Haladvány Kiadvány 2007.03.31.

Hujter Mihály: **Százhuszonhárom éves feladat, I.**

(Készült a T047340 számú OTKA részbeni támogatásával)

Tekintsünk pozitív egész számokat, összesen n darabot, ahol n is pozitív egész. A számokat jelölje $a_1, a_2, ..., a_n$. Az egyszerűbb írásmód kedvéért használjuk az $a_1 = a$, $a_2 = b$, $a_3 = c$ jelöléseket is. Jelölje továbbá A az $a_1, a_2, ..., a_n$ számok alkotta halmazt. Nyilván A elemeinek darabszáma — amit $|A|$ jelöléssel illetünk — legalább 1 és legfeljebb n. Ebben a dolgozatban az A halmazról mindig feltesszük, hogy az elemei *relatív prímek*. Mit is jelent ez? Egy lehetséges értelmezés a következő: $|A| = 1$ esetén akkor és csak akkor relatív prímek az A halmaza elemei, ha $A = \{1\}$. Ha $|A| \geq 2$ és $1 \in A$, akkor is relatív prímek az A halmaz elemei. Ha pedig $|A| \geq 2$ és $1 \notin A$, akkor az A halmaz elemeinek relatív prím mivoltát úgy ellenőrizzük, hogy az A halmazból csinálunk egy A^- halmazt a következő módon, aztán akkor és csak akkor tekintjük az A halmaz elemeit relatív prímnek, ha az A^- halmaz elemei is relatív prímek. Jelölje $a_{\max}$ az A halmaz legnagyobb elemét és jelölje $a_{\min}$ a legkisebbet. Az A halmazból úgy készítjük az A^- halmazt, hogy kivesszük A-ból az $a_{\max}$ elemet, és betesszük helyette az $a_{\max} - a_{\min}$ számot. (Ha már eleve benn volt a halmazban, az sem baj.)

A most ismertetett módszer az A halmaz elemei relatív prím mivoltának ellenőrzésére lényegében a jól ismert *Euklideszi algoritmus*.

Az $|A| = 1$ esetben nem sok érdekeset mondhatunk az A halmazról. Az $|A| = 2$ eset már egyáltalán nem ilyen triviális! Tehát most a és b relatív prímek. Százhuszonhárom éve bizonyította be Sylvester és Curran Sharp a következő tételt:

1. Tétel (*Sylvester–Curran Sharp*, 1884) Ha a, b pozitív egészek és relatív prímek, akkor a legnagyobb egész szám, mely nem áll elő $ax + by$ alakban nemnegatív egész x-szel és y-nal a következő: $ab - a - b$.

A tétel szemléltetésére álljon itt egy példa: Ha egy pénzváltó dollárt és eurót vált forintra; csak egész összegeket hajlandó váltani; egy dollárért 193 forintot, egy euróért 247 forintot ad, akkor a $193 \cdot 247 - 193 - 247 = 47\,231$ összeg felett minden egész számot kifizethet forintban, de a 47 231 forint pénzösszeget nem

fizetheti ki. Ez az állítás természetesen azon a felismerésen alapul, hogy 193 és 247 relatív prímek, mely tényről a következő levezetés győz meg minket:

$$\begin{aligned}
\{193, 247\} &\rightarrowtail \{193, 247 - 193\} = \{54, 193\} \\
\{54, 193\} &\rightarrowtail \{54, 193 - 54\} = \{54, 139\} \\
\{54, 139\} &\rightarrowtail \{54, 139 - 54\} = \{54, 85\} \\
\{54, 85\} &\rightarrowtail \{54, 85 - 54\} = \{31, 54\} \\
\{31, 54\} &\rightarrowtail \{31, 54 - 31\} = \{23, 31\} \\
\{23, 31\} &\rightarrowtail \{23, 31 - 23\} = \{8, 23\} \\
\{8, 23\} &\rightarrowtail \{8, 23 - 8\} = \{8, 15\} \\
\{8, 15\} &\rightarrowtail \{8, 15 - 8\} = \{7, 8\} \\
\{7, 8\} &\rightarrowtail \{7, 8 - 7\} = \{1, 7\} \\
\{1, 7\} &\rightarrowtail \{1, 6\} \rightarrowtail ... \rightarrowtail \{1, 2\} \rightarrowtail \{1\}
\end{aligned}$$

Az 1. tételt konstruktívan fogjuk bizonyítani. Ez azt jelenti, hogy nemcsak azt fogjuk megmutatni, hogy $ab - a - b$ nem áll elő $ax + by$ alakban nemnegatív egész x-szel és y-nal, hanem azt is, hogy hogyan lehet ténylegesen előállítani egy tetszőleges, $N > ab - a - b$ számot.

Az 1. tétel bizonyítása: Az általánosság korlátozása nélkül feltehetjük, hogy $a \leq b$. Ha $a = b$, akkor a és b relatív prím mivoltából csak az $a = b = 1$ eset lehetséges. Ilyenkor $ab - a - b = -1$. Valóban, minden nemnegatív egész N szám előáll $ax + by$ alakban például $x = N$, $y = 0$ választással. A továbbiakban feltehetjük tehát, hogy $a < b$. Az $a = 1$ eset is nagyon könnyű, hiszen ilyenkor $ab - a - b = -1$, és ugyanúgy, mint az előbb, minden nemnegatív egész N szám előáll $ax + by$ alakban például $x = N$, $y = 0$ választással. A továbbiakban feltehetjük tehát, hogy $1 < a < b$. Ilyen esetekre egy indirekt bizonyítást fogunk adni.

Tegyük fel, hogy van ellenpélda a tétel állítására. Tekintsük azt az ellenpédát, melyre $a < b$ és b a lehető legkisebb. Ha több ellenpélda is van ezen legkisebb b számmal, akkor tekintsük azt az ellenpéldát ezek közül, ahol a értéke a lehető legnagyobb. Rögzítsük tehát ezeket az a és b számokat. Képezzük a $\beta = b - a$ számot. Mivel az a és β számok pozitívak, relatív prímek és közülük a nagyobbik is kisebb, mint b, az 1. tétel állítása igaz az a és β számokra. Tehát a legnagyobb egész szám, mely nem áll elő $ax + \beta y$ alakban nemnegatív egész x-szel és y-nal, pontosan $a\beta - a - \beta = a(b - a) - b$. Minden ennél nagyobb egész szám előáll tehát $ax + \beta y$ alakban nemnegatív egész x-szel és y-nal, sőt még azt is feltehetjük, hogy $y < a$, mert $y \geq a$ esetén az $a(x + \beta) + \beta(y - a)$ alakú előállítás is jó lenne.

Most tekintsünk egy tetszőleges $N > ab - a - b$ egész számot. Meg fogjuk mutatni, hogy ez előáll $ax + by$ alakban nemnegatív egész x-szel és y-nal. Elegendő csak az olyan N számokkal foglalkoznunk, melyekre $N \leq ab - b$, mert ha $N > ab - b$, és ha $N - a$ előáll $ax + by$ alakban nemnegatív egész x-szel és y-nal, akkor $N = a(x + 1) + by$.

Tehát $ab - a - b < N \leq ab - b$. Mivel

$$(ab - a - b) - (a(b - a) - b) = a(a - 1)$$

ezért $a(b-a)-b < N - a(a-1)$; következésképpen $N - a(a-1)$ előáll $ax + \beta y$ alakban nemnegatív egész x-szel és y-nal, azaz

$$\begin{aligned} N &= a(a-1) + ax + \beta y \\ &= a(a-1) + ax + (b-a)y \\ &\quad a(a - 1 + x - y) + by \end{aligned} \tag{1}$$

Tekintettel arra, hogy még azt is feltehettük, hogy $y \leq a - 1$, megkaptuk az N szám egy alkalmas előállítását, hiszen $a - 1 + x - y \geq x$.

Abból indultunk ki, hogy a tétel állítása nem érvényes. De a fentiekben tetszőleges $N > ab - a - b$ egész számot előállítottunk, tehát csak akkor nem lehet $ab - a - b$ a legnagyobb szám, ami nem áll elő $ax + by$ alakban nemnegatív egész x-szel és y-nal, ha maga $ab - a - b$ is előáll $ax + by$ alakban nemnegatív egész x-szel és y-nal. Itt is feltehetjük, hogy $y \leq a - 1$. Úgy fogunk ellentmondásra kilyukadni, hogy előállítjuk az $a\beta - a - \beta$ számot is $ap + \beta q$ alakban valamely nemnegatív egész p-re és q-ra. Tudjuk, hogy

$$\begin{aligned} a\beta - a - \beta &= ab - a - b - a(a-1) \\ &= ax + by - a(a-1) \\ &= ax + (a+\beta)y - a(a-1) \\ &= a(1 + x + y - a) + \beta y \end{aligned} \tag{2}$$

Már csak azt kell megmutatnunk, hogy $1 + x + y - a \geq 0$. De ha ez nem lenne így, akkor

$$1 + x + y - a \leq -1$$

és

$$a(1 + x + y - a) + \beta y \leq -a + \beta y$$

lenne, amiből — (2) miatt —

$$a\beta - a - \beta \leq \beta y - a$$

azaz $a-1 \leq y$ következne. Azonban $a-1 \geq y$, tehát $y = a-1$ és $1+x+y-a = -1$. Ez utóbbi viszont lehetlen, mert $1 + x + (a-1) - a = -1$, azaz $x = -1$ jönne ki. Ezzel az 1. tétel bizonyítása befejeződött. ■

Hogy fenti bizonyítás konstruktív jellegét szemléltethessük, a fenti példán megmutatjuk, hogyan fizethető ki pontosan 50000 forint. Mivel

$$50000 - 47\,231 = 2769 \text{ és } \frac{2769}{193} \approx 14.3$$

ezért elegendő megmutatnunk, hogy

$$50000 - 14 \cdot 193 = 47\,298$$

forint kifizethető. Most

$$\begin{aligned} a &= 193 \\ b &= 247 \\ \beta &= b - a = 247 - 193 = 54 \\ a(a-1) &= 193 \cdot 192 = 37\,056 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 54 forintot érő és 193 forintot érő pénzekkel (mindegyikből természetesen nemnegatív egész szám egységnyit véve) a

$$47\,298 - 37\,056 = 10\,242$$

forintra rúgó pénzösszeg. Mármost

$$\begin{aligned} 54 \cdot 193 - 54 - 193 &= 10\,175 \\ 10\,242 - 10\,175 &= 67 \\ \frac{67}{54} &\approx 1.2 \\ 10\,242 - 1 \cdot 54 &= 10188 \end{aligned}$$

Ezért elegendő 10188 forintot kifizetni 54 és 193 forintot érő pénzegységekkel.

Az új szereposztás a következő:

$$\begin{aligned} a &= 54 \\ b &= 193 \\ \beta &= b - a = 193 - 54 = 139 \\ a(a-1) &= 54 \cdot 53 = 2862 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 54 forintot érő és 139 forintot érő pénzekkel a

$$10188 - 2862 = 7326$$

forint érték. Mármost

$$\begin{aligned} 54 \cdot 139 - 54 - 139 &= 7313 \\ 7326 - 7313 &= 13 \\ \frac{13}{54} &< 1 \end{aligned}$$

Tehát most 7326 forintot kell kifizetni.

Az új szereposztás a következő:

$$\begin{aligned} a &= 54 \\ b &= 139 \\ \beta &= b - a = 139 - 54 = 85 \\ a(a-1) &= 54 \cdot 53 = 2862 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 54 forintot érő és 85 forintot érő pénzekkel a

$$7326 - 2862 = 4464$$

forint érték. Mármost

$$\begin{aligned} 54 \cdot 85 - 54 - 85 &= 4451 \\ 4464 - 4451 &= 13 \\ \frac{13}{54} &< 1 \end{aligned}$$

Tehát most 4464 forintot kell kifizetni.

Az új szereposztás a következő:

$$\begin{aligned} a &= 54 \\ b &= 85 \\ \beta &= b - a = 85 - 54 = 31 \\ a(a-1) &= 54 \cdot 53 = 2862 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 31 forintot érő és 54 forintot érő pénzekkel a

$$4464 - 2862 = 1602$$

forint érték. Mármost

$$\begin{aligned} 31 \cdot 54 - 31 - 54 &= 1589 \\ 1602 - 1589 &= 13 \\ \frac{13}{31} &< 1 \end{aligned}$$

Tehát most 1602 forintot kell kifizetni.

Az új szereposztás a következő:

$$\begin{aligned} a &= 31 \\ b &= 54 \\ \beta &= b - a = 54 - 31 = 23 \\ a(a-1) &= 31 \cdot 30 = 930 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 23 forintot érő és 31 forintot érő pénzekkel a

$$1602 - 930 = 672$$

forint érték. Mármost

$$\begin{aligned} 23 \cdot 31 - 23 - 31 &= 659 \\ 672 - 659 &= 13 \\ \frac{13}{23} &< 1 \end{aligned}$$

Tehát most 672 forintot kell kifizetni.

Az új szereposztás a következő:

$$\begin{aligned} a &= 23 \\ b &= 31 \\ \beta &= b - a = 31 - 23 = 8 \\ a(a-1) &= 23 \cdot 22 = 506 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 8 forintot érő és 23 forintot érő pénzekkel a

$$672 - 506 = 166$$

forint érték. Mármost

$$\begin{aligned} 8 \cdot 23 - 8 - 23 &= 153 \\ 166 - 153 &= 13 \\ \frac{13}{8} &\approx < 1.6 \\ 166 - 1 \cdot 8 &= 158 \end{aligned}$$

Tehát most 158 forintot kell kifizetni.

Az új szereposztás a következő:

$$\begin{aligned} a &= 8 \\ b &= 23 \\ \beta &= b - a = 23 - 8 = 15 \\ a(a-1) &= 8 \cdot 7 = 56 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 8 forintot érő és 15 forintot érő pénzekkel a

$$158 - 56 = 102$$

forint érték. Mármost

$$\begin{aligned} 8 \cdot 15 - 8 - 15 &= 97 \\ 102 - 97 &= 5 \\ \frac{5}{8} &< 1 \end{aligned}$$

Tehát most 102 forintot kell kifizetni.

Az új szereposztás a következő:

$$\begin{aligned} a &= 8 \\ b &= 15 \\ \beta &= b - a = 15 - 8 = 7 \\ a(a-1) &= 8 \cdot 7 = 56 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 7 forintot érő és 8 forintot érő pénzekkel a

$$102 - 56 = 46$$

forint érték. Mármost

$$\begin{aligned} 7 \cdot 8 - 7 - 8 &= 41 \\ 46 - 41 &= 5 \\ \frac{5}{7} &< 1 \end{aligned}$$

Tehát most 46 forintot kell kifizetni.

Az új szereposztás a következő:

$$\begin{aligned} a &= 7 \\ b &= 8 \\ \beta &= b - a = 8 - 7 = 1 \\ a(a-1) &= 7 \cdot 6 = 42 \end{aligned}$$

Azt kell tehát csak megkeresnünk, hogyan fizethető ki 1 forintot érő és 7 forintot érő pénzekkel a

$$46 - 42 = 4$$

forint érték. Mivel már van 1 forintosunk, ki tudjuk fizetni a 4 forintot így:

$$4 = 1 \cdot 4 + 7 \cdot 0$$

Visszafelé haladva az (1) képlet alapján ezeket kapjuk:

$$\begin{aligned} 4 + 42 &= 1 \cdot 4 + 7 \cdot 0 + 7 \cdot 6 = 1 \cdot 4 + 7 \cdot (0 + 6) \\ &= 1 \cdot 4 + 7 \cdot 6 = 1 \cdot 4 + 7 \cdot (4 + 2) \\ &= (1 + 7) \cdot 4 + 7 \cdot 2 = 8 \cdot 4 + 7 \cdot 2 = 46 \end{aligned}$$

$$\begin{aligned} 46 + 56 &= 7 \cdot 2 + 8 \cdot 4 + 8 \cdot 7 = 7 \cdot 2 + 8 \cdot (4 + 7) \\ &= 7 \cdot 2 + 8 \cdot 11 = 7 \cdot 2 + 8 \cdot (2 + 9) \\ &= (7 + 8) \cdot 2 + 8 \cdot 9 = 15 \cdot 2 + 8 \cdot 9 = 102 \end{aligned}$$

$$\begin{aligned} 102+56 &= 15\cdot 2+8\cdot 9+8\cdot 7 = 15\cdot 2+8\cdot (9+7)\\ &= 15\cdot 2+8\cdot 16 = 15\cdot 2+8\cdot (2+14)\\ &= (15+8)\cdot 2+8\cdot 14 = 23\cdot 2+8\cdot 14 = 158 \end{aligned}$$

$$\begin{aligned} 158+8 &= 8\cdot 14+23\cdot 2+8 = 8\cdot (14+1)+23\cdot 2\\ &= 8\cdot 15+23\cdot 2 = 166 \end{aligned}$$

$$\begin{aligned} 166+506 &= 8\cdot 15+23\cdot 2+23\cdot 22 = 8\cdot 15+23\cdot (2+22)\\ &= 8\cdot 15+23\cdot 24 = 8\cdot 15+23\cdot (15+9)\\ &= (8+23)\cdot 15+23\cdot 9 = 31\cdot 15+23\cdot 9 = 672 \end{aligned}$$

$$\begin{aligned} 672+930 &= 23\cdot 9+31\cdot 15+31\cdot 30 = 23\cdot 9+31\cdot (15+30)\\ &= 23\cdot 9+31\cdot 45 = 23\cdot 9+31\cdot (9+36)\\ &= (23+31)\cdot 9+31\cdot 36 = 54\cdot 9+31\cdot 36 = 1602 \end{aligned}$$

$$\begin{aligned} 1602+2862 &= 31\cdot 36+54\cdot 9+54\cdot 53 = 31\cdot 36+54\cdot (9+53)\\ &= 31\cdot 36+54\cdot 62 = 31\cdot 36+54\cdot (36+26)\\ &= (31+54)\cdot 36+54\cdot 26 = 85\cdot 36+54\cdot 26 = 4464 \end{aligned}$$

$$\begin{aligned} 4464+2862 &= 85\cdot 36+54\cdot 26+54\cdot 53 = 85\cdot 36+54\cdot (26+53)\\ &= 85\cdot 36+54\cdot 79 = 85\cdot 36+54\cdot (36+43)\\ &= (85+54)\cdot 36+54\cdot 43 = 139\cdot 36+54\cdot 43 = 7326 \end{aligned}$$

$$\begin{aligned} 7326 + 2862 &= 139 \cdot 36 + 54 \cdot 43 + 54 \cdot 53 = 139 \cdot 36 + 54 \cdot (43 + 53) \\ &= 139 \cdot 36 + 54 \cdot 96 = 139 \cdot 36 + 54 \cdot (36 + 60) \\ &= (139 + 54) \cdot 36 + 54 \cdot 60 = 193 \cdot 36 + 54 \cdot 60 = 10188 \end{aligned}$$

$$10188 + 54 = 193 \cdot 36 + 54 \cdot 60 + 54 = 193 \cdot 36 + 54 \cdot 61 = 10242$$

$$\begin{aligned} 10242 + 37056 &= 54 \cdot 61 + 193 \cdot 36 + 193 \cdot 192 \\ &= 54 \cdot 61 + 193 \cdot (36 + 192) \\ &= 54 \cdot 61 + 193 \cdot 228 \\ &= 54 \cdot 61 + 193 \cdot (61 + 167) \\ &= (54 + 193) \cdot 61 + 193 \cdot 167 \\ &= 247 \cdot 61 + 193 \cdot 167 = 47\,298 \end{aligned}$$

$$\begin{aligned} 47\,298 + 2702 &= 247 \cdot 61 + 193 \cdot 167 + 193 \cdot 14 \\ &= 247 \cdot 61 + 193 \cdot (167 + 14) \\ &= 247 \cdot 61 + 193 \cdot 181 = 50000 \end{aligned}$$

Most vagyunk tehát készen a példával: 50000 forintot 181 dollárként plusz 61 euróként lehet pontosan kifizetni.

Bármennyire is hosszadalmas volt az eljárásunk a konkrét példán, azért a javasolt módszerünk egy hatékony eljárás! Ez azt jelenti, hogy nem lényegesen lassabb, mint a relatív prímség ellenőrzésére szolgáló euklideszi algoritmus.

2. Tétel (a *Sylvester–Curran Sharp*-tétel következménye) Ha $n \geq 3$, továbbá $a_1, a_2, ..., a_n$ pozitív egészek és relatív prímek, akkor létezik olyan legnagyobb egész szám, amely nem áll elő $a_1x_1 + a_2x_2 + ... + a_nx_n$ alakban nemnegatív egész $x_1, x_2, ..., x_n$ számokkal.

Világos, hogy a tétel állításában megengedhetnénk az $n = 1$ és $n = 2$ eseteket is, hiszen az $n = 1$ eset triviális, az $n = 2$ esetet pedig az 1. tétel adja.

A 2. tétel bizonyítása: Az $a_1+a_2+...+a_n$ összeg értéke szerinti teljes indukcióval bizonyítunk. Az $a_1+a_2+...+a_n \leq 2$ eset nyilvánvaló. Akkor is készen vagyunk, ha az

$$\{a_1, a_2, ..., a_n\}$$

halmaz elemeinek száma n-nél kevesebb. Feltehetjük tehát, hogy a halmazban legalább 3 különböző szám van. Jelölje P az $a_1, a_2, ..., a_n$ számok szorzatát. Az indukciós feltevés alapján létezik olyan Q nemnegatív egész szám, hogy az

$$(\{a_1, a_2, ..., a_n\} \setminus \{a_{\max}\}) \cup \{a_{\max} - a_{\min}\}$$

halmaz elemeiből nemnegatív egész y_j együtthatókkal összerakható minden Q-nál nem kisebb egész szám. Most már csak azt kell észrevenni, hogy bármely $S \geq Q + P$ egész szám összerakható nemnegatív egész együtthatókkal a

$$\{a_1, a_2, ..., a_n\}$$

halmazból, mert az $S - P$ számot ki tudjuk rakni a

$$(\{a_1, a_2, ..., a_n\} \setminus \{a_{\max}\}) \cup \{a_{\max} - a_{\min}\}$$

halmazból, sőt azt is feltehetjük, hogy az $a_{\max} - a_{\min}$ számot a $P/a_{\max}$ számnál kisebb együtthatóval kell venni — hiszen $P/a_{\max}$ osztható minden olyan a_i-vel, melyre $a_i \neq a_{\max}$ —, és ha y_0 jelöli az $a_{\max} - a_{\min}$ szám együtthatóját $S - P$ összerakásában, akkor

$$(a_{\max} - a_{\min})\, y_0 = a_{\max} y_0 - a_{\min} y_0$$

és

$$P = a_{\min} \cdot (P/a_{\min}) > a_{\min} \cdot (P/a_{\max})$$

miatt az $(S - P) + P = S$ szám is összeáll nemnegatív egész együtthatókkal a

$$\{a_1, a_2, ..., a_n\}$$

halmazból. Ezzel az 2. tétel bizonyítása befejeződött. ■

Hivatkozások

Curran Sharp,W.J., *Mathematical questions, with their solutions*, Educational Times 41 (1884) 21.

Sylvester,J., *Mathematical questions, with their solutions*, Educational Times, 41 (1884), 21.