A kínai maradéktétel és alkalmazása

A kínai maradéktétel legalább 2000 éves, erről számos számelméleti könyvben olvashatunk.

Az utóbbi időben a tételt a nagy számokkal végzett számításokra kidolgozott algoritmusokban alkalmazzák eredményesen, de számos elemi aritmetikai feladat épül a szóban forgó tételre. Íme erre egy egyszerű példa:

1. feladat

Ha néhány gyereket párosával állítunk sorba, akkor egy gyerek marad a sor végén, ha hármasával, akkor pedig kettő. Hányan maradnak a sor végén, ha hatosával állítjuk őket sorba?

1. megoldás

Legyen *M* a gyerekek száma. A feltételek alapján egy időben igaz, hogy $M = 2 \cdot x + 1$ és $M = 3 \cdot y + 2$, ahol $x, y \in \mathbb{N}^*$. Ezek alapján $3M = 6x + 3$ és $2M = 6y + 4$, ahonnan kivonással kapjuk, hogy

$$M = 6(x - y) - 1 = 6(x - y - 1) + 5,$$

ami azt jelenti: ha hatosával állítjuk sorba a gyermekeket (amennyiben több mint 6 gyerek van), akkor a sor végén 5 gyermek marad.

2. megoldás

Az előző megoldás eredményeit használva tulajdonképpen a $2x + 1 = 3y + 2 \Leftrightarrow \quad \Leftrightarrow 2x - 3y = 1$ diofantoszi egyenletet kell megoldanunk a természetes számok halmazán.

Könnyen belátható, hogy $x_0 = 2$ és $y_0 = 1$ egy partikuláris megoldás. Ezért a $2x - 3y = 1$ egyenlet egész megoldásai

$x = b \cdot n + x_0 = -3n + 2$ és $y = -a \cdot n + y_0 = -2n + 1$, ahol $n \in \mathbb{Z}$**.**

Bevezetve a $-n = m$ jelölést, $x = 3m + 2$ és $y = 2m + 1$ adódik, és jelen esetben $m \in \mathbb{N}$ kell hogy legyen.

Tehát $M = 2x + 1 = 3y + 2 = 2(3m + 2) + 1 = 3(2m + 1) + 2 = 6m + 5$, vagyis válaszunk ugyanaz, mint az előző megoldás esetén.

Könnyen belátható, hogy ha az 1. feladat esetén kettőnél több feltétel (adat) lenne, akkor sem az 1. megoldás, sem a 2. megoldás nem lenne értékesíthető.

Ezért általánosabb megoldási módszerekre van szükségünk. Erre szolgál az ún. kínai maradéktétel. Mielőtt azonban bemutatnánk a kínai maradéktételnek egy elemi változatát, szükségünk van néhány számelméleti alapfogalomra és eredményre.

Értelmezés. Az *a* és *b* természetes számok legkisebb közös többszörösének nevezzük azt az $M := [a, b]$ természetes számot, amelynek a következő tulajdonságai vannak:

1) $a \mid M$ és $b \mid M$;

2) bármely más olyan M' természetes szám esetén, amelyre $a \mid M'$ és $b \mid M'$ is teljesül, következik, hogy $M \mid M'$.

1. segédtétel. Bármely *x* természetes szám esetén, ha az $m_1, m_2 \in \mathbb{N}^*$ számokra igaz, hogy $m_1 \mid x$ és $m_2 \mid x$, akkor $M = [m_1, m_2] \mid x$.

Bizonyítás

Feltételezzük az ellenkezőjét: $M \nmid x$. Ekkor $x = q \cdot M + r$, ahol $q, r \in \mathbb{N}$ és $0 < r < M$, tehát $r \neq 0$.

Mivel $m_1 \mid x$, ezért $m_1 \mid q \cdot M + r$, de $m_1 \mid M$, így $m_1 \mid r$. (1)

Mivel $m_2 \mid x$, ezért $m_2 \mid q \cdot M + r$, de $m_2 \mid M$, így $m_2 \mid r$. (2)

Az előző értelmezés 2) feltétele, valamint az $m_1 \mid r$ és $m_2 \mid r$ alapján kell hogy teljesüljön $M \mid r$, ami lehetetlen, hiszen $0 < r < M$. Tehát a feltétel hamis, ezért $r = 0$ kell hogy legyen, így $M \mid x$.

2. segédtétel. Az m_1, m_2, ..., m_k szám $[m_1, m_2, .., m_k] = M$ legkisebb közös többszörösét a következőképpen határozzuk meg:

$[m_1, m_2] := M_2$; $[M_2, m_3] := M_3$; $[M_3, m_4] := M_4, \ldots, [M_{k-1}, m_k] := M_k$, ahol M_k éppen *M*-mel egyenlő.

Bizonyítás

Az m_1 és m_2 számok közös többszörösei megegyeznek M_2 többszöröseivel. Így az m_1 és m_2 többszörösei, valamint az m_3 többszörösei közül kiválasztjuk a

legkisebb közös többszöröst, ami annyit jelent, mint az M_2 többszörösei és az m_3 többszörösei közül kiválasztani a legkisebb közös többszöröst, az M_3-at, és így tovább, eljárásunk véges számú lépés után éppen az *M*-et adja meg.

3. segédtétel. Bármely $x, m_1, m_2, .., m_k \in \mathbb{N}^*$ esetén, ha $m_1 \mid x,\ m_1 \mid x,\ ..,\ m_k \mid x$, akkor

$$M = [m_1, m_2, .., m_k] \mid x \text{ minden } k \in \mathbb{N}^* \setminus \{1\} \text{ esetben.}$$

Bizonyítás

Az 1. segédtétel és a 2. segédtétel alapján felírható, hogy:

$m_1 \mid x$ és $m_2 \mid x \Rightarrow M_2 = [m_1, m_2] \mid x$,

$M_2 \mid x$ és $m_3 \mid x \Rightarrow M_3 = [M_2, m_3] \mid x$,

.....

$M_{k-1} \mid x$ és $m_k \mid x \Rightarrow M = [M_{k-1}, m_k] \mid x$, amit bizonyítani akartunk.

Következmény. Ha az $m_1, m_2, .., m_k$ páronként relatív prím, és mindegyikük osztja az *x*-et, akkor $m_1 m_2 .. m_k \mid x$.

Bizonyítás

Az állítás nyilvánvaló, hiszen ha az $m_1, m_2, .., m_k$ páronként relatív prím, akkor $M = [m_1, m_2, .., m_k] = m_1 m_2 ... m_k$, és alkalmazzuk a 3. segédtételt.

Megjegyzés. Ha az $m_1, m_2, .., m_k$ páronként nem relatív prím, akkor az előbbi állítás nem igaz. Íme egy ellenpélda: 2 | 12, 4 | 12 és 6 | 12, de a $2 \cdot 4 \cdot 6 \mid 12$ hamis.

A kínai maradéktétel

Legyen $c_1, c_2, ..., c_k$ és $m_1, m_2, ..., m_k$ nullától különböző egész szám és $m_1, m_2, ..., m_k$ páronként relatív prím. Akkor

(a) létezik egy olyan $x \in \mathbb{Z}$ szám, amelyre egy időben igaz, hogy:

$$m_1 \mid x - c_1,\ m_2 \mid x - c_2, ...,\ m_k \mid x - c_k \text{; (*)}$$

(b) az előző oszthatóságokat teljesítő *x* megoldások

$$x = x_0 + m_1 m_2 ... m_k \cdot t \text{ alakúak, (**)}$$

ahol $t \in \mathbb{Z}$ tetszőleges és x_0 a (*) oszthatóságok egy tetszőleges (úgynevezett partikuláris) megoldása.

Bizonyítás

A tételre létezik induktív bizonyítás, de számunkra értékesebb egy konstruktív bizonyítás, mert így az egyes feladatok megoldása során algoritmikusan alkalmazható. A következő, konstruktív bizonyítást lépésekre bontva mutatjuk be.

1) Legyen $M_i = \frac{m_1 m_2 .. m_k}{m_i}$ minden $i \in \{1,\ 2,\ ...,\ k\}$ esetén.

2) Nyilvánvaló, hogy $(M_i, m_i) = (m_1 m_2 .. m_{i-1} m_{i+1} .. m_k, m_i) = 1$, hiszen $m_1, m_2, .., m_k$ páronként relatív prím. Ugyanakkor belátható, hogy $m_i \mid M_j$ minden $i \neq j$ és $i, j \in \{1,\ 2,\ ...,\ k\}$ esetén.

3) Mivel $(M_i, m_i) = 1$, ezért az előző paragrafus 1. tétele alapján az $M_i \cdot y - m_i \cdot z = c_i$ egyenletnek minden $i \in \{1, 2, .., k\}$ esetén van egész megoldása. Legyen rendre (y_i, z_i) az előző egyenletek egy-egy partikuláris megoldása minden $i \in \{1, 2, .., k\}$ esetén. Tehát $M_i y_i - m_i z_i = c_i$ minden $i \in \{1, 2, ..., k\}$ értékre.

(1)

4) Képezzük az $x_0 := M_1 y_1 + M_2 y_2 + ... + M_k y_k$ összeget.

(2)

(a) Igazoljuk, hogy minden $i \in \{1, 2, .., k\}$ esetén $m_i \mid x_0 - c_i$.

Valóban, $x_0 - c_i \overset{(2)}{=} \sum_{\substack{j=1 \\ i \neq j}}^{k} M_j y_i + (M_i y_i - c_i) \overset{(1)}{=} m_i z_i + \sum_{\substack{j=1 \\ j \neq i}}^{k} M_j y_i \ \vdots\ m_i$, hiszen $m_i \mid M_j$ minden $i \neq j,\ i, j \in \{1, 2, .., k\}$ esetén.

Tehát x_0 valóban megoldása a (*) oszthatóságoknak.

(b) Igazoljuk, hogy az $x = x_0 + m_1 m_2 .. m_k \cdot t$ alakú számok megoldásai a (*) oszthatóságoknak. Ez igaz, hiszen
$x - c_i = x_0 + m_1 m_2 .. m_k \cdot t - c_i = (x_0 - c_i) + m_1 m_2 .. m_k \cdot t \ \vdots\ m_i$ minden $i \in \{1, 2, .., k\}$ esetén, hiszen $x_0 - c_i \vdots m_i$ is igaz.

Most azt igazoljuk, ha az *x* a (*) oszthatóságnak megoldása, akkor $x = x_0 + m_1 m_2 ... m_k \cdot t$ alakú. Valóban, hiszen $m_i \mid x - c_i$ és $m_i \mid x_0 - c_i \Leftrightarrow x - c_i = \alpha_i m_i$ és $x_0 - c_i = \beta_i m_i$ minden $i \in \{1, 2, .., k\}$ esetén $(\alpha_i, \beta_i \in \mathbb{Z}^*)$.

Tehát $x - x_0 = (\alpha_i - \beta_i) \cdot m_i$, vagyis $m_i \mid x - x_0$ minden $i \in \{1, 2, .., k\}$ esetén. A 3. Segédtétel következménye értelmében, mivel $m_1, m_2, .., m_k$ páronként relatív prímek és mind osztják az $x - x_0$ különbséget, ezért $m_1 m_2 .. m_k \mid x - x_0$, vagyis létezik $t \in \mathbb{Z}$, amelyre igaz, hogy $x - x_0 = m_1 m_2 .. m_k \cdot t \Leftrightarrow x = x_0 + m_1 m_2 .. m_k \cdot t$.

Ezzel a tételt bizonyítottuk.

Megjegyzés. Észrevehető, hogy a $c_1 = c_2 = ... = c_k = 0$ esetén a kínai maradéktétel éppen a 3. segédtétel következményére redukálódik, de ezt éppen a maradéktétel bizonyításakor használtuk. Ezért kellett ezt másképpen bizonyítanunk, és így a kínai maradéktétel a $c_1 = c_2 = ... = c_k = 0$ esetben is igaz.

2. feladat

Oldjuk meg az 1. példát a kínai maradéktétel segítségével, és próbáljunk arra is választ adni, hogy hányan lehettek a gyermekek!

Megoldás

Jelölje *x* a gyermekek számát. A feladat szövege alapján olyan pozitív *x*-et keresünk, amelyre egy időben igaz, hogy

$$2 \mid x - 1 \text{ és } 3 \mid x - 2 .$$

A kínai maradéktétel bizonyítási algoritmusát követve rendre felírható:

1) $m_1 = 2$ és $m_2 = 3$ relatív prím, és $c_1 = 1$, $c_2 = 2$.

2) $M_1 = \frac{m_1 m_2}{m_1} = 3$ és $M_2 = \frac{m_1 m_2}{m_2} = 2$.

3) Képezzük az $M_i y - m_i z = c_i$ diofantoszi egyenleteket:

$$3y - 2z = 1, \text{ illetve } 2y - 3z = 2 .$$

Észrevehető, hogy egy-egy partikuláris megoldásuk:

$$y_1 = 3 \text{ és } z_1 = 4, \text{ illetve } y_2 = 4 \text{ és } z_2 = 2 .$$

4) A feladat egy partikuláris megoldása tehát:

$$x_0 = M_1 y_1 + M_2 y_2 = 3 \cdot 3 + 2 \cdot 4 = 17 .$$

5) A feladat általános megoldása (lásd a (**) képletet):
$x = x_0 + m_1 m_2 t = 17 + 6t = 6t + 12 + 5 = 6(t+2) + 5 := 6n + 5$, ahol ezúttal $n \in \mathbb{N}^*$.

Tehát a csapatban 11, 17, 23,… gyermek lehetett, akiket hatosával állítva sorba, a sor végén 5 gyermek marad.

Megjegyzés. A feladatra bemutatott három megoldás alapján könnyen eldönthető, hogy *k* = 2 esetén a kínai maradéktétel nem rövidebb, mint a 2. megoldásnál az $ax + by = c$ típusú egyenlet megoldása. Mi több, *k* = 2 esetén kényelmesebb ez utóbbit használni, mert ekkor az $(m_1, m_2) = d \neq 1$ esetben is választ tudunk adni.

3. feladat (kínai feladat, **Szung Csi** oldotta meg először kb. 350 körül)
Melyik az a szám, amelyet 3-mal, 5-tel, illetve 7-tel osztva maradékul 2-t, 3-at, illetve 2-t kapunk?

Megoldás

Olyan $x \in \mathbb{Z}$ számot keresünk, amelyre egy időben igaz, hogy:

$$3 \mid x-2 \ ; \ 5 \mid x-3 \ ; \ 7 \mid x-2 \, .$$

1) $m_1 = 3, \ m_2 = 5, \ m_3 = 7$ páronként relatív prím, $c_1 = 2, \ c_2 = 5, \ c_3 = 2$.

2) $M_1 = \frac{m_1 m_2 m_3}{m_1} = 35$; $M_2 = \frac{m_1 m_2 m_3}{m_2} = 21$; $M_3 = \frac{m_1 m_2 m_3}{m_3} = 15$.

3) Képezzük az $M_i y - m_i z = c_i$ egyenleteket minden $i \in \{1, 2, 3\}$ esetén:

$35y - 2z = 2$, illetve $21y - 5z = 3$, illetve $15y - 7z = 2$,

amelyeknek egy-egy partikuláris megoldása:
$y_1 = 1, \ z_1 = 11$, illetve $y_2 = 3, \ z_2 = 12$, illetve $y_3 = 2, \ z_3 = 4$.

4) A feladat egy partikuláris megoldása:
$$x = x_0 + m_1 m_2 m_3 t = 128 + 105t = 105t + 105 + 23 = 105(t+1) + 23 \, ,$$

vagyis $x = 105n + 23$, ahol $n \in \mathbb{Z}$.

4. feladat
Melyek azok a négyjegyű természetes számok, amelyeket ha rendre 5-tel, 6-tal, 7-tel, 11-gyel osztunk, rendre a 4, 5, 6, 10 maradékot kapjuk?

Megoldás

Olyan $x \in \mathbb{N}^*$ számokat keresünk, amelyekre

$$5 \mid x-4 \ ; \ 6 \mid x-5 \ ; \ 7 \mid x-6 \ \text{ és } \ 11 \mid x-10 \, .$$

A feladat a kínai maradéktétellel is megoldható (ezt az érdeklődő Olvasóra bízzuk), azonban érdemes a feladat sajátosságára felfigyelni, és ezt kiaknázni.

Az oszthatósági feltétel alapján:

$$x-4=5t_1 \ ; \ x-5=6t_2 \ ; \ x-6=7t_3 \ \text{ és } \ x-10=11t_4 \ \ (t_1,t_2,t_3,t_4 \in \mathbb{N}^*).$$

Ezért $x+1=5(t_1+1);\ x+1=6(t_2+1);\ x+1=7(t_3+1)$ és $x+1=11(t_4+1)$, vagyis $x+1$ oszthatóak az 5, 6, 7, 11 páronként relatív prím számokkal, ezért a 3. segédtétel következménye (ami a kínai maradéktétel sajátos esete) alapján igaz, hogy $5\cdot 6\cdot 7\cdot 11=2130 \mid x+1$, vagyis $x+1=2310t$, illetve $x=2310t-1 \, (t \in \mathbb{N}^*)$.

Mivel csak négyjegyű számokat keresünk, így csak a $t \in \{1,\ 2,\ 3,\ 4\}$ értékek felelnek meg, amelyekre

$$x \in \{2309,\ 4619,\ 6929,\ 9239\} \, .$$

5. feladat

Egy matematikust megkérdeztek, hogy mikor született, ő a következőket válaszolta: „Ha születési évszámomat rendre 5-tel, 7-tel, 9-cel és 11-gyel osztod el, rendre a 3, 4, 5 és 6 maradékot kapod”. Mikor született a matematikus?

Megoldás

Olyan $x \in \mathbb{N}$ számot keresünk, amelyre

$$5 \mid x-3;\ 7 \mid x-4;\ 9 \mid x-5 \ \text{ és } \ 11 \mid x-6.$$

A feladat ezúttal is megoldható a kínai maradéktétel segítségével, de ezúttal is a feladat egy sajátosságára figyelünk fel.

Az oszthatósági feltételek alapján:

$$x-3=5t_1;\ x-4=7t_2;\ x-5=9t_3 \ \text{ és } \ x-6=11t_4 \ \ (t_1,t_2,t_3,t_4 \in \mathbb{N}^*).$$

Ezért $2x-1=5(2t_1+1)$; $2x-1=7(2t_2+1)$; $2x-1=9(2t_3+1)$ és $2x-1=11(2t_4+1)$, vagyis $2x-1$ osztható az 5, 7, 9 és 11 páronként relatív prímszámok mindegyikével, ezért a 3. segédtétel következménye alapján

$$3465=5\cdot 7\cdot 9\cdot 11 \mid 2x-1 \, ,$$

ami azt jelenti, hogy $2x-1=3465(2t+1)=2\cdot 3465t+3465$, ahonnan. $x=3465n+1733, \ \ n \in \mathbb{N}$. Mivel születési évszámról van szó, ezért csak $n=0$ felel meg; a matematikus 1733-ban született.

6. feladat (Hindu feladat, **Brahmagupta**, 588-660?, művéből származik.)

Egy kofa tojásokat vitt a piacra eladni. Egy figyelmetlen járókelő felborította a tojásokkal teli kosarat. Illendő viselkedéssel azonnal meg is kérdezte, hogy hány tojás volt a kosárban, mert kifizeti. A kofa ezt válaszolta:

– Nem tudom, hány tojás volt a kosárban, ellenben tudom, hogy ha ezeket akár 2-esével, 3-asával, 4-esével, 5-ösével vagy 6-osával venném ki a kosárból, mindig 1 tojás maradna, de ha 7-esével venném ki, akkor egy sem maradna a kosárban.

Szegény járókelő bizony volt mit töprengjen, amíg kiszámította, hogy hány tojást is kell kifizetnie.

Próbáljatok segíteni a járókelőnek!

Megoldás

Legyen *x* a kosárban levő tojások száma. Erre egy időben igaz, hogy: $2 \mid x-1$; $3 \mid x-1$; $4 \mid x-1$; $5 \mid x-1$; $6 \mid x-1$ és $7 \mid x$.

Azonban a 2, 3, 4, 5, 6, 7 számok páronként nem mind relatív prímek, így nem alkalmazható azonnal a kínai maradéktétel.

Mivel a 2, 3, 4, 5, 6 számok mindegyike osztja az $(x-1)$-et, ezért a 3. segédtétel alapján

$$60 = [2, 3, 4, 5, 6] \mid x-1 .$$

Tehát ezúttal olyan *x*-et keresünk, amelyre

$$60 \mid x-1 \text{ és } 7 \mid x ,$$

ahol ezúttal a 60 és a 7 relatív prím, tehát alkalmazható a kínai maradéktétel (még akkor is, ha $c_2 = 0$, lásd a tétel utáni megjegyzést).

Sorra írjuk fel a lépéseket:

1) $m_1 = 60$ és $m_2 = 7$; $c_1 = 1$ és $c_2 = 0$.

2) $M_1 = \frac{m_1 m_2}{m_{11}} = 7$ és $M_2 = \frac{m_1 m_2}{m_2} = 60$.

3) Képezzük az $M_i y - m_i z = c_i$ diofantoszi egyenleteket:

$$7y - 60z = 1 \text{, illetve } 60y - 7z = 0 ,$$

amelyeknek egy-egy partikuláris megoldása:

$$y_1 = 43,\ z_1 = 5 \text{, illetve } y_2 = 7,\ z_2 = 60 .$$

4) A kitűzött feladat egy partikuláris megoldása:

$$x = x_0 + m_1 m_2 t = 721 + 420t = 420(t+1) + 301 .$$

Tehát $x = 420n + 301$, ahol $n \in \mathbb{N}$, vagyis $x \in \{301,\ 721,\ 1141,\ ...\}$.

Mivel nem valószínű, hogy a kofa elbírt 721 tojást (vagy többet), ezért minden bizonnyal, a kosárban 301 tojás lehetett.

Általánosítási lehetőségek kapcsán

Az érdeklődő Olvasóban természetesen felmerülhet a kérdés, hogy mit állíthatunk abban az esetben, ha a kínai maradéktételben az $m_1, m_2, .., m_k$ szám nem relatív prím?

Könnyen belátható, hogy ilyen esetekben nem is biztos, hogy van megoldás. Például nem található olyan $x \in \mathbb{Z}$ érték, amelyre $2 \mid x-1$ és $4 \mid x-2$, hiszen $x-1$ és $x-2$ egymás utáni számok, ezért az egyik páratlan szám.

A megoldhatóság érdekében vizsgáljuk előbb a $k=2$ esetet, vagyis az

$$m_1 \mid x-c_1 \text{ és } m_2 \mid x-c_2$$

oszthatóságot, ahol ezúttal $(m_1, m_2) \neq 1$.

Az 1. feladat 2. megoldásának a gondolatmenetét követve felírható:

$$m_1 \mid x-c_1 \Leftrightarrow x-c_1 = m_1 x_1 \text{ és } m_2 \mid x-c_2 \Leftrightarrow x-c_2 = m_2 x_2, \text{ ahonnan}$$

$$m_1 x_1 - m_2 x_2 = c_2 - c_1, \qquad (*)$$

ahol $x_1, x_2 \in \mathbb{Z}$. Az előző paragrafus 1. tétele értelmében a (*) egyenlet akkor és csak akkor oldható meg az egész számok halmazán, ha $(m_1, m_2) \mid c_2 - c_1$. Ekkor a megoldás

$$x = m_1 m_2 \cdot t + m_1 \cdot x_1^0 + c_1 = m_1 m_2 \cdot t + m_2 x_2^0 + c_2,$$

ahol $t \in \mathbb{Z}$ és x_1^0, x_2^0 a (*) egyenlet egy partikuláris megoldása.

Tehát a $k=2$ esetben a feltett kérdésre a válasz egyszerű. Ez a válasz ötletet adhat arra, hogy $k>3$ esetén is megválaszoljuk a kérdést.

1. tétel. Adott $k \in \mathbb{N}^* \setminus \{1\}$ esetén legyenek $c_1, c_2, ..., c_k$ és $m_1, m_2, .., m_k$ egész számok. Az

$$m_1 \mid x-c_1;\ m_2 \mid x-c_2;\ ...;\ m_k \mid x-c_k$$

oszthatóságnak akkor és csak akkor van $x \in \mathbb{Z}$ megoldása, ha

$$(m_i, m_1) \mid c_j - c_i \text{ minden } 1 \leq i < j \leq k \text{ esetén.}$$

Amennyiben x_0 egy partikuláris megoldás, úgy az

$$x = x_0 + [m_1, m_2, .., m_k] \cdot t,\ t \in \mathbb{Z}$$

a feladat összes megoldását szolgáltatja.

Bizonyítás

A tétel egy induktív bizonyítását a szakirodalomban [37] számmal jelölt könyv 515. lapján olvashatjuk. Az induktív bizonyítás hátránya, hogy nem ad konkrét módszert arra, hogy miként keressünk egy x_0 partikuláris megoldást.

7. feladat

Egy juhásznak kevesebb, mint 200 juha van. Ha 3-asával, 4-esével, 5-ösével, illetve 6-osával számolja meg őket, rendre 1, 2, 3, illetve 4 juh marad. Hány juha van összesen?

Megoldás

Olyan $x \in \mathbb{N}$ számot keresünk, amelyre egy időben igaz, hogy:

$$3 \mid x-1;\ 4 \mid x-2;\ 5 \mid x-3 \ \text{ és } \ 6 \mid x-4.$$

Tehát $c_1 = 1,\ c_2 = 2,\ c_3 = 3,\ c_4 = 4$ és $m_1 = 3,\ m_2 = 4,\ m_3 = 5,\ m_4 = 6$. Mivel az $m_1, m_2,\ m_3, m_4$ páronként nem mind relatív prím, előbb ellenőrizzük, hogy teljesülnek-e a tételben leírt, a megoldáshoz szükséges és elégséges feltételek:

$3 \mid x-1$ és $6 \mid x-4$ esetén $(3, 6) = 3 \mid (-1+4) = 3$ igaz,

$4 \mid x-2$ és $6 \mid x-4$ esetén $(4, 6) = 2 \mid (-2+4) = 2$ igaz.

Tehát a feladatnak van egész megoldása. Amennyiben észrevesszük, hogy $x_0 = -2$ esetén

$$3 \mid -2-1;\ 4 \mid -2-2;\ 5 \mid -2-3 \ \text{ és } \ 6 \mid -2-4$$

éppen egy partikuláris megoldás, akkor, mivel [3, 4, 5, 6] = 60, az 1. tétel alapján a feladat összes megoldása: $x = 60t - 2,\ t \in \mathbb{N}$. Mivel a juhásznak 200-nál kevesebb juha van, ezért $t \in \{1,\ 2,\ 3\}$ esetén a juhok lehetséges száma: $x \in \{58,\ 118,\ 178\}$.

A kínai maradéktétel egy másik általánosítása a következő:

2. tétel. Adott $k \in \mathbb{N}^* \setminus \{1\}$ esetén legyen $a_1, a_2, ..., a_k;\ c_1, c_2, ..., c_k;\ m_1, m_2, ..., m_k$ olyan egész szám, amelyre $(a_i, m_i) = 1$ és $(m_i, m_j) = 1$ minden $i \neq j$, i és $j \in \{1, 2, ..., k\}$ esetén. Ekkor az

$$m_1 \mid a_1 x - c_1;\ m_2 \mid a_2 x - c_2;\ ...;\ m_k \mid a_k x - c_k$$

oszthatóságoknak közös egész megoldásuk van, és az általános megoldást az

$$x = x_0 + m_1 m_2 ... m_k \cdot t$$

összefüggés szolgáltatja, ahol $t \in \mathbb{Z}$ és x_0 egy partikuláris megoldás.

Bizonyítás

A kínai maradéktétel bizonyításakor leírtakat kissé módosítva átültethetjük a jelen esetre is. Ezúttal azonban az $M_i y - m_i z = c_i$ egyenletek helyett az $a_i M_i y - m_i z = c_i$ egyenleteket képezzük. Az $(a_i, m_i) = (M_i, m_i) = 1$ feltételek miatt, az utóbbi egyenleteknek van egész megoldásuk. Könnyen ellenőrizhető, hogy $x = M_1 y_1 + M_2 y_2 + ... + M_k y_k$ tényleg megoldása az oszthatóságoknak.

Továbbá a kínai maradéktétel (*b*) pontja is enyhén módosul: Az $x = x_0 + m_1 m_2 ... m_k \cdot t$ valóban megoldása az oszthatóságoknak, hiszen:

$$a_i x - c_i = a_i (x_0 + m_1 m_2 ... m_k \cdot t) - c_i = (a_i x_0 - c_i) + a_i m_1 m_2 ... m_k \cdot t,$$

és így $x - c_i \vdots m_i$ minden $i \in \{1,\ 2,...,\ k\}$ esetén. Az is belátható, hogy minden egész megoldás $x = x_0 + m_1 m_2 ... m_k \cdot t$ alakú. Mivel $a_i x - c_i \ \vdots \ m_i$ és $a_i x_0 - c_i \ \vdots \ m_i$, ezért $a_i x - c_i = m_i \alpha_i$ és $a_i x_0 - c_i = m_i \beta_i$ $(\alpha_i, \beta_i \in \mathbb{Z}^*$ és $i \in \{1,\ 2,...,\ k\})$. Tehát $a_i (x - x_0) = m_i (\alpha_i - \beta_i)$, ezért $m_i \mid a_i (x - x_0)$. De $(a_i, m_i) = 1$, következik, hogy

$m_i \mid x - x_0$ minden $i \in \{1,\ 2,\ldots,\ k\}$ esetén, ezért $m_1 m_2 \ldots m_k \mid x - x_0$, vagyis $x - x_0 = m_1 m_2 \ldots m_k \cdot t$, tehát $x = x_0 + m_1 m_2 \ldots m_k \cdot t$, ahol $t \in \mathbb{Z}$.

8. feladat

Egy egész szám háromszorosát 4-gyel osztva a maradék 1, a kétszeresét 5-tel osztva a maradék 3, az ötszörösét 7-tel osztva a maradék 2, a hétszeresét 9-cel osztva a maradék 8. Melyik ez a szám?

Megoldás

Olyan $x \in \mathbb{Z}$ számot keresünk, amelyre egy időben teljesül:

$$4 \mid 3x - 1;\ 5 \mid 2x - 3;\ 7 \mid 5x - 2 \ \ és \ \ 9 \mid 7x - 8.$$

A kínai maradéktétel lépéseit követjük az előbbi tétel módosításai szerint:

1) $a_1 = 3;\ a_2 = 2;\ a_3 = 5;\ a_4 = 7;$

$c_1 = 1;\ c_2 = 3;\ c_3 = 2;\ c_4 = 8;$

$m_1 = 4;\ m_2 = 5;\ m_3 = 7;\ m_4 = 9;$

$(a_1, m_1) = (a_2, m_2) = (a_3, m_3) = (m_1, m_2) = (m_2, m_3) = (m_3, m_1) = 1$ teljesül.

2)

$$M_1 = \frac{m_1 m_2 m_3 m_4}{4} = 315; M_2 = \frac{m_1 m_2 m_3 m_4}{5} = 252; M_3 = \frac{m_1 m_2 m_3 m_4}{7} = 180; M_4 = \frac{m_1 m_2 m_3 m_4}{9} = 140.$$

3) A 2. tétel alapján képezzük az $a_i M_i y - m_i z = c_i$ egyenleteket:

$$945y - 4z = 1;\ 504y - 5z = 3;\ 900y - 7z = 2 \ \ és \ \ 980y - 9z = 8.$$

Ezeknek egy-egy partikuláris megoldása rendre:

$y_1 = 1$ és $z_1 = 236$; $y_2 = 2$ és $z_2 = 201$; $y_3 = 4$ és $z_3 = 514$; $y_4 = 1$ és $z_4 = 108$.

4) A feladat egy partikuláris megoldása:

$$x_0 = M_1 y_1 + M_2 y_2 + M_3 y_3 + M_4 y_4 = 315 + 504 + 720 + 140 = 1697.$$

5) Ugyancsak a 2. tétel alapján a feladat általános megoldása:

$x = x_0 + m_1 m_2 m_3 m_4 t = 1697 + 1260t = 1260(t+1) + 419$, vagyis $x = 1260n + 419$, ahol $n \in \mathbb{Z}$.

Befejezésül megjegyezzük, hogy a jelen paragrafusban tárgyalt problémák az úgynevezett lineáris kongruenciák témakörébe tartoznak, ellenben ebben a paragrafusban csak az elemi megközelítéséről írtunk, csupán elemi eszközök segítségével.