow 2^{70} \equiv 1 \pmod{71} \rightsquigarrow 8 \cdot 2^{67} \equiv 1 \pmod{71}$

$8x \equiv 1 \equiv 72 \pmod{71} \Leftrightarrow x \equiv 9 \pmod{71}$

Tehát $2^{67} \equiv 9 \pmod{71}$.

T Ha $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$,..., $a \equiv b \pmod{m_n}$, ahol $a, b \in \mathbb{Z}$, $m_1, \ldots, m_n \in \mathbb{N}^+$, akkor

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_n]}.$$

B $m_1 \mid (a-b)$, $m_2 \mid (a-b)$,..., $m_n \mid (a-b) \rightsquigarrow$ $[m_1, m_2, \ldots, m_n] \mid (a-b)$.

P Oldjuk meg fejben a következő három kongruenciarendszert!

(a) $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, $x \equiv 1 \pmod{7}$

(b) $x \equiv 2 \pmod{3}$, $x \equiv 4 \pmod{5}$, $x \equiv 6 \pmod{7}$

(c) $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 4 \pmod{6}$

m *(a)* $x \equiv 1 \pmod{105}$ *(b)* $x \equiv -1 \pmod{105}$
(c) $x \equiv -2 \pmod{12}$

Kongruenciák

Kínai maradéktétel

T **Kínai maradéktétel**

Legyenek m_1, m_2,... m_n pozitív, páronként relatív prím egészek, és legyen $M = m_1 m_2 \dots m_n$. Az

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

kongruenciarendszer egyértelműen megoldható modulo M.

B Legyen $M_k = M/m_k = m_1 \dots m_{k-1} m_{k+1} \dots m_n$. Mivel $(M_k, m_k) = 1$, ezért az $M_k x_k \equiv 1 \ (m_k)$ kongruencia minden k-ra egyértelműen megoldható. Tekintsük az

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 + \ldots + a_n M_n x_n$$

összeget. Ez egyrészt megoldása mindegyik kongruenciának (mert $a_i M_i x_i \equiv a_i \cdot 1 \equiv a_i \ (m_i)$, de $a_k M_k x_k \equiv 0 \ (m_i)$, ha $k \neq i$, mert $M_k \equiv 0 \ (m_i)$). Másrészt, ha x' egy másik megoldás, akkor $x \equiv x'$ (m_k), azaz $m_k \mid (x - x') \ \forall k$, következésképp $M \mid (x - x')$, tehát a megoldás egyértelmű mod M.

P Oldjuk meg az

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

kongruenciarendszert!

m1 A bizonyítás alapján: $M = 165$, $M_1 = 55$, $M_2 = 33$, $M_3 = 15$,

$M_1 x_1 \equiv 1 \ (3) \rightsquigarrow 1x_1 \equiv 1 \ (3) \rightsquigarrow x_1 = 1$,
$M_2 x_2 \equiv 1 \ (5) \rightsquigarrow 3x_2 \equiv 1 \equiv 6 \ (5) \rightsquigarrow x_2 = 2$,
$M_3 x_3 \equiv 1 \ (11) \rightsquigarrow 4x_3 \equiv 1 \equiv 12 \ (11) \rightsquigarrow x_3 = 3$,

$x \equiv 55 \cdot 1 \cdot 2 + 33 \cdot 2 \cdot 3 + 15 \cdot 3 \cdot (-4) \equiv 110 + 198 - 180 \equiv 128 \ (165)$.

A megoldás $x \equiv 128 \pmod{165}$.

Egy táblázatba összefoglalva:

m_i	3	5	11
M_i	55	33	15
x_i	1	2	3
a_i	2	3	-4
	110	198	-180

$$\rightsquigarrow x \equiv 110 + 198 - 180 \equiv 128 \pmod{165}$$

ahol x_i az M_i inverze modulo m_i azaz az $M_i x_i \equiv 1 \ (m_i)$ kongruencia megoldása.

m2

$$\begin{aligned} x &\equiv 2 \ (3) \\ x &= 2 + 3y \end{aligned}$$

$$\begin{aligned} x &\equiv 3 \ (5) \\ 2 + 3y &\equiv 3 \ (5) \\ 3y &\equiv 1 \equiv 6 \ (5) \\ y &\equiv 2 \ (5) \\ y &= 2 + 5z \\ x &= 8 + 15z \end{aligned}$$

$$\begin{aligned} x &\equiv -4 \ (11) \\ 8 + 15z &\equiv -4 \ (11) \\ 4z &\equiv -12 \ (11) \\ z &\equiv -3 \ (11) \\ z &= -3 + 11u \\ x &= -37 + 165u \\ x &\equiv -37 \equiv 128 \ (165) \end{aligned}$$

P Oldjuk meg a $6x \equiv 4 \ (20)$, $3x \equiv -2 \ (13)$ kongruenciarendszert.

m Először megoldjuk az egyes kongruenciákat, aztán egyesítjük a megoldásokat a kínai maradéktétel módszerével.

$6x \equiv 4 \ (20) \ \Leftrightarrow \ 3x \equiv 2 \ (10) \ \Leftrightarrow \ 3x \equiv 12 \ (10) \ \Leftrightarrow \ x \equiv 4 \ (10)$

$3x \equiv -2 \ (13) \ \Leftrightarrow \ 3x \equiv -15 \ (13) \Leftrightarrow x \equiv -5 \ (13)$

m_i	10	13
M_i	13	10
x_i	7	4
a_i	4	-5
	364	-200

$\rightsquigarrow x \equiv 364 - 200 \equiv 164 \equiv 34 \pmod{130}$

Mj Nem relatív prím modulusú lineáris kongruenciarendszereknek pontosan akkor van megoldása, ha a kongruenciák közül bármely kettőnek van közös megoldása.

Kongruenciák

Néhány egyszerű alkalmazás

Oszthatósági szabályok

- 2-hatvány: $(a_n \dots a_1 a_0)_{10} \equiv (a_{k-1} \dots a_1 a_0)_{10} \pmod{2^k}$,
  mert $2^k \mid 10^\ell$, ha $\ell \geq k$. (Tehát a 2-vel való oszthatóságot az utolsó jegy, 4-gyel való oszthatóságot az utolsó két jegy, stb. dönti el. Hasonlóan az 5-re és 5-hatványokra.
- 9: $(a_n \dots a_1 a_0)_{10} \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \pmod 9$,
  mert $10^k \equiv 1^k \equiv 1 \pmod 9$
- 11: $(a_n \dots a_1 a_0)_{10} \equiv a_0 - a_1 + a_2 - \dots + (-1)^n a_n \pmod{11}$,
  mert $10^k \equiv (-1)^k \pmod{11}$.

Ellenőrző számjegy

A magyar személyi szám 11-jegyű, az utolsó az ellenőrző számjegy:
$x_{11} \equiv x_1 + 2x_2 + 3x_3 + \dots + 10x_{10} \pmod{11}$.
Ez jelzi, ha elírnak egyetlen számjegyet vagy ha kettőt felcserélnek (kivéve, ha a két utolsót). Ezért újabb személyi számoknál már az $x_{11} \equiv 10x_1 + 9x_2 + 8x_3 + \dots + x_{10} \pmod{11}$ képletet használják (inkább közeli számjegyek felcserélése valószínű).

Kongruenciák

Maradékosztályok gyűrűje

- Két egész szám összegének, különbségének, szorzatának maradéka modulo m csak attól függ, hogy a tényezők melyik maradékosztályba tartoznak.

D Legyen $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ és definiáljuk a $\langle \mathbb{Z}_m, \oplus, \otimes \rangle$ struktúrát a következőképp: ha $a, b \in \mathbb{Z}_m$, akkor $a \oplus b := a + b \bmod m$, $a \otimes b := a \cdot b \bmod m$.

P Írjuk fel $\mathbb{Z}_2$ művelettábláit:

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

- A továbbiakban – ha félreértést nem okoz – $\mathbb{Z}_n$ alatt a $\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ algebrai struktúrát értjük, amelynek műveleteire is inkább a '$+$' és '$\cdot$' jeleket használjuk, azaz $\mathbb{Z}_n = \langle \mathbb{Z}_n, +, \cdot \rangle$.

P $\mathbb{Z}_{11}$-ben $6 + 8 = 3$ és $6 \cdot 8 = 4$.

D **Definíció**

Legyen egy R halmazon értelmezve két kétváltozós művelet: $+$ és $\cdot$ ($a \cdot b = ab$ egyszerűbben írva).

R gyűrű, ha teljesülnek rá a következő axiómák:

(A1) $(a+b)+c = a+(b+c) \quad \forall a,b,c \in R$ ($+$ asszociatív)

(A2) $a+b = b+a \quad \forall a,b \in R$ ($+$ kommutatív)

(A3) $\exists 0 \in R$: $0+a = a+0 = a \quad \forall a \in R$ ($\exists$ additív neutrális elem)

(A4) $\forall a \in R\ \exists(-a) \in R$: $a+(-a) = (-a)+a = 0$ ($\exists$ additív inverz)

(M1) $(ab)c = a(bc) \quad \forall a,b,c \in R$ ($\cdot$ asszociatív)

(D) $(a+b)c = ac+bc$ és $c(a+b) = ca+cb\ \forall a,b,c$ (disztributivitás)

D R kommutatív gyűrű, ha gyűrű és

(M2) $ab = ba \quad \forall a,b \in R$ ($\cdot$ kommutatív)

D R egységelemes gyűrű, ha gyűrű, és

(M3) $\exists 1 \in R$: $1a = a1 = a \quad \forall a \in R$ ($\exists$ multiplikatív neutrális elem)

P $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ egységelemes kommutatív gyűrűk. $2\mathbb{Z}$ kommutatív gyűrű, de nem egységelemes. $\mathbb{N}$ nem gyűrű, mert nincs benne additív inverz.

Mj A gyűrűaxiómákból következik, hogy $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in R$.

D **Definíció**

K test, ha egységelemes kommutatív gyűrű, $|K| \geq 2$, és
(M4) $\forall 0 \neq a \in K \quad \exists a^{-1}\colon \quad aa^{-1} = a^{-1}a = 1$ ($\exists$ multiplikatív inverz)

Mj Minden test nullosztómentes, azaz $ab = 0 \Rightarrow a = 0$ vagy $b = 0$, mert ha pl $a \neq 0$, akkor $0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$.

D Ha K test: $a - b := a + (-b)$ és $\frac{a}{b} := a(b^{-1})$.

P $\mathbb{R}$, $\mathbb{Q}$ test, de $\mathbb{Z}$ nem.

T $\mathbb{Z}_m$ egységelemes kommutatív gyűrű minden m-re.

B $\mathbb{Z}$-ben teljesülnek az axiómák, és ez öröklődik a modulo m végzett műveletekre is a kongruenciák műveleti tulajdonságai miatt. Pl.
$((a+b) \bmod m) + c) \bmod m \equiv ((a+b) \bmod m) + c \equiv (a+b) + c = a + (b+c) \equiv a + ((b+c) \bmod m) \equiv (a + ((b+c) \bmod m)) \bmod m.$

T $\mathbb{Z}_p$ test, ha p prím.

B Ha $0 \neq a \in \mathbb{Z}_p$, akkor $(a, p) = 1$, ezért létezik inverze modulo p, azaz van olyan $b \in \mathbb{Z}_p$, amelyre $ab \equiv 1 \pmod{m}$ a $\mathbb{Z}$-ben, azaz $ab = 1$ $\mathbb{Z}_p$-ben. (Ha p nem prím, akkor $\mathbb{Z}_p$ még csak nem is nullosztómentes.)

P Írjuk fel $\mathbb{Z}_5$ és $\mathbb{Z}_6$ művelettábláit:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Mj $\mathbb{Z}_m$-et tekinthetjük úgy is, hogy a modulo m maradékosztályok halmaza, amelyen természetes módon vannak értelmezve a műveletek, és ezeket a maradékosztályokat egy-egy elemükkel reprezentáljuk. Ilyen értelemben bármely egész szám jelölheti a $\mathbb{Z}_m$ egy elemét, csak az egy osztályba esőket egyenlőknek tekintjük. Pl. $\mathbb{Z}_5$-ben $8 = 3 = -2$.

D $\mathbb{Z}_m^*$ a redukált maradékosztályok halmaza modulo m, amelyen a szorzás művelete értelmezve van, de az összeadás nem.

Mj Z_m^*-on a szorzás asszociatív, kommutatív, van egységelem, sőt minden elemének van multiplikatív inverze, azaz $\mathbb{Z}_m^*$ csoport.

P Írjuk fel $\mathbb{Z}_6^*$ és $\mathbb{Z}_9^*$ szorzástábláját!

m

$\cdot$	1	5
1	1	5
5	5	1

$\cdot$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1