Kongruenciák

Diszkrét modellek alkalmazásai

1. Definíció és tulajdonságok

1.1. Definíció. Az $a \in \mathbb{Z}$ és $b \in \mathbb{Z}$ számok **kongruensek** modulo $m \in \mathbb{N}^+$, ha $m \mid b - a$.
Jelölés: $a \equiv b \pmod{m}$, vagy röviden $a \equiv b\ (m)$. Tagadás jelölése: $a \not\equiv b \pmod{m}$.
További elnevezések: az m a **modulus**, az "$a \equiv b \pmod{m}$" állítás pedig egy **kongruencia**.

Példa. $14 \equiv 34 \pmod{10}$ ("14 és 34 kongruens modulo 10"), mert $10 \mid 34 - 14$.

Ebből a példából sejthető, hogy $a \equiv b \pmod{10}$ pontosan akkor lesz igaz, ha a és b utolsó számjegye megegyezik (legalábbis ha $a, b \in \mathbb{N}$). Általában belátható, hogy $a \equiv b \pmod{m}$ pontosan akkor igaz, ha a és b m-mel való osztási maradéka megegyezik, azaz $a \bmod m = b \bmod m$. Leegyszerűsítve úgy is fogalmazhatunk, hogy "kongruens" = "azonos maradékot ad".

Példa. $9 \equiv 23\ (7)$, mert $7 \mid 23 - 9$, és valóban: 9-nek és 23-nak is 7-tel osztva 2 a maradéka.

(Megjegyzés: ne keverjük a "mod" jelölés kétféle használatát: az "$a \bmod m$" kifejezésben ez a maradékos osztás maradékát jelöli, pl. $34 \bmod 10 = 4$, az "$a \equiv b \pmod{m}$" kifejezésben pedig a teljes "egyenletre" (pontosabban *kongruenciára*) vonatkozik a "mod", a fent leírtak alapján. Ilyenkor egyik oldalon sem kell feltétlenül a maradéknak állnia, pl. $14 \equiv 34 \pmod{10}$ egyik oldalán sincs 4.)

Kongruenciákat olyankor használunk, amikor egy számításnak csak a maradéka érdekel bennünket (egy rögzített m-re). Például így számolunk az órákkal: ha most 18 óra van, akkor 10 órával később nem 28 óra lesz, hanem $28 \bmod 24 = 4$ óra. Ezt úgy is írhatjuk, hogy $18 + 10 \equiv 4\ (24)$.

1.2. Tétel (a kongruencia tulajdonságai)**.** *Tetszőleges $m \in \mathbb{N}^+$ esetén:*

1. *reflexív:* $\forall a \in \mathbb{Z} : a \equiv a\ (m)$;
2. *szimmetrikus:* $\forall a, b \in \mathbb{Z} : a \equiv b\ (m) \implies b \equiv a\ (m)$;
3. *tranzitív:* $\forall a, b, c \in \mathbb{Z} : a \equiv b\ (m) \ \wedge\ b \equiv c\ (m) \implies a \equiv c\ (m)$.
4. *összeadás:* $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z} : a_1 \equiv b_1\ (m) \ \wedge\ a_2 \equiv b_2\ (m) \implies a_1 + a_2 \equiv b_1 + b_2\ (m)$.
5. *kivonás:* $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z} : a_1 \equiv b_1\ (m) \ \wedge\ a_2 \equiv b_2\ (m) \implies a_1 - a_2 \equiv b_1 - b_2\ (m)$.
6. *szorzás:* $\forall a_1, a_2, b_1, b_2 \in \mathbb{Z} : a_1 \equiv b_1\ (m) \ \wedge\ a_2 \equiv b_2\ (m) \implies a_1 a_2 \equiv b_1 b_2\ (m)$.
7. *hatványozás:* $\forall a, b \in \mathbb{Z}, n \in \mathbb{N} : a \equiv b\ (m) \implies a^n \equiv b^n\ (m)$.

2. Maradékosztályok

A fenti tétel szerint a kongruencia ($\equiv$) mint reláció reflexív, szimmetrikus és tranzitív – vagyis *ekvivalenciareláció* (lásd pl. Diszkrét matematika I). Az ekvivalenciarelációról pedig tudjuk, hogy meghatározza az alaphalmaz egy *osztályfelbontását*, azaz felbontja azt diszjunkt halmazok uniójára. Az $a \equiv b \pmod{m}$ kongruencia a következő osztályokra bontja fel $\mathbb{Z}$-t:

$$\{km \quad \mid k \in \mathbb{Z}\},$$
$$\{km+1 \mid k \in \mathbb{Z}\},$$
$$\{km+2 \mid k \in \mathbb{Z}\},$$
$$\ldots,$$
$$\{km+m-1 \mid k \in \mathbb{Z}\}.$$

Látható, hogy pontosan azok a számok kerültek egy osztályba, amelyek m-mel osztva ugyanazt a maradékot adják. Például $m = 5$ esetén az osztályok a következők:

$$\{5k \quad \mid k \in \mathbb{Z}\} = \{\ldots, -10, -5, 0, 5, 10, \ldots\},$$
$$\{5k+1 \mid k \in \mathbb{Z}\} = \{\ldots, -9, -4, 1, 6, 11, \ldots\},$$
$$\{5k+2 \mid k \in \mathbb{Z}\} = \{\ldots, -8, -3, 2, 7, 12, \ldots\},$$
$$\{5k+3 \mid k \in \mathbb{Z}\} = \{\ldots, -7, -2, 3, 8, 13, \ldots\},$$
$$\{5k+4 \mid k \in \mathbb{Z}\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}.$$

2.1. Definíció. Adott m modulus esetén a kongruencia mint ekvivalenciareláció által meghatározott osztályokat az m szerinti **maradékosztályok**nak nevezzük [*congruence class*]. Jelölés: $\overline{a}$ az a maradékosztály, amely tartalmazza $a \in \mathbb{Z}$-t. (Ha m nem egyértelmű a kontextusból, akkor: $\overline{a}_m$.)

Példa. $m = 5$ esetén $\overline{3} = \{5k+3 \mid k \in \mathbb{Z}\} = \{\ldots, -7, -2, 3, 8, 13, \ldots\}$.

Az $\overline{a}$ definíciója értelmes, mert minden $a \in \mathbb{Z}$ pontosan egy maradékosztályban van benne. Viszont egy maradékosztálynak több jelölése is van, például $m = 5$ esetén $\overline{3} = \overline{8} = \overline{28} = \overline{-2} = \ldots$.

2.2. Definíció. Az m szerinti összes maradékosztály halmazát $\mathbb{Z}_m$-mel jelöljük (alternatív jelölések: $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\langle m \rangle$), azaz $\mathbb{Z}_m := \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

(Megjegyzés: $\mathbb{Z}_m$ elemei nem számok, hanem halmazok (maradékosztályok), pl. $2 \neq \overline{2}$, de $2 \in \overline{2}$.)

Ha a maradékosztályokra egyérelműen szeretnénk hivatkozni, akkor mindegyikből választani kell egy *reprezentánst*. Azaz szükségünk lesz a következőre:

2.3. Definíció. Egy egész számokból álló halmazt, amely minden maradékosztályból pontosan egy elemet (*reprezentást*) tartalmaz, **teljes maradékrendszer**nek nevezünk (modulo m).

Példa. A következők mindegyike teljes maradékrendszer modulo 5:
$\{0, 1, 2, 3, 4\}$, $\{1, 2, 3, 4, 5\}$, $\{-2, -1, 0, 1, 2\}$, $\{34, 35, 36, 37, 38\}$, $\{10, 6, -3, 23, -6\}$ stb.

Minden m-re végtelen sok teljes maradékrendszer van. Minden teljes maradékrendszernek pontosan m eleme van. Az egyik leggyakrabban használt teljes maradékrendszer: $\{0, 1, 2, \ldots, m-1\}$.

Maradékosztályok között műveleteket is lehet végezni:

2.4. Definíció. Adott $m \in \mathbb{N}^+$ modulusra és bármely $a, b \in \mathbb{Z}$-re:

- $\overline{a} + \overline{b} := \overline{a+b}$,
- $\overline{a} - \overline{b} := \overline{a-b}$,
- $\overline{a} \cdot \overline{b} := \overline{ab}$.

Példa. $m = 10$ esetén $\overline{7} + \overline{3} \cdot \overline{6} = \overline{7} + \overline{18} = \overline{7} + \overline{8} = \overline{15} = \overline{5}$. Ezt a számítást kongruenciákkal is felírhatjuk a következőképpen: $7 + 3 \cdot 6 \equiv 7 + 8 \equiv 5 \ (10)$.

A maradékosztályokkal való számolást **moduláris aritmetiká**nak nevezzük.

3. Lineáris kongruenciák

Fent a tulajdonságoknál láthattuk, hogy a kongruenciákat lehet összeadni, kivonni, szorozni és hatványozni. Nem volt szó azonban osztásról – és nem véletlenül. Például a $4 \equiv 14\ (10)$ kongruenciát nem oszthatjuk el 2-vel, mert $2 \not\equiv 7\ (10)$. De akkor mit tudunk kezdeni az osztással?

Először is: mit is jelent pontosan az osztás? A valós számok körében b/a azt az egyértelmű $x \in \mathbb{R}$ számot jelenti, amelyre $ax = b$. (Például $6/2 = 3$ a $2x = 6$ megoldása.) Vagyis az osztás nem más, mint egy lineáris egyenlet megoldása. Érdemes tehát a lineáris egyenletek moduláris megfelelőjével foglalkozni:

3.1. Definíció. Az $ax \equiv b \pmod{m}$ kongruenciát, ahol $a, b \in \mathbb{Z}$ ismert paraméterek és $x \in \mathbb{Z}$ az ismeretlen, **lineáris kongruenciá**nak nevezzük [*linear congruence*].

Példa. A $2x \equiv 6 \pmod{10}$ egy lineáris kongruencia, amelynek *egy* megoldása $x = 3$.

Most vizsgáljuk meg, hogyan tudjuk egy lineáris kongruencia összes megoldását megtalálni.

Először is vegyük észre, hogy ha találtunk egy x megoldást, akkor $x + m$, $x + 2m$ stb. szintén megoldások, hiszen "modulo m" számolunk, azaz csak az m szerinti maradék számít. Tehát például ha $2x \equiv 6\ (10)$ egy megoldása $x = 3$, akkor megoldásai még az $x = 13$, $x = 23$, $x = -7$ stb. is. Ezt a végtelen sok megoldást röviden úgy foglalhatjuk össze, hogy $x \equiv 3\ (10)$.

(Az egyszerűség kedvéért a továbbiakban az egymással kongruens megoldásokat nem különböztetjük meg, hanem azt mondjuk, hogy a lineáris kongruencia *egyértelműen megoldható*, ha a megoldások mind kongruensek egymással modulo m; vagy *két megoldása van*, ha a megoldások két különböző maradékosztályból vannak; és így tovább.)

Az $ax \equiv b \pmod{m}$ lineáris kongruencia megoldásához elegendő az $x = 0, 1, 2, \ldots, m-1$ számokat végigpróbálgatni, hiszen bármely más szám kongruens ezen x-ek valamelyikével. (Vagyis éppen egy teljes maradékrendszer elemeit kell ellenőrizni.) A fenti példa esetében tehát csak 10 számot kell végignézni. Például számítsuk ki a következő moduláris szorzótábla-részletet (ahol az első sorban x, a másodikban $2x$ mod 10, a harmadikban pedig $3x$ mod 10 szerepel):

```
sage: matrix([[a*x % 10 for x in range(10)] for a in range(1,4)])
[0 1 2 3 4 5 6 7 8 9]
[0 2 4 6 8 0 2 4 6 8]
[0 3 6 9 2 5 8 1 4 7]
```

Innen a következőket olvashatjuk le:

- A $2x \equiv 6\ (10)$ kongruenciának *két* megoldása is van:
  - $x \equiv 3\ (10)$ (erre rájöhettünk abból, hogy $6/2 = 3$);
  - $x \equiv 8\ (10)$ (ez már kevésbé nyilvánvaló).

  Vagy, mivel távolságuk éppen 5, ezért összevonhatjuk őket egyetlen kongruenciába: $x \equiv 3\ (5)$.
- Most nézzük a $3x \equiv 8\ (10)$ kongruenciát. A táblázatból leolvasható, hogy ennek pontosan egy megoldása van: $x \equiv 6\ (10)$. (Ez sem nyilvánvaló, hiszen $8/3$ nem egész szám. Viszont 8 helyett vehetünk egy másik 8-ra végződő számot: $18/3 = 6$.)
- Sőt, általában a $3x \equiv b\ (10)$ alakú kongruenciák is egyértelműen megoldhatóak, hiszen a harmadik sorban minden maradék pontosan egyszer szerepel.
- És mi a helyzet a $2x \equiv b\ (10)$ alakú kongruenciákkal? Mivel a második sorban csak páros számok szerepelnek, ezért páratlan b-kre nincs megoldás. Viszont mindegyik páros maradék pontosan kétszer szerepel, ezért páros b-kre két megoldás is lesz.

Az olyan kis modulusokra, mint $m = 10$, a fenti kimerítő keresés ("brute force"), azaz az m szám végigpróbálgatása jól működik. Nagyobb m-ekre viszont ennél hatékonyabb módszert kell keresni.

Ehhez bontsuk ki az $ax \equiv b \pmod m$ lineáris kongruenciát a definíció alapján:

$$\begin{aligned} ax &\equiv b \pmod m \\ &\Downarrow \quad \text{(kongruencia definíciója)} \\ m &\mid b - ax \\ &\Downarrow \quad \text{(oszthatóság definíciója)} \\ \exists y \in \mathbb{Z} &: my = b - ax \\ &\Downarrow \quad \text{(átrendezés)} \\ \exists y \in \mathbb{Z} &: ax + my = b \end{aligned}$$

Vagyis visszavezettük egy lineáris diofantikus egyenletre, amelyet az előző jegyzetben (Legnagyobb közös osztó) már megoldottunk. Itt most elég csak az x-szel foglalkozni, az y-ra nincs szükségünk. Tudjuk, hogy ennek az egyenletnek akkor és csak akkor van megoldása, ha $\text{lnko}(a,m) \mid b$, és ha x_0 egy megoldás x-re, akkor végtelen sok megoldás van: $x = x_0 + k \cdot m \,/\, \text{lnko}(a,m)$, ahol k végigfut az egész számok halmazán. Vagyis a megoldások lépésköze $m \,/\, \text{lnko}(a,m)$, ami azt jelenti, hogy 0-tól $m-1$-ig pontosan $\text{lnko}(a,m)$ darab megoldás van. Speciálisan, ha $\text{lnko}(a,m) = 1$, azaz a és m relatív prímek, akkor egyértelműen megoldható. Tehát:

Lineáris kongruencia megoldása:

Bemenet: $a, b \in \mathbb{Z}, m \in \mathbb{N}^+$, a kongruencia ($ax \equiv b \pmod m$) paraméterei
Kimenet: az összes megoldás 0 és $m-1$ között
$(g, x_g, y_g) :=$ bővített euklideszi algoritmus(a,m) *(y_g nem kell)*
ha $g \nmid b \rightarrow$ *nincs megoldás*
Első megoldás: $x_0 := x_g \cdot b/g \bmod m/g$
Összes megoldás: $x_0,\ x_0 + m/g,\ x_0 + 2m/g,\ \ldots,\ x_0 + (g-1)m/g$
(azaz: $x = x_0 + k \cdot m/g \quad (k = 0, 1, \ldots, g-1)$)
(azaz: $x \equiv x_0 \pmod{m/g}$)

Példa. A $2x \equiv 6\ (10)$ lineáris kongruencia esetén $g = \text{lnko}(2,10) = 2$, és a Bézout-együttható $x_g = 1$ (és $y_g = 0$, de az nem kell). Mivel $g \mid 6$, ezért van megoldás, méghozzá pontosan kettő ($g = 2$): az első $1 \cdot 6/2 \bmod 10/2 = 3 \bmod 5 = 3$, a második pedig $3 + 10/2 = 8$ (ahogy azt fent is láttuk).

Példa. A $3x \equiv 8\ (10)$ esetén $g = \text{lnko}(3,10) = 1$, a Bézout-együttható pedig $x_g = -3$. Mivel $g \mid 8$ és $g = 1$, ezért pontosan egy megoldás van: $x := -3 \cdot 8/1 \bmod 10/1 = -24 \bmod 10 = 6$.

Megjegyzés: az előző jegyzetben a lineáris diofantikus egyenleteknél tett megjegyzés alapján itt is leegyszerűsíthetjük a számítást, ha a kongruenciát leosztjuk $\text{lnko}(a,m)$-mel (a modulust is), ekkor ugyanis a fenti algoritmusban $g = 1$, azaz pontosan egy megoldás lesz (az új modulus szerint). Például a $2x \equiv 6\ (10)$ kongruenciát 2-vel leosztva azt kapjuk, hogy $x \equiv 3\ (5)$, amely már maga a megoldás. Másik példa: $4x \equiv 6\ (10) \longrightarrow 2x \equiv 3\ (5)$, ezt a fenti módon megoldva kijön, hogy $x \equiv 4\ (5)$, amit visszaírva 10-es modulusra: $x \equiv 4\ (10)$ és $x \equiv 9\ (10)$.

Lineáris kongruenciákat természetesen a Sage is meg tud oldani, a `solve_mod()` függvénnyel:

```
sage: solve_mod(2*x == 6, 10)
[(8,), (3,)]
sage: _[1][0]   # a második megoldás
3
sage: for (xx,) in solve_mod(2*x == 6, 10):
....:     assert xx*2 % 10 == 6   # ellenőrzés
```

4. Moduláris inverz

Most foglalkozzunk a lineáris kongruenciák azon speciális esetével, amikor a jobb oldal 1.

4.1. Definíció. $a \in \mathbb{Z}$ **moduláris inverze** modulo m az $ax \equiv 1 \pmod{m}$ lineáris kongruencia megoldása. Jelölés: $a^{-1} \bmod m$. Ha ez létezik, akkor azt mondjuk, hogy a **invertálható** modulo m.

Példa. 3 moduláris inverze 7 modulo 10, mert a $3x \equiv 1\ (10)$ kongruenciának megoldása az $x = 7$.

Példa. 2 nem invertálható modulo 10, mert a $2x \equiv 1\ (10)$ kongruenciának nincs megoldása.

Ahogy a lineáris kongruencia az osztás megfelelője volt, úgy a moduláris inverz a reciproké $(1/x)$: például 3 inverze $\mathbb{R}$-ben (azaz reciproka) 1/3, modulárisan pedig 7 (modulo 10), ugyanis mindkettőre igaz, hogy ha megszorozzuk 3-mal (a megfelelő módon), akkor 1-et kapunk.

Könnyen belátható, hogy az inverz, ha létezik, mindig egyértelmű: a fenti $\text{lnko}(a, m) \mid b$ feltételben ugyanis most $b = 1$, ezért az inverz akkor és csak akkor létezik, ha $\text{lnko}(a, m) = 1$, ekkor viszont már láttuk, hogy pontosan egy megoldás van. Emeljük ki még egyszer:

4.2. Tétel. *$a \in \mathbb{Z}$ akkor és csak akkor invertálható modulo m, ha a és m relatív prímek.*

Példa. $m = 10$-re invertálható az 1, 3, 7 és 9 (mert 0, 2, 4, 5, 6 és 8 mind osztható 2-vel vagy 5-tel).

4.3. Tétel. *Ha m prímszám, akkor minden $a \not\equiv 0 \pmod{m}$ szám invertálható modulo m.*

Vagyis prímszám modulus esetén $a = 0$ kivételével minden maradék invertálható. Ez megfelel annak, hogy $\mathbb{R}$-ben 0 kivételével minden számmal lehet osztani.

Kis m-ekre itt is működik a kimerítő keresés ("brute force"), azaz hogy végignézzük az összes számot 1-tól $m-1$-ig, és amelyik a-val szorozva 1 maradékot ad, az lesz az inverz.

Nagy m-ekre pedig a lineáris kongruencia megoldásának egyszerűsített változatát használhatjuk:

Moduláris inverz(a, m):

> **Bemenet:** $a \in \mathbb{Z}, m \in \mathbb{N}^+$
> $(g, x_g, y_g) :=$ bővített euklideszi algoritmus(a, m) *(y_g nem kell)*
> **ha** $g \neq 1 \rightarrow$ *nem invertálható*
> **Kimenet:** $x_g \bmod m$

Vagyis ha van inverz, akkor az megegyezik az a-hoz tartozó Bézout-együtthatóval (legalábbis modulo m).

Miért érdekes a moduláris inverz? Például ha sok $3x \equiv b\ (10)$ típusú lineáris kongruenciát szeretnénk megoldani különböző b-kre, akkor elég megoldani $b = 1$-re: $3x \equiv 1\ (10)$, azaz kiszámítani 3 inverzét modulo 10 (ami 7), és akkor a $3 \cdot 7 \equiv 1\ (10)$ kongruenciát megszorozva b-vel megkapjuk a b-s kongruencia megoldását is: $3 \cdot 7b \equiv b\ (10)$, azaz $x \equiv 7b\ (10)$. Általában:

4.4. Tétel. *Ha $a \in \mathbb{Z}$ inverze a^{-1} modulo m, akkor $ax \equiv b \pmod{m}$ megoldása $x \equiv a^{-1}b \pmod{m}$.*

(Ez olyan, mint amikor $\mathbb{R}$-ben az osztást úgy végezzük el, hogy az osztó reciprokával szorzunk.)

A Sage a moduláris inverzet az `inverse_mod()` függvénnyel tudja kiszámítani:

```
sage: inverse_mod(3, 10)
7
sage: inverse_mod(2, 10)
[...]
ZeroDivisionError: inverse of Mod(2, 10) does not exist
```

5. Bankszámlaszámok

A magyar bankszámlaszámok 3×8 vagy 2×8 számjegyből állnak, például:

10402166-50526765-81771006.

Az első 8 számjegy azonosítja a bankot (pontosabban a bankfiókot, amelyből az első három számjegy a bank, lásd [3] és [4]). A többi 16 vagy 8 számjegyet a bank határozza meg az ügyfél azonosítására.

Az elgépelések elkerülése végett a bankszámlaszámoknak teljesíteniük kell a következő szabályt (*ellenőrzőösszeget*): ha a számjegyeket megszorozzuk rendre az $1, 3, 7, 9, 1, 3, 7, 9, \ldots$ számokkal, akkor ezen szorzatok összegének 0-ra kell végződnie. (Pontosabban ennek külön-külön is teljesülnie kell az első 8 és a többi 16 vagy 8 számjegyre, de ezzel most nem foglalkozunk.)

Jelöljük a bankszámlaszám számjegyeit b_i-vel (b_1-től b_{24}-ig, nullákkal kiegészítve, ha 16-jegyű), az ellenőrző szorzókat pedig c_i-vel ($c_1 = 1$, $c_2 = 3$, $c_3 = 7$, $c_4 = 9$, …, $c_{24} = 9$). Ekkor a fenti szabályt a következő kongruenciával írhatjuk fel:

$$\sum_{i=1}^{24} b_i c_i \equiv 0 \pmod{10}.$$

Miért jó ez a szabály, és miért pont az $1, 3, 7, 9$ szorzókat használjuk? Azt szeretnénk, hogy ha az egyik számjegyet elgépeljük, akkor a rossz számlaszám lebukjon az ellenőrzésen. Ha a helyes számjegy b_j volt, az elrontott pedig b'_j, akkor a fenti összegben $b_j c_j$ helyére $b'_j c_j$ került, vagyis az összeg $(b'_j - b_j)c_j$-vel változott. A rossz számlaszám akkor megy át az ellenőrzésen, ha a változás 10-zel osztható, azaz $(b'_j - b_j)c_j \equiv 0 \pmod{10}$. Ha $x := (b'_j - b_j)$ az ismeretlen, akkor ez egy lineáris kongruencia: $c_j x \equiv 0 \pmod{10}$. Ennek nyilván megoldása az $x = 0$, azaz hogy $b'_j = b_j$, tehát hogy a számlaszám helyes. Azt szeretnénk, hogy ezenkívül más megoldása ne legyen. Fent láttuk, hogy az ilyen kongruencia akkor és csak akkor oldható meg *egyértelműen*, ha c_j és 10 relatív prímek. Négy ilyen egyjegyű c_j szám van: 1, 3, 7 és 9, ezekkel a szorzókkal tehát biztosan lebukik egy elrontott számjegy. (Más szorzókkal nem feltétlenül, pl. ha $c_j = 4$ lenne, és egy 3-at elírtunk 8-ra, akkor az összeg változása $(8 - 3) \cdot 4 = 20$ lenne, vagyis nem bukna le az elírás.)

Ennek a módszernek azonban vannak korlátai. Például ha egynél több számjegyet rontunk el, az már nem feltétlenül derül ki (csak 90% eséllyel). Valamint attól, hogy az ellenőrzőösszeg hibás, még nem tudjuk, hogy melyik számjegyet rontottuk el (vagyis ez a módszer *hibadetektáló*, de nem *hibajavító* tulajdonságú). Megjegyzés: ha viszont valahonnan mégis tudjuk, hogy melyik számjegy a hibás, akkor a helyes számjegyet vissza tudjuk állítani egy lineáris kongruencia megoldásával, amely a szorzó (1, 3, 7 vagy 9) miatt egyértelműen megoldható. Ezt használja a bank is, amikor létrehoz egy új számlaszámot: először megalkotja az első 23 számjegyét, majd kiszámítja belőlük az utolsót.

6. Kínai maradéktétel

Most nézzük meg, hogyan lehet egyszerre több kongruenciát megoldani különböző modulusokkal:

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n}, \end{cases}$$

ahol $m, n \in \mathbb{N}^+$, $a, b, x \in \mathbb{Z}$, és x az ismeretlen. Ezt úgy hívjuk, hogy *szimultán kongruenciarendszer*. Azaz ismerjük egy szám maradékát m és n szerint is, és ebből szeretnénk kideríteni a számot.

6.1. Tétel (Kínai maradéktétel [*Chinese remainder theorem (CRT)*])**.**
A fenti szimultán kongruenciarendszernek akkor és csak akkor van megoldása, ha $\text{lnko}(m,n) \mid a-b$*, és ekkor a megoldás egyértelmű modulo* $\text{lkkt}(m,n)$ *(vagyis a megoldások* $\text{lkkt}(m,n)$ *szerint ismétlődnek).*

De ebből még nem tudjuk, hogy hogyan számíthatjuk ki a megoldást.

A fenti szimultán kongruenciarendszer ekvivalens a következő egyenletekkel (a kongruencia és az oszthatóság definíciója alapján – lásd fent a lineáris kongruenciák levezetésénél):

$$um = a - x,$$
$$vn = b - x,$$

ahol $u, v \in \mathbb{Z}$. Ezeket kivonva egymásból egy lineáris diofantikus egyenletet kapunk u-ra és v-re:

$$um - vn = a - b,$$

amelyet már meg tudunk oldani. Ebből könnyen be lehet bizonyítani a fenti tételt, valamint levezethető a megoldás képlete x-re (a levezetést mellőzzük):

Kínai maradéktétel:

Bemenet: $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}^+$, a két kongruencia paraméterei
$(g, u_g, v_g) :=$ bővített euklideszi algoritmus(m, n)
ha $g \nmid a - b \rightarrow$ *nincs megoldás*
Kimenet: $x \equiv (av_g n + bu_g m)/g \pmod{mn/g}$ (megjegyzés: $mn/g = \text{lkkt}(m,n)$)
(vagy: $x \equiv a + (b-a)u_g m/g \pmod{mn/g}$)
(vagy: $x \equiv b + (a-b)v_g n/g \pmod{mn/g}$)

Megjegyzés: ha tudjuk, hogy m és n relatív prímek, akkor a számítás leegyszerűsödik, mert mindig van megoldás, és nem kell leosztani g-vel. Ekkor a közös modulus egyszerűen mn.

1. Példa.

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

A bővített euklideszi algoritmus eredménye 5-re és 7-re: $(1, 3, -2)$, azaz a modulusok relatív prímek. Ilyenkor mindig van megoldás, és $x \equiv 3 \cdot (-2) \cdot 7 + 2 \cdot 3 \cdot 5 \pmod{5 \cdot 7}$, azaz $x \equiv 23 \pmod{35}$.

2. Példa.

$$\begin{cases} x \equiv 1 \pmod 6 \\ x \equiv 3 \pmod 4 \end{cases}$$

A bővített euklideszi algoritmus eredménye 6-ra és 4-re: $(2, 1, -1)$. Mivel $2 \mid 1-3$, ezért van megoldás, mégpedig $x \equiv (1 \cdot (-1) \cdot 4 + 3 \cdot 1 \cdot 6)/2 \pmod{6 \cdot 4/2}$, azaz $x \equiv 7 \pmod{12}$.

3. Példa.

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 3 \pmod 4 \end{cases}$$

Hasonlóan kezdjük, de most $2 \nmid 2 - 3$, ezért nincs megoldás. Ez ránézésre is látható, hiszen a két kongruencia ellentmond egymásnak: az első szerint x páros, a második szerint pedig páratlan.

A kínai maradéktétel nemcsak két, hanem tetszőleges számú kongruenciára megfogalmazható. Ennek a megoldásához a fenti módszert alkalmazzuk többször egymás után: egyszerre mindig csak két kongruenciát oldunk meg, majd az eredményt mint kongruenciát beírjuk a megoldott két kongruencia helyére, és így egy eggyel kevesebb kongruenciából álló rendszert kapunk. Ezt addig folytatjuk, amíg

egyetlen kongruencia marad csak, és akkor az lesz a megoldás. Ha bármelyik lépésben azt kapjuk, hogy nincs megoldás, akkor az egész eredeti szimultán kongruenciarendszernek sincs megoldása.

Nézzünk erre is egy példát: Szun Cu, az ókori kínai matematikus (akiről a tétel a nevét kapta), a következő problémát fogalmazta meg:

> *"Bizonyos dolgok számát nem ismerjük. Ha hármasával számoljuk őket, akkor kettő marad; ötösével számolva három marad; és hetesével számolva kettő. Hány dolog van összesen?"*

Ezt átírva kongruenciákra:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

Először oldjunk meg ebből kettőt. Az utolsó két kongruenciát fent már megoldottuk (1. Példa): $x \equiv 23 \pmod{35}$. Ezt beírva a fenti rendszerbe:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 23 \pmod{35}. \end{cases}$$

Ezt is oldjuk meg: a bővített euklideszi algoritmus 3-ra és 35-re azt adja, hogy $(1, 12, -1)$, és a fenti képletből kijön, hogy $x \equiv 2 \cdot (-1) \cdot 35 + 23 \cdot 12 \cdot 3 \equiv 23 \pmod{105}$.

Sage-ben a kínai maradéktételre a `crt()` függvényt használhatjuk. Két kongruencia esetén csak megadjuk a négy paramétert: `crt(a, b, m, n)`, több kongruencia esetén pedig egy-egy listában adjuk meg a jobb oldalakat és a megfelelő modulusokat: `crt([a, b, ...], [m, n, ...])`. A függvény a legkisebb nemnegatív megoldást adja vissza (a közös modulust nem adja meg). Például:

```
sage: crt(1,3, 6,4)     # a fenti 2. Példa
7
sage: crt(2,3, 6,4)     # a fenti 3. Példa
[...]
ValueError: no solution to crt problem since gcd(6,4) does not divide 2-3
sage: crt([2,3,2], [3,5,7])   # Szun Cu példája
23
```

7. Szerző

Ezt a jegyzetet Uray M. János írta, részben felhasználva az alábbi forrásokat:

[1] https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa

[2] https://en.wikipedia.org/wiki/Modular_arithmetic

[3] Bankszámlaszámok felépítése: 35/2017. (XII. 14.) MNB rendelet, 1. melléklet

[4] Bankkódok, bankfiókkódok (a bankszámlaszámok első nyolc számjegye): https://www.mnb.hu/penzforgalom/a-hazai-penzforgalmi-infrastruktura/hitelesito-tabla

[5] https://en.wikipedia.org/wiki/Chinese_remainder_theorem

Hibákat, észrevételeket itt lehet jelezni: uray.janos@inf.elte.hu.