Eksplicitno rješenje opće linearne diofantske jednadžbe na jedan drugačiji način

Petar Svirčević[1]

Sažetak. *Ovdje ćemo linearnu diofantsku jednadžbu s n nepoznanica rješavati tako da definiramo $n-1$ parametara i s njima generirati sustav od n linearnih jednadžbi. Matricu sustava podijelimo u blokove i onda invertiramo, ali tako da vrijednost determinante te nove matrice bude jednaka 1. Nakon rješenja matrične jednadžbe jednostavno iščitavamo vrijednosti cjelobrojnih varijabli, koje su funkcije uvedenih $n-1$ parametara. I konačno na kraju dajemo nekoliko zadataka na kojima se navedeno primjenjuje.*

Ovdje ćemo upotrijebiti standardne oznake za skupove; $\mathbb{N}$ je skup prirodnih brojeva, $\mathbb{Z}$ skup cijelih brojeva, $\mathbb{Q}$ skup racionalnih brojeva, $\mathbb{R}$ skup realnih brojeva, $\mathbb{C}$ skup kompleksnih brojeva i $\mathbb{Z}^n$ *Kartezijev produkt* skupova $\mathbb{Z}$, dakle $\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n}$, $n \in \mathbb{N}$.

Nadalje za n cijelih brojeva $a_1, a_2, \ldots, a_n$ različitih od nule, tj. $a_1, a_2, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$, je $M(a_1, a_2, \ldots, a_n)$ najveća zajednička mjera tih brojeva, tj. najveći prirodni broj s kojim je djeljiv svaki od tih zadanih cijelih brojeva.

Definicija 1. Jednadžba

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \tag{1}$$

je *opća linearna diofantska jednadžba*, ili *diofantska jednadžba*, ako je $a_i \in \mathbb{Z} \setminus \{0\}$, $b \in \mathbb{Z}$, gdje su x_i nepoznanice, dok su a_i i b fiksni brojevi za $i = 1, 2, \ldots, n$.

Definicija 2. Jednadžba (1) je *sređena jednadžba* ako je $M(a_1, a_2, \ldots, a_n, b) = 1$ za $b \neq 0$ ili $M(a_1, a_2, \ldots, a_n) = 1$ za $b = 0$.

Definicija 3. Uređena n-torka

$$x^0_{(n)} = (x^0_1, x^0_2, \ldots, x^0_n) \in \mathbb{Z}^n \tag{2}$$

je partikularno rješenje linearne diofantske jednadžbe (1) onda i samo onda ako je $a_1x^0_1 + a_2x^0_2 + \ldots + a_nx^0_n = b$.

Definicija 4. Uređena n-torka

$$(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n \tag{3}$$

je opće rješenje jednadžbe (1) onda i samo onda ako je $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, za sve moguće uređene n-torke s tim svojstvom.

Napomena 1. Kada se radi o diofantskim jednadžbama oblika

$$a_1x_1 + a_2x_2 = b \tag{4}$$

onda se već na standardni način dokazuju teoremi koje ćemo sada navesti.

Teorem 1. *Diofantska jednadžba (4) ima cjelobrojno rješenje, onda i samo onda ako* $M(a_1, a_2) \mid b$.

---

[1] Autor je professor u mirovini na Tehničkoj školi Zagreb; e-pošta: `petar.svircevic@zg.t-com.hr`

Teorem 2. *Ako diofantska jednadžba (4) ima jedno cjelobrojno rješenje* (x_1^0, x_2^0), *onda ona ima beskonačno mnogo cjelobrojnih rješenja.*

Teorem 3. *Ako je* (x_1^0, x_2^0) *bilo koje rješenje jednadžbe (4), onda su sva njena cjelobrojna rješenja* (x_1, x_2) *obuhvaćena formulama*

$$x_1 = x_1^0 - a_2 t, \quad x_2 = x_2^0 + a_1 t, \tag{5}$$

za $\forall t \in \mathbb{Z}$.

U daljnjem razmatranju će biti potrebno partikularno rješenje jednadžbe

$$a_1 x_1 + a_2 x_2 = 1. \tag{6}$$

Kako naći rješenje te jednadžbe ako je $M(a_1, a_2) = 1$? Iz (6) slijedi

$$a_1 x_1 \equiv 1 \pmod{a_2}. \tag{7}$$

Dakle, u (7) se uvrštava redom $x_1 = \pm 1, \pm 2, \ldots$ i prvu vrijednost za koju je to točno označava s x_1^0, a pomoću toga se dobije i cijeli broj $x_2^0 = (1 - a_1 x_1^0)/a_2$, dakle za jednadžbu (6) znamo uvijek naći partikularno rješenje (x_1^0, x_2^0) ako je $M(a_1, a_2) = 1$.

Sada pokušajmo riješiti diofantsku jednadžbu

$$a_1 x_1 + a_2 x_2 = b \tag{8}$$

na drugačiji način. Ako $M(a_1, a_2) \mid b$, tada postoji $\alpha_1, \alpha_2 \in \mathbb{Z}$ tako da je

$$a_1 \alpha_2 - a_2 \alpha_1 = 1, \tag{9}$$

a to je tip jednadžbe (6). Partikularno rješenje od (9) je (α_1^0, α_2^0). Nadalje ako je (x_1, x_2) neko rješenje od (8), tada je

$$\alpha_1^0 x_1 + \alpha_2^0 x_2 = t, \tag{10}$$

gdje je $t \in \mathbb{Z}$. Jednadžbe (8) i (10) čine sustav jednadžbi

$$\left.\begin{array}{rcl} a_1 x_1 + a_2 x_2 &=& b \\ \alpha_1^0 x_1 + \alpha_2^0 x_2 &=& t \end{array}\right\}, \tag{11}$$

a njegovo rješenje je

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ \alpha_1^0 & \alpha_2^0 \end{bmatrix}^{-1} \begin{bmatrix} b \\ t \end{bmatrix}, \tag{12}$$

budući je ovo ***Cramerov sustav***, determinanta sustava je različita od nule, naime,

$$\begin{vmatrix} a_1 & a_2 \\ \alpha_1^0 & \alpha_2^0 \end{vmatrix} = a_1 \alpha_2^0 - a_2 \alpha_1^0 = 1, \tag{13}$$

jer smo uvažili (9). Zbog (13) inverzna matrica ima cjelobrojne elemente, dakle

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \alpha_2^0 & -a_2 \\ -\alpha_1^0 & a_1 \end{bmatrix} \begin{bmatrix} b \\ t \end{bmatrix} \tag{14}$$

ili

$$x_1 = \alpha_2^0 b - a_2 t = \begin{vmatrix} b & a_2 \\ t & \alpha_2^0 \end{vmatrix}, \tag{15a}$$

$$x_2 = -\alpha_1^0 b + a_1 t = \begin{vmatrix} a_1 & b \\ -\alpha_1^0 & t \end{vmatrix}. \tag{15b}$$

Lako se provjeriti da su (15a) i (15b) komponente rješenja od (8), ako se uvaži (9). Nadalje može se dokazati da je to rješenje jedinstveno, uz uvjet da $M(a_1, a_2) \mid b$.

Vratimo se na sređenu diofantsku jednadžbu

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b, \tag{16}$$

gdje je $b \neq 0$ i $M(a_1, a_2, \ldots, a_n, b) = 1$. Ona, zapravo, predstavlja hiperravninu u E^n prostoru, pa točka $T(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ u toj hiperravnini ima $n-1$ stupanj slobode, a to znači da se može proizvoljno izabrati $n-1$ koordinatu te točke, no mogu se naći sve točke na toj hiperravnini čije su koordinate cjelobrojne, pa ćemo njih, odnosno parametre, označiti s $t_1, t_2, \ldots, t_{n-1} \in \mathbb{Z}$. Dakle dobivamo sustav jednadžbi

$$\left.\begin{array}{ccccccccl}
x_1 & & & & & & & = & t_1\\
 & & x_2 & & & & & = & t_2\\
 & & & & \ddots & & & \vdots & \vdots\\
 & & & & & & x_{n-1} & = & t_{n-1}\\
a_1x_1 & + & a_2x_2 & + & \ldots & + & a_{n-1}x_{n-1} + a_nx_n & = & b
\end{array}\right\} \tag{17}$$

Sustav (17) je Cramerov, jer mu je determinanta sustava

$$D = \begin{vmatrix} 1 & 0 & \ldots & 0 & 0\\ 0 & 1 & \ldots & 0 & 0\\ \vdots & \vdots & \ldots & \vdots & \vdots\\ 0 & 0 & \ldots & 1 & 0\\ a_1 & a_2 & \ldots & a_{n-1} & a_n \end{vmatrix} = a_n \neq 0.$$

Ako je

$$D_i = \begin{vmatrix} 1 & 0 & \ldots & 0 & t_1 & 0 & \ldots & 0 & 0\\ 0 & 1 & \ldots & 0 & t_2 & 0 & \ldots & 0 & 0\\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots & \ldots & \vdots & \vdots\\ 0 & 0 & \ldots & 0 & t_{n-1} & 0 & \ldots & 1 & 0\\ a_1 & a_2 & \ldots & a_{i-1} & b & a_{i+1} & \ldots & a_{n-1} & a_n \end{vmatrix},$$

tada su komponente rješenja sustava (17) racionalne i dane s $x_i = D_i/D$, dakle općenito $x_i \notin \mathbb{Z}$ kada D_i nije djeljivo s D za svaki $i = 1, 2, \ldots, n$. Prema tome parametrizacija (17) općenito nije dobra. Moramo postići takvu parametrizaciju da je determinanta sustava $D \equiv 1$, onda će biti $x_i \in \mathbb{Z}$. Prema tome postavljamo parametrizaciju

$$\left.\begin{array}{c}
x_1 = t_1\\
x_2 = t_2\\
\vdots\\
x_{n-2} = t_{n-2}\\
\alpha_{n-1}x_{n-1} + \alpha_nx_n = t_{n-1}\\
a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} + a_nx_n = b
\end{array}\right\}. \tag{18}$$

Neka je determinanta tog sustava

$$D = \begin{vmatrix} 1 & 0 & \ldots & 0 & 0 & 0\\ 0 & 1 & \ldots & 0 & 0 & 0\\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots\\ 0 & 0 & \ldots & 1 & 0 & 0\\ 0 & 0 & \ldots & 0 & \alpha_{n-1} & \alpha_n\\ a_1 & a_2 & \ldots & a_{n-2} & a_{n-1} & a_n \end{vmatrix} = 1,$$

ili

$$D = \begin{vmatrix} \alpha_{n-1} & \alpha_n \\ a_{n-1} & a_n \end{vmatrix}, \tag{19}$$

a zvat ćemo je ***pomoćna diofantska jednadžba*** s nepoznanicama α_{n-1}, α_n. No, da bi ona postojala mora biti

$$M(\alpha_{n-1}, \alpha_n) = 1, \tag{20}$$

dakle ako je

$$M(a_1, a_2, \ldots, a_n) = M(\alpha_{n-1}, \alpha_n) = 1 \tag{21}$$

i

$$a_n\alpha_{n-1} - a_{n-1}\alpha_n = 1, \tag{22}$$

sustav (18) ima rješenje. Već smo pokazali da jednadžba (22) ima rješenje po α_{n-1} i α_n, pa neka je jedno partikularno rješenje $(\alpha_{n-1}^0, \alpha_n^0)$. Što ako je $M(a_{n-1}, a_n) \neq 1$? U tom slučaju mora postojati i i j $(i \neq j)$, tako da je $M(a_i, a_j) = 1$, jer kada to ne bi bilo onda bi dobili $M(a_1, a_2, \ldots, a_n) \neq 1$, a to je kontradikcija, jer $M(a_1, a_2, \ldots, a_n) = 1$ je nužan uvjet da sređena diofantska jednadžba ima rješenje. Dakle, ako je $M(a_{n-1}, a_n) \neq 1$, uvijek možemo preraspodijeliti sumande u (16), tako da za koeficijente zadnja dva sumanda bude $M(a_i, a_j) = 1$.

Na osnovu iznesenog zaključujemo da je za sređenu diofantsku jednadžbu (16) nužan i dovoljan uvjet dan s

$$M(a_1, a_2, \ldots, a_n, b) = 1, \tag{23}$$

a nužan i dovoljan uvjet za parametrizaciju te jednadžbe (odnosno postojanje rješenja), u oblik (18), je

$$M(a_1, a_2, \ldots, a_n) = M(a_{n-1}, a_n) = 1. \tag{24}$$

Očigledno je da se ovi uvjeti o rješivosti i parametrizaciji sređene diofantske jednadžbe mogu prikazati i u obliku implikacije

$$M(a_1, a_2, \ldots, a_n) = 1 \implies \prod_{i,j;i\neq j}^{n} (M(a_i, a_j) - 1) = 0. \tag{25}$$

Pretpostavimo da smo našli α_{n-1}^0 i α_n^0 tako da je $D \equiv 1$, odnosno da je $a_n\alpha_{n-1}^0 - a_{n-1}\alpha_n^0 = 1$, pa sustav (18) možemo pisati u matričnoj formi

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-2} \\ x_{n-1} \\ x_n \end{bmatrix} = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \ldots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 & 0 \\ 0 & 0 & \ldots & 0 & \alpha_{n-1}^0 & \alpha_n^0 \\ a_1 & a_2 & \ldots & a_{n-2} & a_{n-1} & a_n \end{bmatrix}^{-1} \cdot \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n-2} \\ t_{n-1} \\ b \end{bmatrix}. \tag{26}$$

Sada je glavni problem invertiranje matrice sustava. Prije nego što pređemo na to, recimo još kako se invertira matrica rastavljanjem na blokove. Uzmimo da je A kvadratna regularna matrica n-tog reda. Treba naći matricu $B = A^{-1}$ takvu da je

$$AB = BA = I. \tag{27}$$

U tu svrhu matrice A, B i I razbijamo u blokove, tako da (27) poprima oblik

$$\begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \cdot \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} I_1 & O_1 \\ O_2 & I_2 \end{bmatrix}, \tag{28}$$

gdje su I_1 i I_2 jedinične matrice reda m odnosno reda $(n-m)$; O_1 i O_2 su nul-matrice (svi su elementi 0) reda $m \times (n-m)$ odnosno reda $(n-m) \times m$. Lako se vidi da (28) ima smisla ako su A_{11}, B_{11} i I_1 kvadratne matrice istog reda, dakle m, a odatle slijedi da su A_{22}, B_{22}, I_2 kvadratne matrice reda $(n-m)$. Iz (28) se dobivaju sljedeće relacije

$$A_{11}B_{11} + A_{12}B_{21} = I_1, \tag{29}$$

$$A_{11}B_{12} + A_{12}B_{22} = O_1, \tag{30}$$

$$A_{21}B_{11} + A_{22}B_{21} = O_2 \tag{31}$$

$$A_{21}B_{12} + A_{22}B_{22} = I_2, \tag{32}$$

a odatle se lako dobiju veze

$$B_{11} = (A_{11} - A_{12}A_{22}^{-1}A_{21})^{-1}, \tag{33}$$

$$B_{12} = -B_{11}A_{12}A_{22}^{-1}, \tag{34}$$

$$B_{21} = -A_{22}^{-1}A_{21}B_{11}, \tag{35}$$

$$B_{22} = A_{22}^{-1} - A_{22}^{-1}A_{21}B_{12}. \tag{36}$$

Mora se pretpostaviti, da su matrice A_{22} i $A_{11} - A_{12}A_{22}^{-1}A_{21}$ regularne, da bi postupak rješavanja matričnih jednadžbi od (29) do (32) bio moguć. U našem slučaju, kako se vidi iz (26), zgodno je uzeti

$$A_{11} = I_{n-2}, \tag{37}$$

$$A_{12} = O_{n-2,2}, \tag{38}$$

$$A_{21} = \begin{bmatrix} 0 & 0 & \dots & 0 \\ a_1 & a_2 & \dots & a_{n-2} \end{bmatrix}, \tag{39}$$

$$A_{22} = \begin{bmatrix} \alpha_{n-1}^0 & \alpha_n^0 \\ a_{n-1} & a_n \end{bmatrix}. \tag{40}$$

Dakle $B_{11} = (I_{n-2} - O_{n-2,2}A_{22}^{-1}A_{21})^{-1} = I_{n-2}^{-1} = I_{n-2}$,

$$B_{11} = I_{n-2}, \tag{41}$$

$$B_{12} = -I_{n-2}O_{n-2,2}A_{22}^{-1}$$

ili

$$B_{12} = O_{n-2,2}, \tag{42}$$

$$\begin{aligned} B_{21} &= -\begin{bmatrix} \alpha_{n-1}^0 & \alpha_n^0 \\ a_{n-1} & a_n \end{bmatrix}^{-1} A_{21}B_{11} \\ &= -\begin{bmatrix} a_n & -\alpha_n^0 \\ -a_{n-1} & \alpha_{n-1}^0 \end{bmatrix} \begin{bmatrix} 0 & 0 & \dots & 0 \\ a_1 & a_2 & \dots & a_{n-2} \end{bmatrix} I_{n-2} \end{aligned}$$

ili

$$B_{21} = \begin{bmatrix} \alpha_n^0 a_1 & \alpha_n^0 a_2 & \dots & \alpha_n^0 a_{n-2} \\ -\alpha_{n-1}^0 a_1 & -\alpha_{n-1}^0 a_2 & \dots & -\alpha_{n-1}^0 a_{n-2} \end{bmatrix} \tag{43}$$

i konačno $B_{22}=A_{22}^{-1}-A_{22}^{-1}A_{21}O_{n-2,2}$ ili

$$B_{22}=\begin{bmatrix} a_n & -\alpha_n^0 \\ -a_{n-1} & \alpha_{n-1}^0 \end{bmatrix}. \tag{44}$$

Ako se uvaže formule od (41) do (44), tada (26) prima oblik

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-2} \\ x_{n-1} \\ x_n \end{bmatrix}=\begin{bmatrix} 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ \alpha_2^0 a_1 & \alpha_2^0 a_2 & \dots & \alpha_2^0 a_{n-2} & \alpha_n & -\alpha_n^0 \\ -\alpha_1^0 a_1 & -\alpha_1^0 a_2 & \dots & -\alpha_1^0 a_{n-2} & -\alpha_{n-1} & \alpha_{n-1}^0 \end{bmatrix}^{-1}\cdot\begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n-2} \\ t_{n-1} \\ b \end{bmatrix}. \tag{45}$$

Ove rezultate ćemo iskazati u obliku teorema, gdje ćemo u (45) malo drugačije ispisati zadnja dva retka matrice kao produkte skalara i jednorednih matrica, odnosno inverz matrice drugog reda kako se vidi u (46), s time da označavamo jediničnu matricu i matricu nula, a to smo napravili zbog lakšeg pamćenja našeg algoritma, s time da kažemo da za primjenu na računalu moramo koristiti oblik (45) da bi dobili komponente rješenja zadane jednadžbe.

Teorem 4. **(Diofant)** *Dana je sređena opća linearna diofantska jednadžba* $a_1x_1+a_2x_2+\ldots+a_nx_n=b$, *dakle* $M(a_1,a_2,\ldots,a_n,b)=M(a_1,a_2,\ldots,a_n)=1$ $(b\neq 0)$ *i neka je* $M(a_{n-1},a_n)=1$. *Ako to nije, onda se članovi jednadžbe mogu prerasporediti, tako da za zadnja dva koeficijenta to vrijedi. Nadalje,* $(\alpha_{n-1}^0,\alpha_n^0)$ *je partikularno rješenje pomoćne diofantske jednadžbe* $D=\begin{vmatrix} \alpha_{n-1} & \alpha_n \\ a_{n-1} & a_n \end{vmatrix}=1$, *pa je opće rješenje dano s matričnom vezom*

$$\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_{n-2} \\ x_{n-1} \\ x_n \end{bmatrix}=\begin{bmatrix} I_{n-2} & O_{n-2,2} \\ \begin{matrix} \alpha_2^0[a_1\ a_2\ \dots\ a_{n-2}] \\ -\alpha_1^0[a_1\ a_2\ \dots\ a_{n-2}] \end{matrix} & \begin{bmatrix} \alpha_{n-1}^0 & \alpha_n^0 \\ a_{n-1} & a_n \end{bmatrix}^{-1} \end{bmatrix}\begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_{n-2} \\ t_{n-1} \\ b \end{bmatrix} \tag{46}$$

ili respektivno s komponentama

$$\left.\begin{aligned} x_1&=t_1 \\ x_2&=t_2 \\ &\vdots \\ x_{n-2}&=t_{n-2} \\ x_{n-1}&=\alpha_n^0(a_1t_1+a_2t_2+\ldots+a_{n-2}t_{n-2})+a_nt_{n-1}-\alpha_n^0 b \\ x_n&=-\alpha_{n-1}^0(a_1t_1+a_2t_2+\ldots+a_{n-2}t_{n-2})-a_{n-1}t_{n-1}+\alpha_{n-1}^0 b \end{aligned}\right\}. \tag{46a}$$

Napomena 1. Matricu $\begin{bmatrix} \alpha_{n-1}^0 & \alpha_n^0 \\ a_{n-1} & a_n \end{bmatrix}^{-1}$ u (46) nismo invertirali iz mnemotehničkih razloga.

Sada ćemo na nekoliko primjera primijeniti algoritam (46) i (46a).

Zadatak 1. Riješiti diofantsku jednadžbu
$$7x_1 - 5x_2 + 11x_3 + 3x_4 - 2x_5 = 4. \tag{47}$$

Rješenje. Budući je $M(7,-5,11,3,-2) = M(7,-5,11,3,-2,4) = M(3,-2) = 1$, što znači da jednadžba ima rješenje. Lako se pokaže da je $(1,-1)$ partikularno rješenje pomoćne diofantske jednadžbe $\begin{vmatrix} \alpha_4 & \alpha_5 \\ 3 & -2 \end{vmatrix} = 1$. Dakle, $\alpha_4^0 = 1$ i $\alpha_5^0 = -1$, pa ako se te vrijednosti uvrste u (46) slijedi
$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} I_3 & O_{3,2} \\ (-1)[7 \ -5 \ 11] & \begin{bmatrix} 1 & -1 \\ 3 & -2 \end{bmatrix}^{-1} \\ -(+1)[7 \ -5 \ 11] & \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ 4 \end{bmatrix}, \tag{48}$$
ili
$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ -7 & 5 & -11 & -2 & 1 \\ -7 & 5 & -11 & -3 & 1 \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ 4 \end{bmatrix}, \tag{49}$$
gdje to vrijedi za $\forall t_1,\ t_2,\ t_3,\ t_4 \in \mathbb{Z}$. No iz (49) vidi se da se mogu ispisati i komponente rješenja diofantske jednadžbe (47), dakle: $x_1 = t_1$, $x_2 = t_2$, $x_3 = t_3$, $x_4 = -7t_1 + 5t_2 - 11t_3 - 2t_4 + 4$, $x_5 = -7t_1 + 5t_2 - 11t_3 - 3t_4 + 4$. Npr., ako je za specijalni slučaj $t_1 = t_2 = t_3 = t_4 = 1$, tada je $x_1 = x_2 = x_3 = 1$; $x_4 = -11$; $x_5 = -12$; pa se lako provjeri da je $(1,1,1,-11,-12)$ partikularno rješenje zadane jednadžbe. Jasno je da se mogu varirati parametri t_i $(i = 1,2,3,4)$ preko skupa $\mathbb{Z}$ i uvijek će uređena petorka (x_1,x_2,x_3,x_4,x_5) zadovoljavati danu jednadžbu.

Zadatak 2. Riješiti diofantsku jednadžbu
$$3x_1 - 5x_2 + 3x_3 + 9x_4 = 1. \tag{50}$$

Rješenje. Jednadžba je sređena jer je $M(3,-5,3,9,1) = 1$, a ima i rješenje jer je $M(3,-5,3,9) = 1$. No, ne može se direktno parametrizirati zbog, $M(a_{n-1},a_n) = M(3,9) = 3 \neq 1$, već je moramo prerasporediti (postoje i druge mogućnosti). Dakle, neka je
$$3x_3 + 9x_4 + 3x_1 - 5x_2 = 1, \tag{51}$$
pa je $M(3,5) = 1$. Partikularno rješenje pomoćne diofantske jednadžbe $\begin{vmatrix} \alpha_1 & \alpha_2 \\ 3 & -5 \end{vmatrix} = 1$ je $(-2,3)$ dakle $\alpha_1^0 = -2$ i $\alpha_2^0 = 3$. Na osnovu iznesenog matrično rješenje jednadžbe (51) je
$$\begin{bmatrix} x_3 \\ x_4 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} I_2 & O_{2,2} \\ 3[3 \ 9] & \begin{bmatrix} -2 & 3 \\ 3 & -5 \end{bmatrix}^{-1} \\ 2[3 \ 9] & \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ 1 \end{bmatrix}$$
ili
$$\begin{bmatrix} x_3 \\ x_4 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 9 & 27 & -5 & -3 \\ 6 & 18 & -3 & -2 \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ t_3 \\ 1 \end{bmatrix},$$

a odatle su komponente rješenja:

$$x_1 = 9t_1 + 27t_2 - 5t_3 - 3, \quad x_2 = 6t_1 + 18t_2 - 3t_3 - 2, \quad x_3 = t_1, \quad x_4 = t_2. \tag{52}$$

Ako je $t_1 = t_2 = t_3 = 0$, iz (52) slijedi partikularno rješenje $(-3, -2, 0, 0)$. Slično se za $t_1 = t_2 = t_3 = 1$ dobije $(28, 19, 1, 1)$, ili npr. za $t_1 = -1$, $t_2 = 1$, $t_3 = 6$ imamo uređenu četvorku $(-15, -8, -1, 1)$. Svakako, da nužnost točnog rješenja slijedi ako se veze (52) uvrste u (51), a koje zadovoljavaju tu jednadžbu, i onda je pogotovo zadovoljavaju ovi specijalni slučajevi.

Napomena 1. Lagano bi se riješila i homogena $(b = 0)$ opća diofantska jednadžba oblika $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0$, gdje je postupak gotovo isti kao i u prijašnjem slučaju.

Sada ćemo se malo pozabaviti primjenom rješenja opće linearne diofantske jednadžbe na dokazivanje nekih činjenica koje nisu *a priori* jasne.

Zadatak 3. Svaki cijeli broj može se prikazati kao linearna cjelobrojna kombinacija barem dva prosta i međusobno različita broja. (Generalizacija!)

Rješenje. Neka je $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ skup prostih brojeva. Zadatak kaže za $\forall a \in \mathbb{Z}$, gdje je $p_1,\ p_2,\ p_3, \ldots \in \mathbb{P}$, $x_1,\ x_2,\ \ldots,\ x_n \in \mathbb{Z}$ $(n \geq 2)$, vrijedi relacija

$$p_1x_1 + p_2x_2 + \ldots + p_nx_n = a. \tag{53}$$

Budući je $M(p_1, p_2, \ldots, p_n, a) = M(p_1, p_2, \ldots, p_n) = M(p_{n-1}, p_n) = 1$, a to je nužan uvjet da (53) ima rješenje $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$, pa je time tvrdnja zadatka u potpunosti dokazana.

Generalizacija: $p_1^{\alpha_1}x_1 + p_2^{\alpha_2}x_2 + \ldots + p_n^{\alpha_n}x_n = a$, gdje je $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n \in \mathbb{N}$.

Zadatak 4. Na koliko načina možemo posudu od 100 l napuniti posudama od 3 l i 5 l?

Rješenje. Dakle tražimo $x_1,\ x_2 \in \mathbb{N} \cup \{0\}$, tako da je $x_1 \cdot 3\ \mathrm{l} + x_2 \cdot 5\ \mathrm{l} = 100\ \mathrm{l}$, ili jednostavnije

$$3x_1 + 5x_2 = 100. \tag{54}$$

Budući je $M(3, 5, 100) = M(3, 5) = 1$, iz (54) slijedi

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 1 & 2 \end{bmatrix}^{-1} \begin{bmatrix} 100 \\ t \end{bmatrix} = \begin{bmatrix} 2 & -5 \\ -1 & 3 \end{bmatrix} \begin{bmatrix} 100 \\ t \end{bmatrix},$$

ili

$$x_1 = 200 - 5t, \quad x_2 = -100 + 3t. \tag{55}$$

Budući je $x_1,\ x_2 \geq 0$, tada je $200 - 5t \geq 0$ i $-100 + 3t \geq 0$, a odatle slijedi $t = 34, 35, 36, 37, 38, 39, 40$, dakle postoji 7 rješenja, tj. posuda od 100 l može se napuniti pomoću posuda od 3 l i 5 l na 7 načina. Konkretna rješenja su $(30, 2)$, $(25, 5)$, $(20, 8)$, $(15, 11)$, $(10, 14)$, $(5, 17)$, $(0, 20)$.

Zadatak 5. Na koliko se načina može proizvod, čija je cijena 26 €, kupiti pomoću novčanica od 2 €, 5 € i 10 € bez ostatka?

Rješenje. Iz uvjeta zadatka imamo jednadžbu $2x_1 + 5x_2 + 10x_3 = 26$. Budući je $M(5, 10) = 5 \neq 1$, tada slijedi preraspodjela, pa ćemo riješiti jednadžbu

$$10x_3 + 2x_1 + 5x_2 = 26. \tag{56}$$

Iz (56) dobivamo matričnu jednadžbu

$$\begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 10 & 2 & 5 \end{bmatrix}^{-1} \begin{bmatrix} t_1 \\ t_2 \\ 26 \end{bmatrix}$$

ili

$$\begin{bmatrix} x_3 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 20 & 5 & -2 \\ -10 & -2 & 1 \end{bmatrix} \begin{bmatrix} t_1 \\ t_2 \\ 26 \end{bmatrix},$$

dakle rješenjs je

$$x_1 = 20t_1 + 5t_2 - 52, \quad x_2 = -10t_1 - 2t_2 + 26, \quad x_3 = t_1. \tag{57}$$

Budući da se traži $x_1,\ x_2,\ x_3 \geq 0$, iz relacija (53) slijede nejednakosti $20t_1 + 5t_2 \geq 52$, $10t_1 + 2t_2 \leq 26$, $t_1 \geq 0$, a ti su uvjeti zadovoljeni ako je $t_1 = 0$ i $t_2 \in \{11, 12, 13\}$, ili ako je $t_1 = 1$ i $t_2 \in \{7, 8\}$, te napokon $t_1 = 2$ i $t_2 = 3$, pa ako te vrijednosti uvrstimo u (57) dobivamo rješenja $(3, 4, 0)$, $(8, 2, 0)$, $(13, 0, 0)$, $(3, 2, 1)$, $(8, 0, 1)$, $(3, 0, 2)$ s nenegativnim komponentama. Dakle, proizvod možemo kupiti bez ostatka na 6 načina.

Literatura

[1] F. Ayres, Jr., *Matrices*, Shaum's Outline Series, McGraw-Hill 1962.

[2] D. Blanuša, *Viša matematika, I dio*, Tehnička knjiga, Zagreb 1970.

[3] S. Kurepa, *Uvod u matematiku*, Tehnička knjiga, Zagreb 1984.

[4] D. S. Mitrinović, *Matrice i determinante*, Naučna knjiga, Beograd 1972.

[5] M. Radić, *Algebra, II dio*, Školska knjiga, Zagreb 1972.