Moduláris aritmetika

Számelmélet

Diszkrét modellek alkalmazásai

1. Maradékosztályok

1.1. Definíció. Az $a \in \mathbb{Z}$ és $b \in \mathbb{Z}$ számok *kongruensek modulo* $m \in \mathbb{N}^+$, ha $m \mid a - b$.
Jelölés: $a \equiv b \pmod{m}$, vagy röviden $a \equiv b\ (m)$. Tagadás jelölése: $a \not\equiv b \pmod{m}$.
További elnevezések: az m neve *modulus*, az $a \equiv b \pmod{m}$ állítás pedig egy *kongruencia*.
Például $34 \equiv 14 \pmod{10}$, 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 $a, b \in \mathbb{N}$ esetén). Általában belátható, hogy $a \equiv b \pmod{m}$ pontosan akkor igaz, ha a és b m-mel való osztási maradéka megegyezik, azaz $a \bmod m = b \bmod m$. (Megjegyzés: a "mod"-nak két különböző jelentése van: az $a \bmod m$ kifejezésben a maradékos osztás maradékát jelenti, pl. $34 \bmod 10 = 4$, az $a \equiv b \pmod{m}$ kifejezésben pedig a teljes "egyenletre" (kongruenciára) vonatkozik a mod, a fent leírtak alapján.)
A kongruencia ($\equiv$) mint reláció 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: $\forall a, b, c \in \mathbb{Z} : a \equiv b\ (m) \wedge b \equiv c\ (m) \implies a \equiv c\ (m)$.

A fenti három tulajdonság miatt azt mondjuk, hogy a kongruencia *ekvivalenciareláció* (lásd pl. Diszkrét matematika I). Azt is tudjuk, hogy egy ekvivalenciareláció meghatározza az alaphalmaz egy osztályfelbontását. Az $a \equiv b \pmod{m}$ kongruencia a következő osztályokra bontja fel $\mathbb{Z}$-t:

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

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:

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

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

Például $m = 5$ esetén $\overline{3} = \{5k + 3 \mid k \in \mathbb{Z}\}$. Az $\overline{a}$ definíciója értelmes, mert minden $a \in \mathbb{Z}$ pontosan egy maradékosztályban van benne. Viszont a jelölés nem egyértelmű, például $\overline{3} = \overline{8} = \overline{28} = \overline{-2}$.

1.3. Definíció. $\mathbb{Z}_m$ az összes m szerinti maradékosztály halmaza, azaz $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}$.

(Vigyázat: $\mathbb{Z}_m \not\subseteq \mathbb{Z}$, sőt, $\mathbb{Z}_m$ elemei nem is számok, hanem halmazok (maradékosztályok). Azaz például $\overline{2} \neq 2$, de $2 \in \overline{2}$. Ez a különbségtétel a műveleteknél fontos lesz.)

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

1.4. Definíció. Egy egész számokból álló halmazt, amely minden maradékosztályból pontosan egy elemet (*reprezentást*) tartalmaz, *teljes maradékrendszer*nek nevezzük.

Minden m-re több (végtelen sok) teljes maradékrendszer van. Például $m = 5$-re a következők mind teljes maradékrendszerek: $\{0, 1, 2, 3, 4\}$, $\{1, 2, 3, 4, 5\}$, $\{-2, -1, 0, 1, 2\}$, $\{10, 6, -3, 23, -6\}$ stb. Minden teljes maradékrendszernek pontosan m eleme van. Az egyik leggyakrabban használt teljes maradékrendszer: $\{0, 1, 2, \ldots, m-1\}$.

2. Moduláris aritmetika

Gyakran szeretnénk egész számokkal úgy számolni, hogy csak a számítás maradéka érdekel bennünket (egy rögzített m-re). Például ha most 18 óra van, akkor 10 órával később nem 28 óra lesz, hanem $28 \bmod 24 = 4$ óra.

Ezt úgy formalizálhatjuk, hogy maradékosztályokkal számolunk. De hogyan végzünk számtani műveleteket halmazok között? Nézzük például az összeadást: két halmazt úgy adunk össze, hogy az egyik halmaz minden eleméhez hozzáadjuk a másik halmaz minden elemét, és az eredményt betesszük egy halmazba. Például ha $A = \{3, 5\}$ és $B = \{10, 20\}$, akkor $A + B = \{13, 15, 23, 25\}$. Belátható, hogy ha két maradékrendszert így összeadunk, akkor egy másik maradékrendszert kapunk, például $\{24k + 18 \mid k \in \mathbb{Z}\} + \{24k + 10 \mid k \in \mathbb{Z}\} = \{24k + 4 \mid k \in \mathbb{Z}\}$ (azaz $\overline{18} + \overline{10} = \overline{4}$, ahol $m = 24$). Kivonásra, szorzásra hasonlóan működik a dolog. Tehát:

2.1. Tétel. $\forall m \in \mathbb{N}^+, a, b \in \mathbb{Z}$:

1. $\overline{a} + \overline{b} = \overline{a + b}$,
2. $\overline{a} - \overline{b} = \overline{a - b}$,
3. $\overline{a} \cdot \overline{b} = \overline{ab}$,
4. $-\overline{a} = \overline{-a}$.

Például ha $m = 10$, akkor $\overline{7} + \overline{3} \cdot \overline{6} = \overline{7} + \overline{8} = \overline{5}$. Ha ugyanezt számokkal szeretnénk kiszámolni, akkor vegyünk minden lépés után maradékot: $(7 + 3 \cdot 6) \bmod 10 = (7 + (3 \cdot 6 \bmod 10)) \bmod 10 = (7 + 8) \bmod 10 = 5$. Lehetne csak a legvégén venni maradékot, de a folyamatos maradékképzésnek az az előnye, hogy menet közben mindig csak kisebb számokkal kell számolni.

A $\mathbb{Z}_m$-beli műveletek főbb tulajdonságai (hasonlóan $\mathbb{Z}$-hez):

1. kommutatív (+ és $\cdot$): $\forall \overline{a}, \overline{b} \in \mathbb{Z}_m : \overline{a} + \overline{b} = \overline{b} + \overline{a} \ \wedge \ \overline{a}\overline{b} = \overline{b}\overline{a}$;
2. asszociatív (+ és $\cdot$): $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m : \overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c} \ \wedge \ \overline{a}(\overline{b}\overline{c}) = (\overline{a}\overline{b})\overline{c}$;
3. disztributív ($\cdot$ a +-ra): $\forall \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m : \overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{a}\overline{c}$;
4. nullával: $\forall \overline{a} \in \mathbb{Z}_m : \overline{a} + \overline{0} = \overline{a} \ \wedge \ \overline{a} \cdot \overline{0} = \overline{0}$;
5. eggyel: $\forall \overline{a} \in \mathbb{Z}_m : \overline{a} \cdot \overline{1} = \overline{a}$;
6. ellentett: $\forall \overline{a} \in \mathbb{Z}_m : \overline{a} + \overline{-a} = \overline{0}$.

Sage-ben többféleképpen számolhatunk modulárisan. Lehet egyszerű maradékképzésekkel:

```
sage: (7 + (3*6)%10) % 10
5
```

Vagy használhatjuk a $\mathbb{Z}_m$ struktúrát, amelyet a `Zmod(m)` függvénnyel lehet létrehozni:

```
sage: Zmod(10)
Ring of integers modulo 10
sage: Z10 = Zmod(10)
sage: Z10(3)       # a "3" egész számot konverálja 3 maradékosztályává
3
sage: Z10(3) * 6   # a másikat már automatikusan konvertálja
8
sage: 7 + Z10(3) * 6
5
sage: type(Z10(3))
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
sage: type(3)
<class 'sage.rings.integer.Integer'>
```

Fel is sorolhatjuk a $\mathbb{Z}_m$ elemeit a szokásos módon:

```
sage: for a in Zmod(4):
....:     print(a, a^2)
0 0
1 1
2 0
3 1
```

Egy másik megoldás maradékosztály létrehozására a `mod(a, m)` függvény, amellyel nem kell külön létrehozni $\mathbb{Z}_m$-et, és amely ugyanazt a számítást végzi el, mint az `a % m`, csak nem egész számot ad vissza, hanem a megfelelő maradékosztályt:

```
sage: mod(34, 10)
4
sage: _ ^ 2
6
sage: type(mod(34, 10))
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
sage: type(34 % 10)
<class 'sage.rings.integer.Integer'>
```

3. Lineáris kongruenciák

Egy fontos művelet eddig kimaradt: az osztás. Vajon lehet-e $\mathbb{Z}_m$-ben osztani, és ha igen, hogyan? Naivan azt gondolhatnánk, hogy itt is ugyanúgy járhatunk el, mint az összeadás, kivonás és szorzás esetén, azaz például $m = 10$ esetén $\overline{6}/\overline{2} = \overline{3}$ lenne, és például $\overline{8}/\overline{3}$ nem létezik. Ez azonban nem ilyen egyszerű. Sőt, mind a két állítás hamis!

Ehelyett inkább induljunk ki abból, hogy mit jelent az osztás máshol, pl. $\mathbb{Z}$-ben: az osztás nem más, mint a szorzás inverze, azaz ha $a, b \in \mathbb{Z}$, akkor b/a azt az egyértelmű $x \in \mathbb{Z}$ számot jelenti, amelyre $ax = b$. Például:

- $6/2 = 3$, mert $2 \cdot 3 = 6$, és az $x = 3$-on kívül nincs más ilyen szám;
- $8/3$ nem létezik $\mathbb{Z}$-ben, mert nincs olyan $x \in \mathbb{Z}$, hogy $3x = 8$ (egyébként $\mathbb{Q}$-ban lenne);
- $5/0$ sem létezik, mert $0x = 0 \neq 5$;
- $0/0$ pedig azért nem létezik, mert bár van olyan x, hogy $0x = 0$, de nem egyértelmű (sőt, minden x ilyen).

Alkalmazzuk az osztásnak ezt a megközelítését $\mathbb{Z}_m$-re:

3.1. Definíció. $\overline{a}, \overline{b} \in \mathbb{Z}_m$ esetén $\overline{b}/\overline{a}$ az az egyérelmű $\overline{x} \in \mathbb{Z}_m$, amelyre $\overline{ax} = \overline{b}$.

Például $m = 10$ esetén tekintsük a következő szorzási táblázatot (az egyes sorokban az elemek, a kétszereseik és a háromszorosaik vannak):

```
sage: matrix([[b*x for x in Zmod(10)] for b in Zmod(10) if b >= 1 and b <= 3])
[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]
```

Ebből például látható, hogy:

- a $\overline{3}\overline{x} = \overline{8}$ egyenletnek pontosan egy megoldása van (a harmadik sorban egy 8-as van): $\overline{3} \cdot \overline{6} = \overline{8}$, azaz $\overline{8}/\overline{3} = \overline{6}$ (ezt $\mathbb{Z}$-ből nézve nem vártuk volna);
- sőt, bármilyen $\overline{b}/\overline{3}$ létezik, hiszen a harmadik sorban minden elem pontosan egyszer szerepel;
- a $\overline{2}\overline{x} = \overline{6}$ egyenletnek viszont *két* megoldása is van: $\overline{2} \cdot \overline{3} = \overline{6}$ (ezt vártuk) és $\overline{2} \cdot \overline{8} = \overline{6}$, tehát $\overline{6}/\overline{2}$ nem létezik modulo 10!

Hogyan tudjuk a moduláris osztást elvégezni hatékonyan, azaz táblázat ($= m$ elem végigpróbálása) nélkül? Ehhez írjuk fel a definícióban szereplő $\overline{ax} = \overline{b}$ egyenletet kongruenciaként: $ax \equiv b \pmod{m}$, és először ezt próbáljuk meg megoldani.

3.2. Definíció. Az $ax \equiv b \pmod{m}$ kongruenciát, ahol x az ismeretlen, *lineáris kongruenciá*nak nevezzük.

A kongruencia definíciójából $ax \equiv b \pmod{m} \iff m \mid b - ax$, vagyis (az osztó definíciójából) $\exists y \in \mathbb{Z} : my = b - ax$, átrendezve: $ax + my = b$. Tehát csak meg kell oldani egy lineáris diofantikus egyenletet, és elég csak x-re. Tudjuk (lásd az előző jegyzetet: Legnagyobb közös osztó), hogy ennek akkor és csak akkor van megoldása, ha $\operatorname{lnko}(a, m) \mid b$, és ha x_0 egy megoldás x-re, akkor végtelen sok megoldás van, amelyek az $x = x_0 - k \cdot m/\operatorname{lnko}(a, m)$ alakban írhatók fel, ahol k tetszőleges egész szám. A kongruenciához azonban elég az $x \in \{0, 1, \ldots, m-1\}$ halmazra leszűkíteni a megoldásokat, ahol már csak véges sok van. Egészen pontosan hány darab? Ezt abból tudjuk kiszámítani, hogy a megoldások lépésköze $m/\operatorname{lnko}(a, m)$, tehát 0-tól $m-1$-ig pontosan $\operatorname{lnko}(a, m)$ darab megoldás van.

Tehát az $ax \equiv b \pmod{m}$ kongruenciát így oldhatjuk meg:

1. Számítsuk ki a bővített euklideszi algoritmussal $g := \operatorname{lnko}(a, m)$-et és az ehhez tartozó x_0, y_0 Bézout-együtthatókat (pontosabban elég csak x_0-t).
2. Ha $\operatorname{lnko}(a, m) \nmid b$, akkor nincs megoldás.
3. Egyébként pontosan $\operatorname{lnko}(a, m)$ darab megoldás van 0 és $m-1$ között:
   (a) Az első megoldás $x_0 \cdot b/g \bmod m/g$.
   (b) Minden következő megoldás az előzőnél m/g-vel nagyobb.

Például a $2x \equiv 6 \pmod{10}$ lineáris kongruencia esetén $g = \text{lnko}(2, 10) = 2$, és a Bézout-együttható $x_0 = 1$ (és $y_0 = 0$). Mivel $\text{lnko}(2, 10) \mid 6$, 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).

Most térjünk vissza a $\overline{b}/\overline{a}$ osztáshoz. Ez annyiban különbözik a lineáris kongruencia megoldásától, hogy a megoldásnak egyértelműnek kell lennie. Ez a fentiek alapján a következőt jelenti:

3.3. Tétel. *A $\overline{b}/\overline{a}$ hányados (modulo m) akkor és csak akkor létezik, ha a és m relatív prím (azaz $\text{lnko}(a, m) = 1$).*

A $\overline{b}/\overline{a}$ kiszámítása tehát:

1. Számítsuk ki a bővített euklideszi algoritmussal $\text{lnko}(a, m)$-et és az a-hoz tartozó x_0 Bézout-együtthatót.
2. Ha $\text{lnko}(a, m) \neq 1$, akkor nincs megoldás.
3. Egyébként a megoldás $x_0 \cdot b \bmod m$.

Például $\overline{8}/\overline{3}$ (modulo 10) esetén $\text{lnko}(3, 10) = 1$ és $x_0 = -3$, tehát van megoldás, mégpedig $\overline{x} = \overline{-3} \cdot \overline{8} = \overline{6}$.

Az osztásnak van egy hasznos speciális esete, ha $\overline{b} = \overline{1}$:

3.4. Definíció. Az $\overline{a}$ maradékosztály (modulo m) *multiplikatív inverze* $\overline{1}/\overline{a}$. Jelölés: $\overline{a}^{-1}$. Ha ez létezik, azt mondjuk, hogy $\overline{a}$ *invertálható*.

Ez azért hasznos, mert ha sok $\overline{b}/\overline{a}$ hányadost számolunk ugyanazzal az $\overline{a}$-val, akkor elég $\overline{a}^{-1}$-et egyszer kiszámítani:

3.5. Tétel. *$\overline{b}/\overline{a}$ pontosan akkor létezik, ha $\overline{a}$ invertálható, és akkor $\overline{b}/\overline{a} = \overline{b} \cdot \overline{a}^{-1}$.*

Mint láttuk, pontosan azok az elemek invertálhatók, amelyek relatív prímek m-hez. Bizonyos m-ek esetén ez leegyszerűsíti a helyzetet:

3.6. Tétel. *Ha m prímszám, akkor minden $\overline{a} \in \mathbb{Z}_m \setminus \{\overline{0}\}$ elem invertálható.*

Tehát, prímszám modulus esetén $\overline{0}$ kivételével bármivel lehet osztani (akárcsak pl. $\mathbb{Q}$-ban).

Természetesen mindezt a Sage is ki tudja számítani:

```
sage: Z10 = Zmod(10)
sage: Z10(8) / 3
6
sage: Z10(6) / 2
...
ZeroDivisionError: inverse of Mod(2, 10) does not exist
sage: Z10(3).inverse()
7
sage: _ * 3
1
```

Kongruenciákat a `solve_mod()` függvénnyel lehet megoldani:

```
sage: solve_mod(2*x == 6, 10)
[(8,), (3,)]
sage: (_[0][0] * 2, _[1][0] * 2)
(6, 6)
```

4. Kínai maradéktétel

Végezetül 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 ha ismerjük egy szám maradékát m és n szerint is, akkor mi lehet maga a szám?

4.1. Tétel (Kínai maradéktétel)**.** *A fenti szimultán kongruenciarendszernek akkor és csak akkor van megoldása, ha* $\text{lnko}(m, n) \mid b - a$*, és ekkor a megoldás egyértelmű modulo* $\text{lkkt}(m, n)$ *(tehát a megoldások halmaza éppen egy maradékosztály modulo* $\text{lkkt}(m, n)$*).*

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):

$$x - a = um,$$

$$x - b = vn,$$

ahol $u, v \in \mathbb{Z}$. Ezekből x-et kiküszöbölve egy lineáris diofantikus egyenletet kapunk u-ra és v-re:

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

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

A megoldás menete tehát:

1. Számítsuk ki a bővített euklideszi algoritmussal $g := \text{lnko}(m, n)$-et és az ehhez tartozó u_0, v_0 Bézout-együtthatókat.
2. Ha $g \nmid b - a$, akkor nincs megoldás.
3. Egyébként a megoldás: $x \equiv (av_0n + bu_0m)/g \pmod{mn/g}$. (Megjegyzés: $mn/g = \text{lkkt}(m, n)$.)

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.

Első 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 $x \equiv 23 \pmod{35}$.

Második 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 $2 \mid 3-1$, ezért van megoldás, mégpedig $x \equiv (1 \cdot (-1) \cdot 4 + 3 \cdot 1 \cdot 6)/2 \pmod{6 \cdot 4/2}$, azaz $x \equiv 7 \pmod{12}$.

Harmadik példa:

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

Hasonlóan kezdjük, de most $2 \nmid 3 - 2$, ezért nincs megoldás. Ez ránézésre is nyilvánvaló, 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 nincs 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 már fent megoldottuk (első 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 $x \equiv 23 \pmod{105}$.
Sage-ben a `crt()` ("Chinese remainder theorem") függvény tud megoldani szimultán kongruenciarendszereket. Ezt kétféleképpen lehet használni: ha csak két kongruencia van, akkor megadhatjuk a négy paramétert egymás után: `crt(a, b, m, n)`, tetszőleges számú kongruencia esetén pedig két listát kell megadni, elsőben a kongruenciák jobb oldalait, a másodikban pedig a megfelelő modulusokat: `crt([a, b, ...], [m, n, ...])`. Az eredmény az egyik megoldás egész számként (a közös modulust nem adja meg). Például:

```
sage: crt(1,3, 6,4)   # a fenti második példa
7
sage: crt(2,3, 6,4)   # a fenti harmadik 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
```

5. Szerző

Ezt a jegyzetet Uray M. János írta, részben felhasználva Nagy Ádám jegyzetét:
https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa
Hibákat, észrevételeket itt lehet jelezni: uray.janos@inf.elte.hu.