

Elsfokú kongruenciák és kongruencia rendszerek

Az elsőfokú kongruenciák megoldása nem állítja az olvasót leküzdhetetlen feladat elé, hiszen az visszavezethet a már megismert eljárásra, amellyel lineáris diofantoszi egyenleteket oldottunk meg. A kínai maradéktétel a szimultán kongruenciák megoldására ad eljárást, melynek legfontosabb gyakorlati alkalmazása a nagy számokon elvégzend aritmetika számítógépes megvalósítása.

Különböz modulusok

Ebben a fejezetben azt vizsgáljuk, hogy milyen kapcsolat áll fenn különböző modulusú kongruenciák között? Az $a \equiv_m b$ kongruencia definíció szerint akkor és csak akkor teljesül, ha $m \mid b - a$. Ebből azonnal látható, hogy a modulus minden d osztója is osztja $(b - a)$ -t. Ez pedig ismét csak a definíció szerint azt jelenti, hogy a és b modulo d is kongruens.

Példák

1. $22 \equiv_8 46$. Mivel $4 \mid 8$, ezért $22 \equiv_4 46$. Még könnyebben látható a $22 \equiv_2 46$ kongruencia, hiszen 22 és 46 is páros.

2. $13 \equiv_{18} 67$. Mivel 2, 3 és 9 osztója 18-nak, ezért a $13 \equiv_2 67$, $13 \equiv_3 67$, $13 \equiv_9 67$ kongruenciák mindegyike teljesül.

3. A 72 prímtényezős felbontása $72 = 2^3 \cdot 3^2$. Így $2^3 = 8 \mid 72$ és $3^2 = 9 \mid 72$. Ekkor tetszőleges a és b egészekre az $a \equiv_{72} b$ kongruenciából az $a \equiv_8 b$ és az $a \equiv_9 b$ kongruenciák egyidejű teljesülése következik.

Írjuk most fel egymás mellé a modulo 6 és a modulo 3 maradékosztályokat. Ha elég ügyesen rendezzük el adatainkat, akkor azonnal látható az, amit látni szeretnénk. A modulo 6 maradékosztályok mindegyike valamelyik modulo 3 maradékosztály részhalmaza.

modulo 6 maradékosztályok		modulo 3 maradékosztályok	
$0 + 6 \cdot k$	..., -12, -6, 0, 6, 12, 18, 24,...	$0 + 3 \cdot k$	..., -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, 18,...
$3 + 6 \cdot k$	..., -9, -3, 3, 9, 15, 21, 27,...		
$1 + 6 \cdot k$	..., -11, -5, 1, 7, 13, 19, 25,...	$1 + 3 \cdot k$	..., -11, -8, -5, -2, 1, 4, 7, 10, 13, 16, 19,...
$4 + 6 \cdot k$	..., -8, -2, 4, 10, 16, 22, 28,...		
$2 + 6 \cdot k$	..., -10, -4, 2, 8, 14, 20, 26,...	$2 + 3 \cdot k$	..., -10, -7, -4, -1, 2, 5, 8, 11, 15, 17, 21,...

$5 + 6 \cdot k$	$\dots, -7, -1, 5, 11, 17, 23, 29, \dots$		
-----------------	---	--	--

Nem lesz nehéz meggyzni magunkat arról, hogy a fenti tapasztalat nemcsak a 6 és 3 modulusokra, hanem tetszleges m modulusra és az m tetszleges d osztójára is teljesül. Ugyanis egy modulo m maradékosztályba az m -mel kongruens egészek tartoznak. Ha tehát egy maradékosztályban az a egész elfordul, akkor abba a maradékosztályba az összes olyan b egész is bele tartozik, amelyre $a \equiv_m b$. Ám ekkor $d \mid m$ miatt $a \equiv_d b$ is teljesül, ami viszont azt vonja maga után, hogy a és b azonos modulo d maradékosztályba tartozik. Eszerint az a egészet tartalmazó modulo m maradékosztály minden eleme egyben eleme az a -t tartalmazó modulo d maradékosztálynak is. Ezzel beláttuk, hogy az m modulus bármely d osztójára a modulo m maradékosztályok a modulo d maradékosztályok részhalmazai.

Két egész szám legkisebb közös többszörösének mindkét szám osztója. Így az eddig elmondottak szerint az

$$a \equiv_{\text{lkk}(m, n)} b$$

kongruenciából az

$$a \equiv_m b \text{ és } a \equiv_n b$$

kongruenciák egyidej teljesülése következik. Ám ennél több is igaz, mint ahogy azt a következ tétel mutatja.

▼ 13.1.1. Tétel

Az $a \equiv_m b$ és $a \equiv_n b$ kongruenciák egyidej teljesülésének szükséges és elégséges feltétele az $a \equiv_{\text{lkk}(m, n)} b$ kongruencia teljesülése.

Bizonyítás

Az elégségesség teljesülését már láttuk. A szükségesség bizonyításához tegyük fel, hogy $a \equiv_m b$ és $a \equiv_n b$. Ekkor

$$m, n \mid b - a.$$

Itt emlékeztetünk arra a tényre, hogy egy egész szám két osztójának legkisebb közös többszöröse is osztja a számot (ld. 9.11 tétel). Eszerint

$$\text{lkk}(m, n) \mid b - a,$$

és ezzel nyertük az $a \equiv_{\text{lkk}(m, n)} b$ kongruencia teljesülését.

Példák

1. $26 \equiv_4 38$ és $26 \equiv_6 38$ (kéretik ellenrizni). Mivel $\text{lkk}(4, 6) = 12$, így $26 \equiv_{12} 38$.

2. $105 \equiv_3 321$ és $105 \equiv_8 321$. Mivel $\text{lkk}(3, 8) = 3 \cdot 8 = 24$, így $105 \equiv_{24} 321$.

Ha a vizsgált modulusok relatív prímek, akkor legnagyobb közös osztójuk egyenl a szorzatukkal.

Így az elz tétel közvetlen következményeként adódik, hogy

▼ 13.1.2. Tétel

Ha $\text{luko}(m, n) = 1$, akkor

Az $a \equiv_m b$ és $a \equiv_n b$ kongruenciák egyidej teljesülésének szükséges és elégséges feltétele az $a \equiv_{m \cdot n} b$ kongruencia teljesülése.

▼ Egyismeretlenes elsőfokú kongruenciák

Ebben a fejezetben a lineáris egyismeretlenes kongruencia megoldhatóságával foglalkozunk.

▼ 13.2.1. Definíció

Az

$$a \cdot x \equiv_m b$$

kongruenciát **egyismeretlenes elsőfokú kongruenciának** nevezzük. A kongruencia megoldásán olyan c egész számot értünk, amelyre

$$a \cdot c \equiv_m b.$$

A kongruencia megoldásait modulo m keressük, tehát nem tekintjük különbözőnek azokat a megoldásokat, amelyek ugyanazon modulo m maradékosztályba esnek. Nézzünk rögtön egy példát! Tekintsük a

$$4 \cdot x \equiv_{10} 10$$

kongruenciát. Ez a kongruencia definíciója szerint akkor és csak akkor teljesül, ha $6 \mid 10 - 4 \cdot x$, vagyis ha alkalmas y egészre $10 - 4 \cdot x = 6 \cdot y$, amit átrendezve a

$$4 \cdot x + 6 \cdot y = 10$$

diofantoszi egyenlethez jutunk. Kaptuk tehát, hogy a $4 \cdot x \equiv_{10} 10$ kongruencia akkor és csak akkor oldható meg, ha a $4 \cdot x + 6 \cdot y = 10$ diofantoszi egyenlet megoldható. Ez utóbbira viszont már tudjuk a választ, és ez biztató. Gondolatmenetünk általánosan is érvényes, így kimondhatjuk a következő tételt.

▼ 13.2.2. Tétel

Az x egész szám akkor és csak akkor megoldása az

$$a \cdot x \equiv_m b$$

elsőfokú egyismeretlenes kongruenciának, ha létezik olyan y egész szám, amelyre x és y megoldása az

$$a \cdot x + m \cdot y = b$$

diofantoszi egyenletnek.

Bizonyítás

Tegyük fel, hogy x_0 kielégíti az $a \cdot x \equiv_m b$ kongruenciát. Ekkor $a \cdot x_0 \equiv_m b$, így a kongruencia definíciója szerint $m \mid b - a \cdot x_0$, ami viszont akkor és csak akkor teljesül, ha alkalmas y_0 egészre $b - a \cdot x_0 = m \cdot y_0$. Ebből átrendezéssel nyerjük az $a \cdot x_0 + m \cdot y_0 = b$ egyenlőséget, ami pontosan azt fejezi ki, hogy x_0 és y_0 megoldása az $a \cdot x + m \cdot y = b$ diofantoszi egyenletnek.

Fordítva tegyük fel, hogy x_0 és y_0 megoldása az $a \cdot x + m \cdot y = b$ diofantoszi egyenletnek. Ekkor $a \cdot x_0 + m \cdot y_0 = b$, amiből átrendezéssel $m \cdot y_0 = b - a \cdot x_0$. Ez pedig nem más jelent mint azt, hogy $m \mid b - a \cdot x_0$, tehát $a \cdot x_0 \equiv_m b$. Így x_0 megoldása az $a \cdot x \equiv_m b$ kongruenciának.

Tételünk biztosítja, hogy az $a \cdot x \equiv_m b$ kongruencia helyett elegendő megoldani az $a \cdot x + m \cdot y = b$ diofantoszi egyenletet. Fejezzük hát be a

$$4 \cdot x \equiv_6 10$$

kongruencia vizsgálatát!

Els lépésként felírjuk a kongruenciához tartozó

$$4 \cdot x + 6 \cdot y = 10$$

diofantoszi egyenletet, melynek van megoldása, hiszen $\text{luko}(4, 6) = 2 \mid 10$. A diofantoszi egyenlet általános megoldására már van számolási sémánk.

Osztandó	Osztó	Maradék	
4	6	4	
6	4	2	
4	2	0	
$\text{luko}(a, b) = 2, \frac{c}{\text{luko}(a, b)} = \frac{10}{2} = 5$			Partik
$\frac{b}{\text{luko}(a, b)} = 3$			Által

Eltűnk áll tehát a kongruencia összes megoldása. Fel kell azonban tennünk a kérdést, hogy az $x = -5 + 3 \cdot t$ egészek a t paraméter különböző értékeire milyen maradékosztályokba esnek? Vagy másként, hány modulo 6 inkongruens szám van az $x = -5 + 3 \cdot t$ számok között? Az nyilvánvaló, hogy az összes $-5 + 3 \cdot t$ alakú egész ugyanabba a modulo 3 maradékosztályba tartozik, hiszen ezek a számok 3 többszörösében térnek el egymástól. Eszerint a $4 \cdot x \equiv_6 10$ kongruencia megoldása egyértelműen meghatározott modulo 3. Ugyanakkor ezek között a számok között vannak inkongruensek modulo 6.

Például a $t = 0$ és a $t = 1$ értékekhez tartozó megoldások inkongruensek, ugyanis

$$-5 + 3 \cdot 0 = -5,$$

$$-5 + 3 \cdot 1 = -2,$$

és

$$-5 \not\equiv_6 -2.$$

Ám t paraméter 2 és 3 értékeire 1 és 4 adódik, amelyekre már $1 \equiv_6 -5$ és $4 \equiv_6 -2$ teljesül.

Példák

Soroljuk fel az $-5 + 3 \cdot t$ számokat a t paraméter $-5, -4, \dots, 4, 5$ értékeire. A második utasítás azt mutatja, hogy a kapott számok mindegyike 4-gyel vagy 1-gyel kongruens modulo 6.

$$\left[\begin{array}{ll} > \text{seq}(-5+3*t, t=-5..5); \\ & -20, -17, -14, -11, -8, -5, -2, 1, 4, 7, 10 \end{array} \right. \quad (1.2.1)$$

$$\left[\begin{array}{ll} > \text{seq}(-5+3*t \bmod 6, t=-5..5); \\ & 4, 1, 4, 1, 4, 1, 4, 1, 4, 1, 4 \end{array} \right. \quad (1.2.2)$$

További próbálkozásaink sem adnak új inkongruens értéket, ami nem véletlen. Érvényes ugyanis a

13.2.3. Tétel

1. Az $a \cdot x \equiv_m b$ kongruenciának akkor és csak akkor van megoldása, ha $\text{lnko}(a, m) \mid b$.
2. Ha az $a \cdot x \equiv_m b$ kongruenciának létezik megoldása, akkor a modulo m megoldások száma $d = \text{lnko}(a, m)$. Ezek

$$x_0, x_0 + \frac{m}{d}, x_0 + 2 \cdot \frac{m}{d}, \dots, x_0 + (d-1) \cdot \frac{m}{d},$$

ahol x_0 a kongruencia egy megoldása.

Bizonyítás

Az els állítás a 10.7 tétel közvetlen következménye.

A 10.8 tétel szerint az $a \cdot x + m \cdot y = b$ diofantoszi egyenlet általános megoldása $x = x_0 + \frac{m}{d} \cdot t$. A 12.5 tétel pedig biztosítja, hogy ezek a számok egyben megoldásai az $a \cdot x \equiv_m b$ kongruenciának. Elegendő tehát megmutatni, hogy a

$$x_0, x_0 + \frac{m}{d}, x_0 + 2 \cdot \frac{m}{d}, \dots, x_0 + (d-1) \cdot \frac{m}{d}$$

számok páronként inkongruensek modulo m .

Legyen $0 \leq i < j \leq d-1$, és tegyük fel, hogy állításunkkal ellentétben

$$x_0 + i \cdot \frac{m}{d} \equiv_m x_0 + j \cdot \frac{m}{d}.$$

Átrendezés után azt kapjuk, hogy

$$(i-j) \cdot \frac{m}{d} \equiv_m 0.$$

Ez pedig lehetetlen, mert $0 < (i-j) \cdot \frac{m}{d} < m$.

Végül ha az $x = x_0 + \frac{m}{d} \cdot t$ kifejezésben $t \equiv_d i$ valamely $0 \leq i \leq d-1$ egészre, akkor alkalmas q egészre

$$d \cdot q = t - i,$$

amiből $\frac{m}{d}$ -vel való szorzás után

$$m \cdot q = \frac{m}{d} \cdot (t - i) = \frac{m}{d} \cdot t - \frac{m}{d} \cdot i,$$

és így

$$\frac{m}{d} \cdot t \equiv_m \frac{m}{d} \cdot i.$$

Am ekkor

$$x_0 + \frac{m}{d} \cdot t \equiv_m x_0 + \frac{m}{d} \cdot i.$$

Ezzel megmutattuk, hogy minden megoldás az $x_0, x_0 + \frac{m}{d}, x_0 + 2 \cdot \frac{m}{d}, \dots, x_0 + (d-1) \cdot \frac{m}{d}$ számok közül valamelyikkel kongruens.

13.2.4. Algoritmus: Lineáris kongruencia megoldása

Szöveges leírás	Maple metakód
1. <u>Input</u>: a, b, m ($a \cdot x \equiv_m b$) 2. $z := \text{Diofantosz}(a, m, b)$ 3. $d := z_1$: 4. Ha d osztója b Akkor $x_0 = z_2 \cdot \frac{b}{d}$: Legyen $s := [$ $x_0, x_0 + \frac{m}{d}, \dots, x_0 + \left(d-1\right) \frac{m}{d}]$ Különben Legyen $s := []$ # nincs megoldás 4. <u>Output</u>: s a megoldások listája	<u>Input</u>: a, b, m ($a \cdot x \equiv_m b$) $z := \text{Diofantosz}(a, m, b)$: $d := z_1$: if $\text{irem}(b, d) = 0$ then $x_0 = z_2 \cdot \frac{b}{d}$: return $[seq(x_0 + i * m / d \bmod m, i = 0$ $..z[1]-1)]$ else return $[]$ fi <u>Output</u>: A megoldások listája

13.2.5. Maple implementáció

```
> restart;
```

```
[ > with(ant):
```

"Az ANT (Algorithmic Number Theory) csomag üdvözli Önt!" (1.2.5.1)

A **Linkongr** eljárás három paramétere rendre a megoldandó kongruenciában az x együtthatója, a szabad tag és a modulus. Az **equ** opcióval az eljárás megmutatja a megoldandó kongruenciát és a vele ekvivalens diofantoszi egyenletet.

```
[ > Linkongr(4, 10, 6, equ);
```

A megoldandó kongruencia(Linkongr):
 $4x = 10 \bmod 6$

A megoldandó egyenlet(Diofantosz):
 $4x + 6y = 10$

Eredmény(Linkongr):
 $[-5, -2]$ (1.2.5.2)

Ahogy azt az **ant** csomag egyéb eljárásainál már megszokhattuk, a **cal** opcióval a számítás további részletei ttnnek el.

```
[ > Linkongr(4, 10, 6, equ, cal);
```

A megoldandó kongruencia(Linkongr):
 $4x = 10 \bmod 6$

A megoldandó egyenlet(Diofantosz):
 $4x + 6y = 10$

Részletek megjelenítése(Diofantosz):
 $\left[\left[\text{osztandó, osztó, maradék, hányados, } x, y \right], \right.$

$\left[4, 6, 4, 0, -1, 1 \right],$

$\left[6, 4, 2, 1, 1, -1 \right],$

$\left[4, 2, 0, 2, 0, 1 \right],$

$\left[, \text{Inko}(a, b) = 2, \frac{c}{\text{Inko}(a, b)} = 5, \text{Partikuláris megoldás:}, -5, 5 \right],$

$\left[, \frac{b}{\text{Inko}(a, b)} = 3, \frac{a}{\text{Inko}(a, b)} = 2, \text{Általános megoldás:}, -5 + 3t, 5 - 2t \right.$

$\left. \right]$

Eredmény(Diofantosz):
 $[x = -5 + 3t, y = 5 - 2t]$

Inkongruens megoldások(Linkongr):
 $[-5 + 3t, t = 0..1]$

Eredmény(Linkongr):
 $[-5, -2]$ (1.2.5.3)

> Linkongr(412, 10012, 612, equ, cal);

A megoldandó kongruencia(Linkongr):

$$412x = 10012 \bmod 612$$

A megoldandó egyenlet(Diofantosz):

$$412x + 612y = 10012$$

Részletek megjelenítése(Diofantosz):

$\left[\left[\text{osztandó, osztó, maradék, hányados, } x, y \right], \right.$

$\left[412, 612, 412, 0, 52, -35 \right],$

$\left[612, 412, 200, 1, -35, 52 \right],$

$\left[412, 200, 12, 2, 17, -35 \right],$

$\left[200, 12, 8, 16, -1, 17 \right],$

$\left[12, 8, 4, 1, 1, -1 \right],$

$\left[8, 4, 0, 2, 0, 1 \right],$

$\left[, \text{Inko}(a, b) = 4, \frac{c}{\text{Inko}(a, b)} = 2503, \text{Partikuláris megoldás:}, 130156, \right.$
 $\left. -87605 \right],$

$\left[, \frac{b}{\text{Inko}(a, b)} = 153, \frac{a}{\text{Inko}(a, b)} = 103, \text{Általános megoldás:}, 130156 \right.$
 $\left. + 153t, -87605 - 103t \right]$

Eredmény(Diofantosz):

$$[x = 130156 + 153t, y = -87605 - 103t]$$

Inkongruens megoldások(Linkongr):

$$[130156 + 153t, t = 0 \dots 3]$$

Eredmény(Linkongr):

$$[130156, 130309, 130462, 130615]$$

(1.2.5.4)

>

▼ Kínai maradéktétel

A alábbi feladatot Szun-ce, a negyedik században él kínai gondolkodó vetette fel, és megoldást is adott rá .

"Bizonyos dolgok számát nem ismerjük. Ha elosztjuk 3-mal, a maradék 2, ha 5-tel osztunk, a maradék 3, ha pedig 7-tel, a maradék 2. Mennyi a keresett szám?"

Mi szemléltetési megfontolásokból kissé módosított feladatot oldunk meg. A 7-tel való osztás maradékát 2-ről 4-re változtatjuk.

Az a tény, hogy a keresett szám, melyet jelöljünk x -szel, 3-mal osztva 2 maradékot ad, a kongruenciák segítségével úgy fejezhet ki, hogy $x \equiv_3 2$. Ugyanígy, a másik két feltétel is felírható kongruenciákkal, és így végeredményben az alábbi lineáris kongruenciarendszerhez jutunk

$$x \equiv_3 2$$

$$x \equiv_5 3$$

$$x \equiv_7 4.$$

A megoldás alapgondolata az, hogy keressük az x -et a kongruenciák jobb oldalán szereplő konstansok, vagyis a 2, 3 és 4 lineáris kombinációjaként. Vagyis azt kérdezzük, hogy tudjuk-e úgy választani az x_1 , x_2 és x_3 egészeket, hogy az

$$x = 2 \cdot x_1 + 3 \cdot x_2 + 4 \cdot x_3$$

egész szám megoldása legyen egyidejleg mindhárom kongruenciának? Az x_1 , x_2 és x_3 egészekre vonatkozó elvárásaink az alábbi kongruenciákban öltének testet

$$2 \cdot x_1 + 3 \cdot x_2 + 4 \cdot x_3 \equiv_3 2$$

$$2 \cdot x_1 + 3 \cdot x_2 + 4 \cdot x_3 \equiv_5 3$$

$$2 \cdot x_1 + 3 \cdot x_2 + 4 \cdot x_3 \equiv_7 4.$$

Elégké kézenfekvőnek látszik a gondolat, hogy ha az első kongruenciában x_1 -et 1-re, a másik két ismeretlent pedig nullára állítjuk, akkor az első kongruencia teljesül. Igen ám de, ez a gondolat a második kongruencia esetében x_1 -re nullát követelne meg. Ez így sajnos nem működik. Ám vegyük észre, hogy az első kongruencia teljesüléséhez elegendő azt megkövetelni, hogy

$$x_1 \equiv_3 1, \quad x_2 \equiv_3 0, \quad x_3 \equiv_3 0$$

fenn álljon. Megismételve ezt a második és harmadik kongruenciára, az alábbi kongruenciákhoz jutunk:

$$x_1 \equiv_3 1$$

$$x_2 \equiv_3 0$$

$$x_3 \equiv_3 0$$

$$x_1 \equiv_5 0$$

$$x_2 \equiv_5 1$$

$$x_3 \equiv_5 0$$

$$x_1 \equiv_7 0$$

$$x_2 \equiv_7 0$$

$$x_3 \equiv_7 1$$

Vegyük észre, hogy az első oszlopban az $x_1 \equiv_5 0$, és $x_1 \equiv_7 0$ kongruenciák, az

$$x_1 \equiv_{5 \cdot 7} 0$$

kongruenciával helyettesíthetők (ld. 12.4 tétel). Ennek fényében a fenti kongruenciák

$$x_1 \equiv_3 1$$

$$x_2 \equiv_5 1$$

$$x_3 \equiv_7 1$$

$$x_1 \equiv_{5 \cdot 7} 0$$

$$x_2 \equiv_{3 \cdot 7} 0$$

$$x_3 \equiv_{3 \cdot 5} 0$$

alakba írhatók. És most már abban szerencsés helyzetben vagyunk, hogy ezeket a konruenciarendszereket meg tudjuk oldani.

Megoldandó	$x_1 \equiv_3 1$ $x_1 \equiv_{5 \cdot 7} 0$	$x_2 \equiv_5 1$ $x_2 \equiv_{3 \cdot 7} 0$	$x_3 \equiv_7 1$ $x_3 \equiv_{3 \cdot 5} 0$
Megoldás lépései	A második kongruencia miatt $x_1 \mid 5 \cdot 7$ $x_1 = 5 \cdot 7 \cdot y_1.$ Ezt az els kongruenciába helyettesítve a $5 \cdot 7 \cdot y_1 \equiv_3 1$ kongruenciához jutunk, mely megoldható, mert $\text{luko}(5 \cdot 7, 3) = 1.$ A megoldás $y_1 \equiv_3 2,$ amiből $x_1 \equiv_3 (5 \cdot 7) \cdot 2 = 70.$	Mivel $x_2 \mid 3 \cdot 7$, ezért $x_2 = 3 \cdot 7 \cdot y_2.$ Ezt az els kongruenciába helyettesítve a $3 \cdot 7 \cdot y_2 \equiv_5 1$ kongruenciához jutunk, mely megoldható, mert $\text{luko}(3 \cdot 7, 5) = 1.$ A megoldás $y_2 \equiv_5 1,$ amiből $x_2 \equiv_5 (3 \cdot 7) \cdot 1 = 21.$	Mivel $x_3 \mid 3 \cdot 5$, ezért $x_3 = 3 \cdot 5 \cdot y_3.$ Ezt az els kongruenciába helyettesítve a $3 \cdot 5 \cdot y_3 \equiv 1 \pmod{7}$ kongruenciához jutunk, mely megoldható, mert $\text{luko}(3 \cdot 5, 7) = 1.$ A megoldás $y_3 \equiv_7 1,$ amiből $x_3 \equiv_7 (3 \cdot 5) \cdot 1 = 15.$
Ellenrész	$70 \equiv_3 1, 70 \equiv_{5 \cdot 7} 0$	$21 \equiv_5 1, 21 \equiv_{3 \cdot 7} 0$	$15 \equiv_7 1 \pmod{7}, 15 \equiv_{3 \cdot 5} 0$

Talán már el is felejtettük, hogy mi célból vezettük be az x_1 , x_2 és x_3 egészeket. k voltak az együtthatói annak az lineáris kombinációnak, amellyel x -et, a kiindulási kongruenciarendszer megoldását akartuk előállítani. Mivel x_1 , x_2 és x_3 értékei már ismertjük, magát x -et is előállíthatjuk

$$x = 2 \cdot x_1 + 3 \cdot x_2 + 4 \cdot x_3 = 2 \cdot 70 + 3 \cdot 21 + 4 \cdot 15 = 263.$$

És végül az ellenrész. A kapott eredmény valóban megoldása a kiindulási kongruenciarendszernek:

$$263 \equiv_3 2, \text{ mert } 3 \text{ osztója } 263 - 2 = 261\text{-nek,}$$

$$263 \equiv_5 3, \text{ mert } 5 \text{ osztója } 263 - 3 = 260\text{-nak,}$$

$$263 \equiv_7 4, \text{ mert } 7 \text{ osztója } 263 - 4 = 259\text{-nek.}$$

Foglaljuk össze, hogy mit is csináltunk!

1. Az

$$x \equiv_3 2 \quad x \equiv_5 3 \quad x \equiv_7 4$$

kongruenciarendszer megoldását a jobboldali konstansok egy lineáris kombinációjaként kerestük:

$$x = 2 \cdot x_1 + 3 \cdot x_2 + 4 \cdot x_3.$$

2. Rámutattunk, hogy ha

x_1 -et az

$$x_1 \equiv_3 1$$

$$x_1 \equiv_{5 \cdot 7} 0$$

x_2 -t az

$$x_2 \equiv_5 1$$

$$x_2 \equiv_{3 \cdot 7} 0$$

x_3 -at az

$$x_3 \equiv_7 1$$

$$x_3 \equiv_{3 \cdot 5} 0$$

kongruenciarendszerek megoldásaiként választjuk, akkor $x = 2 \cdot x_1 + 3 \cdot x_2 + 4 \cdot x_3$ megoldása lesz a kiindulási kongruenciarendszernek.

3. A 2. pontbeli kongruenciarendszerek megoldását úgy kaptuk, hogy az

$$5 \cdot 7 \cdot y_1 \equiv_3 1$$

kongruencia megoldását
szorozzuk $5 \cdot 7$ -tel:
 $x_1 = 5 \cdot 7 \cdot y_1$.

$$3 \cdot 7 \cdot y_2 \equiv_5 1$$

kongruencia megoldását
szorozzuk $3 \cdot 7$ -tel:
 $x_2 = 3 \cdot 7 \cdot y_2$.

$$3 \cdot 5 \cdot y \equiv_7 1$$

kongruencia
megoldását szorozzuk
 $3 \cdot 5$ -tel
 $x_3 = 3 \cdot 5 \cdot y_3$.

Az $M = 3 \cdot 5 \cdot 7$ jelölést bevezetve könnyebben megjegyezhet alakot kaptunk. Az

$$\frac{M}{3} \cdot y_1 \equiv_3 1$$

kongruencia megoldását
szorozzuk $\frac{M}{3}$ -mal:

$$x_1 = \frac{M}{3} \cdot y_1$$

$$\frac{M}{5} \cdot y_2 \equiv_5 1$$

kongruencia megoldását
szorozzuk $\frac{M}{5}$ -tel:

$$x_2 = \frac{M}{5} \cdot y_2$$

$$\frac{M}{7} \cdot y_3 \equiv_7 1$$

kongruencia
megoldását szorozzuk
 $\frac{M}{7}$ -tel:

$$x_3 = \frac{M}{7} \cdot y_3$$

4. A kiindulási kongruenciarendszer megoldása tehát

$$x = 2 \cdot \frac{M}{3} \cdot y_1 + 3 \cdot \frac{M}{5} \cdot y_2 + 4 \cdot \frac{M}{7} \cdot y_3.$$

Mindaz, amit ezen a példán elvégeztünk, általánosan is érvényes.

13.4.1. Tétel (Kínai maradéktétel)

Ha az $m_1, m_2, \dots, m_k$ modulusok páronként relatív prímek, akkor az

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

$$x \equiv a_k \pmod{m_k}$$

lineáris kongruenciarendszer megoldható, és a megoldás egyértelmű modulo $m_1 \cdot m_2 \cdot \dots \cdot m_k$.

Bizonyítás

Legyen $M = m_1 \cdot m_2 \cdot \dots \cdot m_k$ és tekintsük az

$$\frac{M}{m_i} \cdot y \equiv 1 \pmod{m_i} \quad (1 \leq i \leq k)$$

lineáris kongruenciákat. Az

$$\frac{M}{m_i} = m_1 \cdot \dots \cdot m_{i-1} \cdot m_{i+1} \cdot \dots \cdot m_k$$

elállítás jól mutatja, hogy $\frac{M}{m_i}$ mindegyik m_j -nek többszöröse, kivéve m_i -t, amellyel relatív prím.

Ugyanis, ha lenne közös prímtenyzük, mondjuk p , akkor $p \mid m_1 \cdot \dots \cdot m_{i-1} \cdot m_{i+1} \cdot \dots \cdot m_k$ miatt p osztója lenne valamely i -től különböző j -re m_j -nek is. Ez pedig ellentmond annak, hogy m_i és m_j relatív prímelek.

Tehát valóban $\text{Inko}\left(\frac{M}{m_i}, m_i\right) = 1$, és így az $\frac{M}{m_i} \cdot y \equiv 1 \pmod{m_i}$ kongruenciának van megoldása, mondjuk y_i . Eszerint

$$\frac{M}{m_i} \cdot y_i \equiv 1 \pmod{m_i} \quad (1 \leq i \leq k),$$

amit a_i -vel beszorozva kapjuk, hogy

$$a_i \cdot \frac{M}{m_i} \cdot y_i \equiv a_i \pmod{m_i} \quad (1 \leq i \leq k).$$

Ugyanakkor, ha $j \neq i$, akkor

$$a_j \cdot \frac{M}{m_j} \cdot y_j \equiv 0 \pmod{m_i} \quad (1 \leq i \leq k),$$

így az

$$x = a_1 \cdot \frac{M}{m_1} \cdot y_1 + \dots + a_{i-1} \cdot \frac{M}{m_{i-1}} \cdot y_{i-1} + a_i \cdot \frac{M}{m_i} \cdot y_i + a_{i+1} \cdot \frac{M}{m_{i+1}} \cdot y_{i+1} + \dots + a_k \cdot \frac{M}{m_k} \cdot y_k$$

egészre is minden i -re $(1 \leq i \leq k)$

$x =$

$$\begin{aligned} &= a_1 \cdot \frac{M}{m_1} \cdot y_1 + \dots + a_{i-1} \cdot \frac{M}{m_{i-1}} \cdot y_{i-1} + a_i \cdot \frac{M}{m_i} \cdot y_i + a_{i+1} \cdot \frac{M}{m_{i+1}} \cdot y_{i+1} + \dots + a_k \cdot \frac{M}{m_k} \cdot y_k \equiv \\ &\equiv 0 + \dots + 0 + a_i + 0 + \dots + 0 = a_i \pmod{m_i}. \end{aligned}$$

Ezzel a bizonyítást befejeztük.

Mindez elvezet bennünket az alábbi számolási séma kidolgozásához, melyet a kiindulási

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

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

$$x \equiv 4 \pmod{7}.$$

kongruenciarendszer megoldásával illusztrálunk. Els lépésként ellenrizzük, hogy a modulusok páronként relatív prímelek-e. Ez ugyanis a kínai maradéktétel alkalmazhatóságának feltétele.

--	--	--	--	--	--

a	m	$\frac{M}{m}$	$\frac{M}{m} \cdot y \equiv_m 1$	y	$\frac{M}{m} \cdot y \cdot a$
2	3	35	$35 \cdot y \equiv_3 1$	2	140
3	5	21	$21 \cdot y \equiv_5 1$	1	63
4	7	15	$15 \cdot y \equiv_7 1$	1	60
$M = 3 \cdot 5 \cdot 7$		Összesen			263

A számolási séma inicializálása az a és az m oszlopok kitöltésével történik. Ide írjuk rendre a kongruenciarendszer modulusait illetve a jobboldali konstansokat. Az M a modulusok, vagyis a második oszlopbeli elemek szorzata. A kitöltést az $\frac{M}{m}$ oszloppal folytatjuk. A negyedik oszlop elemei a megoldandó kongruenciák. Ezek megoldása kerül az ötödik oszlopba. Végül az utolsó oszlop elemeit az $\frac{M}{m}$, az y és az a jel oszlopok celláiban található számok szorzataként kapjuk. A számítás az utolsó oszlopban adódó számok összeadásával ér véget. A keletkezett érték a kongruenciarendszer megoldása.

▼ 13.4.2. Algoritmus: Kínai maradéktétel

Szöveges leírás	Maple metakód
1. <u>Input</u>: $a = [a_1, \dots, a_k], m = [m_1, \dots, m_k] \quad (x \equiv a_i \pmod{m_i})$ 2. Ellenrzend. hogy modulusok páronként relatív prímek-e. Ha nem Akkor Vége, a megoldásokról nem mondhatuk semmit 3. Legyen $M := m_1 \cdot \dots \cdot m_k$ 4. Legyen $x := 0$ 5. Az i változó 1, 2, ..., k értékeire hajtjuk végre az alábbi utasításokat Legyen y az $M/m_i \equiv 1 \pmod{m[i]}$ kongruencia megoldása Legyen $x := x + a[i] \cdot M/m[i] \cdot y$ 6. <u>Output</u>: x a megoldások listája	<u>Input</u>: $a = [a_1, \dots, a_k], m = [m_1, \dots, m_k] \quad (x \equiv a_i \pmod{m_i})$ for i to $nops(m) - 1$ do for j from $i + 1$ to $nops(m)$ do if $lnko(m_i, m_j) \neq 1$ then return [] fi od: od: $M := 1$; for i to $nops(m)$ do $M := M \cdot m[i]$ od: $x := 0$; for i to $nops(m)$ do $y := Linkongr(M/m[i], 1, m[i])$; $x := x + a[i] \cdot M/m[i] \cdot y$; od: return $x \pmod{M}$ <u>Output</u>: A megoldások listája

▼ 13.4.3. Maple implementáció

```
> restart:
[
  > with(ant):
    "Az ANT (Algorithmic Number Theory) csomag üdvözli Önt!" (1.3.3.1)
```

A **kinai** eljárás két listát vár aktuális paraméterként. Az els a megoldandó kongruenciarendszer konstansait, a második pedig a megfelel modulusokat tartalmazza. Az **ini** opcióval az eljárás megmutatja a megoldandó kongruenciarendszert, míg a **cal** opcióval a számológéptábla kitöltésébe ad betekintést.

```
> kinai([2,3,4],[3,5,7]);
53 (1.3.3.2)
```

```
> 53 mod 3, 53 mod 5, 53 mod 7;
2, 3, 4 (1.3.3.3)
```

```
> kinai([2,3,4],[3,5,7],ini,cal);
A megoldandó kongruenciarendszer(kinai):
x = 2 mod 3
x = 3 mod 5
x = 4 mod 7
```

Inicializálás(kinai):

$index$	a_i	m_i	$\frac{M}{m_i}$	$\frac{My}{m_i} = 1 \bmod m_i$	y	$x = \frac{My}{m_i} a_i$
1	2	3				
2	3	5				
3	4	7				
$M=105$						

Részletek megjelenítése 1(kinai):

$index$	a_i	m_i	$\frac{M}{m_i}$	$\frac{My}{m_i} = 1 \bmod m_i$	y	$x = \frac{My}{m_i} a_i$
1	2	3	35	$35*y = 1 \bmod 3$		
2	3	5	21	$21*y = 1 \bmod 5$		
3	4	7	15	$15*y = 1 \bmod 7$		
$M=105$						

Részletek megjelenítése 2(kinai):

<i>index</i>	a_i	m_i	$\frac{M}{m_i}$	$\frac{My}{m_i} = 1 \bmod m_i$	y	$x = \frac{My}{m_i}$	$a_i x$
1	2	3	35	$35*y = 1 \bmod 3$	-1	-35	-70
2	3	5	21	$21*y = 1 \bmod 5$	1	21	63
3	4	7	15	$15*y = 1 \bmod 7$	1	15	60
$M=105$			$\sum_{i=1}^3 a_i x_i$				53

Eredmény(kinai):

53

(1.3.3.4)

A kínai maradéktétel alkalmazása során lineáris kongruenciákat kell megoldani, amelyeket viszont diofantoszi egyenletek megoldására vezetünk vissza. Az **all** opció használatával a **kínai** eljárás teljes mélységben megmutatja a meghívott eljárásokat és azok számításainak részleteit.

> kinai([2, 3, 4, 31], [3, 5, 7, 13],all);

A megoldandó kongruenciarendszer(kinai):

$$x = 2 \bmod 3$$

$$x = 3 \bmod 5$$

$$x = 4 \bmod 7$$

$$x = 31 \bmod 13$$

Részletek megjelenítése 1(kinai):

<i>index</i>	a_i	m_i	$\frac{M}{m_i}$	$\frac{My}{m_i} = 1 \bmod m_i$	y	$x = \frac{My}{m_i}$	$a_i x$
1	2	3	455	$455*y = 1 \bmod 3$			
2	3	5	273	$273*y = 1 \bmod 5$			
3	4	7	195	$195*y = 1 \bmod 7$			
4	31	13	105	$105*y = 1 \bmod 13$			
$M=1365$							

A megoldandó kongruencia(Linkongr):

$$455 x = 1 \bmod 3$$

A megoldandó egyenlet(Diofantosz):

$$455 x + 3 y = 1$$

Részletek megjelenítése(Diofantosz):

[[osztandó, osztó, maradék, hányados, x, y],

[455, 3, 2, 151, -1, 152],

[3, 2, 1, 1, 1, -1],

$$\left[2, 1, 0, 2, 0, 1 \right],$$

$$\left[, \lnko(a, b) = 1, \frac{c}{\lnko(a, b)} = 1, \textit{Partikuláris megoldás:}, -1, 152 \right],$$

$$\left[, \frac{b}{\lnko(a, b)} = 3, \frac{a}{\lnko(a, b)} = 455, \textit{Általános megoldás:}, -1 + 3 t, 152 - 455 t \right]$$

Eredmény(Diofantosz):

$$[x = -1 + 3 t, y = 152 - 455 t]$$

Inkongruens megoldások(Linkongr):

$$[-1 + 3 t, t = 0..0]$$

Eredmény(Linkongr):

$$[-1]$$

A megoldandó kongruencia(Linkongr):

$$273 x = 1 \bmod 5$$

A megoldandó egyenlet(Diofantosz):

$$273 x + 5 y = 1$$

Részletek megjelenítése(Diofantosz):

$$\left[\left[\textit{osztandó}, \textit{osztó}, \textit{maradék}, \textit{hányados}, x, y \right],$$

$$\left[273, 5, 3, 54, 2, -109 \right],$$

$$\left[5, 3, 2, 1, -1, 2 \right],$$

$$\left[3, 2, 1, 1, 1, -1 \right],$$

$$\left[2, 1, 0, 2, 0, 1 \right],$$

$$\left[, \lnko(a, b) = 1, \frac{c}{\lnko(a, b)} = 1, \textit{Partikuláris megoldás:}, 2, -109 \right],$$

$$\left[, \frac{b}{\lnko(a, b)} = 5, \frac{a}{\lnko(a, b)} = 273, \textit{Általános megoldás:}, 2 + 5 t, -109 - 273 t \right]$$

Eredmény(Diofantosz):

$$[x = 2 + 5 t, y = -109 - 273 t]$$

Inkongruens megoldások(Linkongr):

$$[2 + 5 t, t = 0..0]$$

Eredmény(Linkongr):

$$[2]$$

A megoldandó kongruencia(Linkongr):

$$195 x = 1 \bmod 7$$

A megoldandó egyenlet(Diofantosz):

$$195x + 7y = 1$$

Részletek megjelenítése(Diofantosz):

$$\left[\left[\begin{array}{l} \text{osztandó, osztó, maradék, hányados, } x, y \end{array} \right], \right. \\ \left[195, 7, 6, 27, -1, 28 \right], \\ \left[7, 6, 1, 1, 1, -1 \right], \\ \left[6, 1, 0, 6, 0, 1 \right], \\ \left[, \text{Inko}(a, b) = 1, \frac{c}{\text{Inko}(a, b)} = 1, \text{Partikuláris megoldás:}, -1, 28 \right], \\ \left[, \frac{b}{\text{Inko}(a, b)} = 7, \frac{a}{\text{Inko}(a, b)} = 195, \text{Általános megoldás:}, -1 + 7t, 28 \right. \\ \left. \left. - 195t \right] \right]$$

Eredmény(Diofantosz):

$$[x = -1 + 7t, y = 28 - 195t]$$

Inkongruens megoldások(Linkongr):

$$[-1 + 7t, t = 0..0]$$

Eredmény(Linkongr):

$$[-1]$$

A megoldandó kongruencia(Linkongr):

$$105x = 1 \bmod 13$$

A megoldandó egyenlet(Diofantosz):

$$105x + 13y = 1$$

Részletek megjelenítése(Diofantosz):

$$\left[\left[\begin{array}{l} \text{osztandó, osztó, maradék, hányados, } x, y \end{array} \right], \right. \\ \left[105, 13, 1, 8, 1, -8 \right], \\ \left[13, 1, 0, 13, 0, 1 \right], \\ \left[, \text{Inko}(a, b) = 1, \frac{c}{\text{Inko}(a, b)} = 1, \text{Partikuláris megoldás:}, 1, -8 \right], \\ \left[, \frac{b}{\text{Inko}(a, b)} = 13, \frac{a}{\text{Inko}(a, b)} = 105, \text{Általános megoldás:}, 1 + 13t, -8 \right. \\ \left. \left. - 105t \right] \right]$$

Eredmény(Diofantosz):

$$[x = 1 + 13t, y = -8 - 105t]$$

Inkongruens megoldások(Linkongr):

$$[1 + 13t, t=0..0]$$

Eredmény(Linkongr):

$$[1]$$

Részletek megjelenítése 2(kinai):

$index$	a_i	m_i	$\frac{M}{m_i}$	$\frac{My}{m_i} = 1 \bmod m_i$	y	$x = \frac{My}{m_i}$	$a_i x$
1	2	3	455	$455*y = 1 \bmod 3$	-1	-455	-910
2	3	5	273	$273*y = 1 \bmod 5$	2	546	1638
3	4	7	195	$195*y = 1 \bmod 7$	-1	-195	-780
4	31	13	105	$105*y = 1 \bmod 13$	1	105	3255
$M = 1365$							$\sum_{i=1}^4 a_i x_i = 3203$

Eredmény(kinai):

$$3203$$

(1.3.3.5)

Kínai maradéktétel és számábrázolás

A kínai maradéktétel egyik fontos felhasználási területe a nagy számok ábrázolása, még pontosabban a nagy számok aritmetikája. Ez a megállapítás csak elsőre meglep. Ha kicsit utána gondolunk, azonnal természetessé válik. A gondolati kihívás abban áll, hogy a kínai maradéktételt új megvilágításba kell helyeznünk.

Nézzük meg egy konkrét példával megvilágítva, hogy mit is csinál a kínai maradéktétel? Megoldja például az

$$x \equiv 3 \bmod 5$$

$$x \equiv 6 \bmod 7$$

$$x \equiv 8 \bmod 13$$

kongruenciarendszert.

```
> kinai([3,6,8],[5,7,13]);
```

$$398$$

(1.4.1)

Ezzel a lépéssel (rögzített modulusok mellett!) a $[3, 6, 8]$ számhármashoz a kínai maradéktétel segítségével hozzárendeltük a 398 természetes számot.

Igen ám, de a számábrázolások során mindig fordítva jártunk el. Mindig arra törekedtünk, hogy a természetes számokhoz találjunk valamilyen ábrázolási módot. Az a kérdés merül tehát fel, hogy a 398 szám ismeretében hogy határozhatjuk meg a $[3, 6, 8]$ számhármast? A válasz nagyon egyszerű, csak rá kell nézni a megoldott kongruenciarendszerre. Rendre venni kell a 398 természetes szám 5-el, 7-tel és 13-mal való osztási maradékait, más szóval a $398 \bmod 5$, $398 \bmod 7$ és a $398 \bmod 13$ számokat.

```
> 398 mod 5, 398 mod 7, 398 mod 13;
```

3, 6, 8

(1.4.2)

Ha tehát rögzítjük az $[5, 7, 13]$ modulusokat, akkor ezek segítségével létrehozhatunk egy

$$n \rightarrow [n \bmod 5, n \bmod 7, n \bmod 13]$$

megfeleltetést. Kérdés, hogy ez a megfeleltetés kölcsönösen egyértelmű-e abban az értelemben, hogy különböző természetes számokhoz különböző rendezett hármast rendel? Sajnos nem, mert például

$$> \quad 853 \bmod 5, 853 \bmod 7, 853 \bmod 13;$$

3, 6, 8

(1.4.3)

tehát megfeleltetésünk a 853-hoz ugyanazt a hármast rendeli, mint 398-hoz.

Elkeseredésre azonban semmi ok, mert a kínai maradéktétel azt mondja, hogy páronként relatív prím modulusok esetén, és a mi modulusaink ilyenek, a kongruenciarendszer megoldása egyértelmű modulo $5 \cdot 7 \cdot 13 = 455$. Ha tehát

$$n \in \{0, 1, \dots, 455\},$$

akkor már teljesül, hogy a fenti hozzárendelés a halmaz különböző elemeihez különböző számhármast rendel.

Mit mondhatunk a számhármast elemiről? Mivel bármely m modulus esetén $n \bmod m$ nem negatív és kisebb m -nél, ezért hozzárendelésünk olyan $[a_1, a_2, a_3]$ hármast hoz létre, amelyekre

$$a_1 \in \{0, 1, \dots, 4\}, a_2 \in \{0, 1, \dots, 6\}, a_3 \in \{0, 1, \dots, 12\}.$$

Most pedig általánosítsunk! Tekintsük az $m_1, m_2, \dots, m_k$ modulusokat, melyekről feltesszük, hogy páronként relatív prímelek, és legyen

$$M = m_1 \cdot m_2 \cdot \dots \cdot m_k$$

Ekkor minden

$$n \in \{0, 1, \dots, M-1\}$$

egész szám egyértelműen reprezentálható az

$$[n \bmod m_1, n \bmod m_2, \dots, n \bmod m_k]$$

rendezett k -assal. Az egyértelműség a $\bmod$ művelet egyértelműségéből adódik.

Ha pedig adott az $[a_1, a_2, \dots, a_k]$ rendezett k -as ($a_i \in \{0, 1, \dots, m_i-1\}$, $i = 1, 2, \dots, k$) és azt kédezzük, hogy melyik az a természetes szám, amelyiket éppen ez a rendezett k -as reprezentál, akkor meg kell keresnünk azt az n -et, amelyre

$$n \equiv a_i \bmod m_i \quad (i = 1, 2, \dots, k).$$

Ez az n szám pedig nem más mint az

$$x \equiv a_1 \bmod m_1$$

$$x \equiv a_2 \bmod m_2$$

...

$$x \equiv a_k \bmod m_k$$

kongruenciarendszer megoldása, ami a modulusok választása miatt létezik és egyértelműen meghatározott modulo M .

Röviden összefoglalva azt mondhatjuk, hogy rögzített modulusok mellett a kódolást, vagyis a természetes számok k -asokkal való reprezentációját, az egyes modulusokkal való maradékos osztásokkal, míg a dekódolást, a k -asok által reprezentált érték kiszámítását, pedig a kínai maradéktétellel végezhetjük el.

Példák

Rögzítsük a 2, 3 modulusokat. Ekkor $M = 2 \cdot 3 = 6$. A $\{0, 1, 2, 3, 4, 5\}$ halmaz elemeit az alábbi rendezett párokkal reprezentálhatjuk

$$\begin{aligned} 0 &\rightarrow [0 \bmod 2, 0 \bmod 3] = [0, 0], \\ 1 &\rightarrow [1 \bmod 2, 1 \bmod 3] = [1, 1], \\ 2 &\rightarrow [2 \bmod 2, 2 \bmod 3] = [0, 2], \\ 3 &\rightarrow [3 \bmod 2, 3 \bmod 3] = [1, 0], \\ 4 &\rightarrow [4 \bmod 2, 4 \bmod 3] = [0, 1], \\ 5 &\rightarrow [5 \bmod 2, 5 \bmod 3] = [1, 2]. \end{aligned}$$

Látható, hogy a reprezentációban résztvevő rendezett párok mind különbözők. Ha most például az $[1, 0]$ párt dekódolni szeretnénk, vagyis meg akarjuk keresni azt az n természetes számot, amelyet az $[1, 0]$ reprezentál, akkor a kínai maradéktételhez kell fordulnunk.

```
> kinai([1,0],[2,3]);
```

3 (1.4.4)

Vegyünk most olyan reprezentációt, melyben rendezett 5-ösök szerepelnek, a modulusok pedig legyenek 4, 5, 11, 13 és 19. Láthatóan ezek páronként relatív prímek.

```
> M:=4*5*11*13*19;
```

$M := 54340$ (1.4.5)

Példaként tekintsük $23014 \in \{0, 1, \dots, 54340\}$ rendezett ötössel való reprezentációját. Az n változónak más-más értéket adva tetszés szerint kísérletezhetünk.

```
> n:=23014;
```

$n := 23014$ (1.4.6)

```
> [n mod 4, n mod 5, n mod 11, n mod 13, n mod 19];
```

[2, 4, 2, 4, 5] (1.4.7)

```
> kinai(%, [4, 5, 11, 13, 19]);
```

23014 (1.4.8)

Természetesen a számok reprezentálhatósága csak az els lépés egy használható számábrázolás felé. A használhatóság másik és egyáltalán nem elhanyagolható feltétele az algebrai műveletek, az összeadás és a szorzás, hatékony elvégezhetősége.

Ezekkel kapcsolatosan jó hírünk van. Emlékezzünk csak arra, hogy mind az összeadás, mind pedig a szorzás művelete modulo m erejéig felcserélhető a **mod** m maradékképzés műveletével. Ezt az összeadás esetén formulával úgy fejeztük ki, hogy

$$(n_1 + n_2) \bmod m_i = (n_1 \bmod m_i + n_2 \bmod m_i) \bmod m_i \quad (i = 1, 2, \dots, k) .$$

Nincs más dolgunk, mint ezt a két egyenlőséget a most bevezett reprezentáció szemszögéből értelmezni. A bal oldalon két egész összegének m_i -vel való osztási maradéka áll, ez pedig nem más, mint az $n_1 + n_2$ összeg reprezentációjának i -edik komponense. Az egyenlőségjel jobb oldalán pedig a n_1 reprezentációjának i -edik komponenséhez adjuk hozzá az n_2 reprezentációjának i -edik komponensét, majd vesszük a modulo m_i maradékot. Mindezt tömören úgy mondhatjuk, hogy

az $n_1 + n_2$ összeg reprezentációjának i -edik komponensét megkapjuk, ha vesszük az összeadandók i -edik komponenseinek modulo m összegét.

Ennél szebb eredményt álmodni sem mertünk! És most számolgassunk a fejezet elején felvett 5, 7 és 13 modulusokkal. Legyen $n_1 = 129$ és $n_2 = 284$. Elsként állítsuk el a rendezett hármassokkal való reprezentációkat rendre a k_1 illetve a k_2 változóknak.

```
[ > n1:=129;n2:=284;
  > k1:=[n1 mod 5,n1 mod 7,n1 mod 13];
                                     k1 := [4, 3, 12]                                (1.4.9)
  > k2:=[n2 mod 5,n2 mod 7,n2 mod 13];
                                     k2 := [4, 4, 11]                                (1.4.10)
```

Adjuk össze komponensenként a k_1 -et és a k_2 -t. Természetesen az els komponenseken modulo 5, a második komponenseken modulo 7, míg a harmadik komponenseken pedig modulo 13 összeadást végzünk:

```
[ > k1[1]+k2[1] mod 5;
                                     3                                (1.4.11)
  > k1[2]+k2[2] mod 7;
                                     0                                (1.4.12)
  > k1[3]+k2[3] mod 13;
                                     10                               (1.4.13)
```

Tehát a komponensenkénti összeadás eredménye $[3, 0, 10]$. És most fordítsuk meg a sorrendet. Elször képezzük az $n_1 + n_2$ összeget, és másodikként reprezentáljuk rendezett hármassal.

```
[ > összeg:=n1+n2;
                                     összeg := 413                                (1.4.14)
  > [összeg mod 5, összeg mod 7, összeg mod 13];
                                     [3, 0, 10]                                (1.4.15)
```

Az eredmény önmagáért beszél.

A szorzás az eddig elmondottak után semmi újdonságot nem hoz. A

$$(n_1 \cdot n_2) \bmod m = ((n_1 \bmod m) \cdot (n_2 \bmod m)) \bmod m$$

egyenlőség biztosítja, hogy az $n_1 \cdot n_2$ összeg reprezentációjának i -edik komponensét megkapjuk, ha vesszük az szorzandók i -edik komponenseinek modulo m_i szorzatát.

Els lépésként vegyük fel a modulusokat. Vigyázzunk azonban arra, hogy páronként relatív prímek legyenek.

```
> m[1]:=10:m[2]:=13:m[3]:=17:m[4]:=19:
> M:=m[1]*m[2]*m[3]*m[4];
M:= 41990 (1.4.16)
```

Az ábrázolási tartomány $\{0, 1, \dots, M-1\}$. Felvesszük az a és b számokat, ezek négyesekkel való reprezentációját rendre az ar illetve a br változókban számoljuk ki. Ezután elvégezzük a komponensenkénti szorzást, majd az eredményt a kínai maradéktétel segítségével vissza alakítjuk decimális számmá. Az utolsó utasítás csak ellenrzési célokat szolgál.

```
> a:=984:b:=28:
> ar:=[a mod m[1],a mod m[2],a mod m[3],a mod m[4]];
ar:= [4, 9, 15, 15] (1.4.17)
```

```
> br:=[b mod m[1],b mod m[2],b mod m[3],b mod m[4]];
br:= [8, 2, 11, 9] (1.4.18)
```

```
> k:=[ar[1]*br[1] mod m[1],ar[2]*br[2] mod m[2],ar[3]*br[3] mod
m[3],ar[4]*br[4] mod m[4]];
k:= [2, 5, 12, 2] (1.4.19)
```

```
> kinai(k, [m[1],m[2],m[3],m[4]]);
27552 (1.4.20)
```

```
> a*b;
27552 (1.4.21)
```

Ejtsünk néhány szót arról is, hogy a most bevezetett, a kínai maradéktételre alapozott reprezentáció milyen számolási megtakarításokkal jár. A példa kedvéért tegyük fel, hogy legfeljebb 100 jegy egészen, vagyis legfeljebb 10^{100} nagyságrend számokon szeretnénk szorzást végezni. Ha mindezt helyiértékes számrendszerben megismert algoritmus alapján szeretnénk elvégezni, akkor össze kellene szorozni a szorzandó mind a 100 jegyét a szorzó mindegyik jegyével, amelyekből ismét csak 100 van. Ez mindösszesen 10^4 szorzás művelet számjegyeken való elvégzését jelenti.

És most tegyük fel, hogy választunk modulusnak 20 darab prímszámot, mégpedig úgy, hogy mindegyikük legalább 10 jegy legyen. Így szorzatuk nem kisebb, mint

$(10^{10})^{20}$, vagyis legalább kétszáz jegy. Ez megfelel is lesz nekünk, mert két legfeljebb 100 jegy egész szorzata legfeljebb 200 jegy.

Els lépésként reprezentáljuk a szorzót és a szorzandót rendezett 20-asokkal. A komponensenkénti szorzás miatt most mindösszesen 20 darab szorzást kell végeznünk. Ha a komponensenkénti szorzást is a helyiértékes szorzási algoritmussal végezzük, akkor ez szorzásonként legfeljebb $10 \cdot 10 = 100$ szorzás. Vagyis mindösszesen legfeljebb 2000

számjegyeken elvégzend szorzáshoz jutunk, ami még akkor is jelents megtakarítás a kiindulási 10^4 mvelettel szemben, ha most eltekintettünk attól, hogy a reprezentáció során maradékos osztásokat kell végezni, és a kapott eredmény dekódolása is mveletek elvégzésével jár.

Végül lássuk, hogy néz ki mindez a gyakorlatban. Elször is állítsuk el a modulusokat. Hogy a páronként való relatív prímiséggel ne legyen gondunk, eleve prímekeket választunk. Úgy járunk el, hogy vesszük a 10^{10} számot és a Maple **nextprime** eljárásával 20 egymás utáni prímet állítunk el.

```
> primek:=NULL:m:=10^10:
  for i to 20 do
    m:=nextprime(m):primek:=primek,m:
  od:
  modulusok:=[primek];
modulusok := [10000000019, 10000000033, 10000000061, 10000000069,
  10000000097, 10000000103, 10000000121, 10000000141, 10000000147,
  10000000207, 10000000259, 10000000277, 10000000279, 10000000319,
  10000000343, 10000000391, 10000000403, 10000000469, 10000000501,
  10000000537]
```

(1.4.22)

Ezután veszünk két véletlen számot 10^{99} és 10^{100} között.

```
> a:=RandomTools[Generate](integer(range=10^99..10^100));
a :=
4360502476087703643478799129600583388226237375598310861111349310\
260242596315037923371797255459738897
```

(1.4.23)

```
> b:=RandomTools[Generate](integer(range=10^99..10^100));
b :=
3571688041795300053591901201138337594976981231584627880122195156\
666489257799942519220831091705809969
```

(1.4.24)

Hogy lássuk kicsit a Maple képességeit is, szorozzuk össze a két legalább 99 jegy számot. De nem az a célunk, hogy a Maple-t csodáljuk! Állítsuk inkább el az a és b számok reprezentációját rendezett huszasokkal, felhasználva a *modulusok* változóban elhelyezett páronként relatív prím modulusokat. Az ar és a br változók egy-egy rendezett 20-ast tartalmaznak, amelyek rendre az a és b egészek reprezentációi.

```
> a*b;
15574354550061247423485523081705601839838931631627173191057573339038\
0966551958125435095252596492993468896147936967058490356668876651\
9916564152605286039827647862358612744438283131398654997001863966\
4193
```

(1.4.25)

```
> ar:=kinrep(a,modulusok);
ar := [9799785729, 4500407240, 5368895567, 5033630389, 5720133393,
  382137565, 5675195233, 2851393216, 5008071625, 6836117545,
  5751569491, 4262786454, 7157641418, 5645193796, 1383571502,
  2559081495, 9280290251, 4202894217, 8717408947, 6289598068]
```

(1.4.26)

```
> br:=kinrep(b,modulusok);
br := [5698994763, 3411537596, 9210168432, 3284036803, 5407821629,
3342628636, 5307750629, 6404996550, 9958057872, 3021620077,
1128581404, 4651412132, 7165146863, 1049013456, 2447635207,
6460795841, 3367086971, 4573301878, 7571328840, 1270777995]
```

(1.4.27)

Végül az **ant** csomag **kinszorzás** eljárásával elvégezzük a komponensenkénti szorzást, persze felhasználva a **modulusok** változóban elhelyezett modulusokat. Az eredményt a **kinai** eljárással visszaalakítjuk decimális számmá. Ebből ellenrészéppen kivonjuk a Maple által kiszámolt szorzatot.

```
> kinszorzás(ar,br,modulusok);
[1980175091, 5904677188, 4252704768, 6113877790, 3375987631, 4503668655,
3171051087, 3662800155, 5772286949, 5121654452, 3236487584,
9025922789, 1794712226, 4823617462, 3540868654, 3208297282,
1964431582, 4171703667, 3776571834, 3001869317]
```

(1.4.28)

```
> kinai(%,modulusok);
15574354550061247423485523081705601839838931631627173191057573339038\
0966551958125435095252596492993468896147936967058490356668876651\
9916564152605286039827647862358612744438283131398654997001863966\
4193
```

(1.4.29)

```
> %-a*b;
0
```

(1.4.30)

Az eredmény 0, tehát jól számoltunk.

Ellenrz kérdések

1. Hogyan változik a modulus, ha a kongruenciát egy k számmal osztjuk?
2. Mikor oszthatjuk a kongruenciát a modulus megváltoztatása nélkül bármely modulusnál kisebb számmal?
3. Mikor oszthatjuk a $a \equiv b \pmod{m}$ kongruenciát korlátozás nélkül az a és b minden osztójával (kivéve m többszöröseit)?
4. Mi a szükséges és elégséges feltétele az $a \equiv_m b$ és $a \equiv_n b$ kongruenciák egyidejű teljesülésének?
5. Ha $m \mid n$, akkor mi a kapcsolat a modulo m és modulo n maradékosztályok között?
6. Mi az $a \cdot x \equiv b \pmod{m}$ kongruencia megoldhatóságának feltétele?
7. Hány megoldása van az $a \cdot x \equiv b \pmod{m}$ kongruenciának?
8. Oldjuk meg az $5 \cdot x \equiv_{12} 1$ kongruenciát!
9. Oldjuk meg az $6 \cdot x \equiv_{20} 2$ kongruenciát!
10. Mondjuk ki a kínai maradéktételt!

11. Oldjuk meg az

$$x \equiv 4 \pmod{2}$$

$$x \equiv 7 \pmod{5}$$

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

lineáris kongruenciarendszert!