Линеарне Диофантове једначине

Деф1. Једначина облика $ax+by=c$, у којој су a,b,c цели бројеви, такви да је $a\cdot b\neq 0$, при чему промењиве x и y узимају вредности из скупа $\mathbb{Z}$ (или неког његовог подскупа) назива се <u>линеарна Диофантова једначина</u>.

Уопште, свака полиномна једначина по променљивама $x,y,z,\dots$, чији су коефицијенти цели (рационални) бројеви, у којој променљиве узимају вредности из скупа $\mathbb{Z}$, назива се Диофантова једначина.

Зашто смо у претходној дефиницији ставили да коефицијенти могу бити рационални бројеви?

Посматрајмо нпр. једначину

$$\frac{2}{3}x-\frac{3}{5}y=\frac{2}{7}$$

Ако ову једначину помножимо са $[3,5,7]=105$, добијамо једначину са целобројним коефицијентима

$$70x-63y=30.$$

Зашто једначину из дефиниције 1 зовемо линеарна Диофантова једначина? — због тога што су променљиве ~~x~~ x и y линеарне, тј. првог степена (x^1, y^1). Ако би било нпр. $3x^2 - 5y^2 = 8$, у питању је квадратна једначина.

Посматрајмо у наставку једначину

$$ax + by = c \quad (1)$$

и начине њеног решавања.

Теорема 1. Линеарна Диофантова једначина $ax + by = c$ има решење акко $d \mid c$, где је $d = (a, b)$.

Доказ.

($\Longrightarrow$) Претпоставимо да ј-на (1) има решење (x_0, y_0), $x_0, y_0 \in \mathbb{Z}$. Тада је $a \cdot x_0 + b y_0 = c$ (јер, бројеви x_0 и y_0 задовољавају ј-ну (1)).

Нека је $d = (a, b)$. Тада $d \mid a$ и $d \mid b$.

Како $d \mid a$, следи да $d \mid a x_0$ ($x_0 \in \mathbb{Z}$), а како $d \mid b$, следи да $d \mid b y_0$ ($y_0 \in \mathbb{Z}$). Сада, $d \mid a x_0$ и $d \mid b y_0$, па

$d \mid a x_0 + b y_0$, тј. $d \mid c$.

($\Leftarrow$) Обратно, претпоставимо да $d \mid c$, где је $d = (a, b)$. Према дефиницији релације дељивости следи да је $c = d \cdot k$, $k \in \mathbb{Z}$.

Како је $d = (a, b)$ постоје (према ономе што смо доказивали код највећег заједничког делиоца) цели бројеви $\alpha, \beta \in \mathbb{Z}$, тако да је $\alpha a + \beta b = d$.

Сада, множећи ове релације са k добијамо

$$\alpha \cdot a \cdot k + \beta \cdot b \cdot k = \underbrace{d k}_{\| \; c}$$

Нека је $\alpha \cdot k = x_0 \in \mathbb{Z}$ и $\beta \cdot k = y_0 \in \mathbb{Z}$. Тада је

$a x_0 + b y_0 = c$, тј. уређени пар (x_0, y_0) је решење једн-не (1). ∎

Показатисмо да ако једн (1) има једно решење (а из претходне теореме то важи када $(a,b) \mid c$) тада она има бесконачно много решења, и показатисмо како да добијемо та решења. Приказатисмо две методе решавања линеарних Диофантових једначина.

Методе решавања

Метода почетног решења

Теорема 2. Ако је $d=(a,b)$, $d \mid c$ и (x_0, y_0) је једно решење линеарне Диофантове једначине $ax+by=c$, тада су сва решења (x,y) дата формулама

$$(2) \quad \begin{cases} x = x_0 + \frac{b}{d} \cdot t \\ y = y_0 - \frac{a}{d} \cdot t \end{cases}, \quad t \in \mathbb{Z}.$$

Доказ.

Покажимо најпре да (x,y) дати формулама (2) заиста представљају решења ј-не $ax+by=c$.

$$a \cdot \left(x_0 + \frac{b}{d} \cdot t\right) + b \cdot \left(y_0 - \frac{a}{d} \cdot t\right) = ax_0 + \frac{ab}{d} \cdot t + by_0 - \frac{ba}{d}$$

$$= ax_0 + by_0 = c.$$

↙ јер је (x_0, y_0) једно решење ј-не $ax+by=c$

Дакле, формулама (2) су заиста дата решења ј-не $ax+by=c$ (заменом оних вредности на левој страни ј-не $ax+by=c$, са десне стране добијамо c)

Докажимо још да је произвољно решење (X, Y) једне $ax+by=c$ облика (2).

Како је (X, Y) решење једне $ax+by=c$, што је

$$a \cdot X + b \cdot Y = c \quad (*)$$

Важи да је (x_0, y_0) једно решење једне $ax+by=c$, одакле следи да је

$$ax_0 + by_0 = c \quad (**).$$

Сада из $(*)$ и $(**)$ добијамо

$$aX + bY = ax_0 + by_0,$$

тј.

$$a \cdot (X - x_0) + b \cdot (Y - y_0) = 0 \quad (***).$$

Поделимо $(***)$ са d, где је $d = (a, b)$. Тада је

$$\frac{a}{d}(X - x_0) + \frac{b}{d}(Y - y_0) = 0,$$

тј.

$$\frac{a}{d}(X - x_0) = -\frac{b}{d}(Y - y_0) \quad (****)$$

Важи да је $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (доказивали смо!).

Из $(****)$ следи да $\frac{b}{d} \mid \frac{a}{d}(X - x_0)$, а како је $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ одавде следи да $\frac{b}{d} \mid X - x_0$, тј. $X - x_0 = \frac{b}{d} \cdot t$, $t \in \mathbb{Z}$

Дакле, $X - x_0 = \frac{b}{d} \cdot t$, па је $X = x_0 + \frac{b}{d} t$.

Како је $X - x_0 = \frac{b}{d} \cdot t$, замењом ове вредности у релацију (****) добијамо

$$\frac{a}{d} \cdot \frac{b}{d} \cdot t = -\frac{b}{d} \cdot (Y - y_0), \text{ тј.}$$

$$\frac{a}{d} \cdot t = -(Y - y_0), \text{ односно}$$

$$Y - y_0 = -\frac{a}{d} \cdot t \Rightarrow Y = y_0 - \frac{a}{d} \cdot t$$

Значи, добили смо да се произвољно решење (X, Y) изражава у облику (2), одакле следи да су сва решења ј-не $ax + by = c$ дата формулама (2).

Т решење (x_0, y_0) се зове партикуларно или почетно решење ⌋

Пример. Решити у скупу $\mathbb{Z}$ једначину $3x + 5y = 1001$.

Решење. Проверимо најпре да ли дата ј-на има решења, тј. налазимо $d = (3,5)$. Користимо Еуклидов алгоритам, требаће нам због још једног разлога.

$$(*) \begin{cases} 5 = 3 \cdot 1 + 2 \\ 3 = 2 \cdot 1 + \boxed{1} \\ 2 = 2 \cdot 1 \end{cases} \Rightarrow (3,5) = 1$$

$1 \mid 1001 \Rightarrow$ ј-на има решења

Да бисмо нашли једно (тзв. тзв. партикуларно) решење ове једначине „имитирали" поступак из доказа Теореме 2, тј. тражимо $\alpha, \beta \in \mathbb{Z}$, такве да је

$$2 \cdot 3 + \beta \cdot 5 = 1$$
$$\parallel$$
$$(\beta, 5).$$

~~Ово смо већ радили!~~

Коришћени релације (*) враћамо се уназад и добијамо:

$$1 = 3 - 2 \cdot 1 = 3 - 1 \cdot (5 - 3 \cdot 1) = 3 - (5 - 3)$$
$$= 3 - 5 + 3 = 2 \cdot 3 + (-1) \cdot 5$$

Дакле,

$$2 \cdot 3 + (-1) \cdot 5 = 1$$

↙ Ми хоћемо да овде буде 1001

Због тога помножимо и леву и десну страну са 1001.

$$2 \cdot 3 + (-1) \cdot 5 = 1 \mid \cdot 1001$$
$$2002 \cdot 3 + (-1001) \cdot 5 = 1001$$

$\Rightarrow (x_0, y_0) = (2002, -1001)$ је једно тзв. партикуларно решење наше једначине, тј. је <u>једно</u> решење (према формулама (2)) облика

$$\begin{aligned} x &= 2002 + \frac{5}{1}\cdot t \\ y &= -1001 - \frac{3}{1}\cdot t \end{aligned}, \quad t \in \mathbb{Z}$$

тј.

$$(x, y) = (2002 + 5t, -1001 - 3t), \quad t \in \mathbb{Z} \quad (**)$$

Напомена. Можемо наћи и било које друго партикуларно решење (не мора то да буде (2002, -1001)), можемо користити и неке друге начине за то.

Нпр. за трећиходну једначину се види да је (332, 1) једно цело решење, па ће опште решење бити облика

$$\begin{aligned} x &= 332 + 5k \\ y &= 1 - 3k \end{aligned}, \quad k \in \mathbb{Z} \quad (***)$$

(Како је другачији општи облик решења, свако решење једне $3x + 5y = 1001$ се може добити применом формуле $(**)$ или формуле $(***)$, за неке t и k.

- Ојлерова метода

Ову методу ћемо приказати кроз пример.

Решити линеарну Диофантову једначину $39x-22y=10$

Проверимо да ли има решење. Како је $(39,22)=1$ и $1 \mid 10$, ја има решење.

$$39x-22y=10 \Rightarrow 22y=39x-10$$

$$\Rightarrow y=\frac{39x-10}{22}=\frac{22x+17x-10}{22}$$

$$=\frac{22x}{22}+\frac{17x-10}{22}=x+\frac{17x-10}{22}=z\in\mathbb{Z}$$

Како $y\in\mathbb{Z}$ и $x\in\mathbb{Z}$, следи да и $\frac{17x-10}{22}$ мора бити цео број, па ставимо да је $\frac{17x-10}{22}=z\in\mathbb{Z}$.

~~Сад~~ $(y=x+z)$

Сада је $17x-10=22z \Rightarrow 17x=22z+10$

$$\Rightarrow x=\frac{22z+10}{17}=\frac{17z+5z+10}{17}$$

$$=z+\frac{5z+10}{17}=z+m$$

$m\in\mathbb{Z}$ (из истог разлога)

$$\frac{5z+10}{17}=m \Rightarrow 5z+10=17m$$

$$\Rightarrow z=\frac{17m-10}{5}=\frac{15m+2m-10}{5}=\frac{15m-10}{5}+\frac{2m}{5}=$$

$= 3m-2+\frac{2m}{5}$

$z = (3m-2) + \frac{2m}{5} \Rightarrow \frac{2m}{5} \in \mathbb{Z} \Rightarrow 5 \mid 2m \Rightarrow 5 \mid m$ ($z \in \mathbb{Z}$, $3m-2 \in \mathbb{Z}$, $(2,5)=1$)

$\Rightarrow m = 5n$, $n \in \mathbb{Z}$

$\Rightarrow z = 3m-2+\frac{2\cdot 5n}{5} = 3m-2+2n = 3\cdot(5n)-2+2n$

$= 17n-2$

$x = z+m = 17n-2+5n = 22n-2$

$y = x+z = 22n-2+17n-2 = 39n-4$

$\Rightarrow$ Решења су облика $(x,y) = (22n-2, 39n-4)$, $n \in \mathbb{Z}$

(има их бесконачно много)

Можемо и овако да запишемо

$$R = \{(22n-2, 39n-4) \mid n \in \mathbb{Z}\}$$

↙ скуп решења