

Линеарне Диофантове једначине

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

Уопште, свака полиномијална 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? Погледајмо нпр. једначину

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

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

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

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

Посматраћемо у наставку једнакост

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

и наћи неке решења.

Теорема 1. Линеарна Диофантова једнакост
 $ax + by = c$ има решење ако и само ако $d | c$, где је $d = (a, b)$.

Доказ.

($\Rightarrow$) Претпоставимо да ј-на (1) има решење

(x_0, y_0) , $x_0, y_0 \in \mathbb{Z}$. Тада је $a \cdot x_0 + b \cdot y_0 = c$

(дакле, бројеви x_0 и y_0 задовољавају ј-ну (1)).

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

Како $d | a$, следи да $d | ax_0$ ($x_0 \in \mathbb{Z}$), а како $d | b$,
следи да $d | by_0$ ($y_0 \in \mathbb{Z}$). Када, $d | ax_0$ и $d | by_0$, та
 $d | ax_0 + by_0$, тј. $d | c$.

($\Leftarrow$) Обратно, предположим да $d|c$, где
 је $d = (a, b)$. Према дефиницији релације деливост
 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 делioca)
 цели бројеви $\alpha, \beta \in \mathbb{Z}$, тако да је $\alpha a + \beta b = d$.

Сада, множењем обе релације са k добијалимо

$$\alpha \cdot a \cdot k + \beta \cdot b \cdot k = \underbrace{d \cdot k}_c$$

Нека је $\alpha \cdot k = x_0 \in \mathbb{Z}$ и $\beta \cdot k = y_0 \in \mathbb{Z}$. Тада је
 $\alpha x_0 + \beta y_0 = c$, тј. уређени пар (x_0, y_0) је

решенje ј-не (1). $\square$

Покажемо да ако јна (1) има једно решенje
 (а из претходне теореме то важи када $(a, b) | c$)

тада она има бесконачно много решенja, и пока-
 жемо како да добијемо сва решенja. Покажемо

две методе решавања линеарних Диофантових
 једначина.

Методе решавања

Метода почетног решења

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

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

Доказ.

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

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

$$= ax_0 + by_0 = c.$$

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

Закле, формулама (2) су заиста дати решења ј-те $ax + by = c$ (закључак обим вредности на левој страни ј-те $ax + by = c$, његове стране добијамо c).

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

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

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

Види да је (x_0, y_0) једино решење је $ax + by = c$,
одакле следи да је

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

Сада из $(*)$ и $(**)$ добијемо

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

тј.

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

Познато $(***)$ са d , где је $d = (a, b)$. Штага је

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

тј.

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

Види 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 $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

одакле следи да $\frac{b}{d} \mid X - x_0$, тј. $X - x_0 = \frac{b}{d} \cdot t, t \in \mathbb{Z}$

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

Како је $X - x_0 = \frac{b}{d} \cdot t$, заменим обе вредности у

релацију (****) добијамо

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

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

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

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

Решење (x_0, y_0) се зове партикуларно или почесно решење

Пример. Решити у скупу $\mathbb{Z}$ једначину $3x + 5y = 1001$.
Решење. Проверимо најпре да ли даје ј-на има решење, па. Нађимо $d = (3, 5)$. Користимо Еуклидов алгоритам, требате нам због још једног разлога.

$$(*) \begin{cases} 5 = 3 \cdot 1 + 2 \\ 3 = 2 \cdot 1 + 1 \\ 2 = 2 \cdot 1 \end{cases} \Rightarrow \begin{matrix} (3, 5) = 1 \\ 1 \mid 1001 \Rightarrow \text{јна има} \\ \text{решење} \end{matrix}$$

-7-

За да смо наћи једно (партикуларно) решење
ове ј-не можемо "имитирати" пошутах из доказа
Теореме 2, тј. изражимо $\alpha, \beta \in \mathbb{Z}$, такве да је

$$\alpha \cdot 3 + \beta \cdot 5 = 1$$

"
 $(\mathbb{Z}_5)$.

~~Ово смо~~ Ово смо већ видели!

Користећи релације (*) вратимо се уназад и
добивамо:

$$\begin{aligned} 1 &= 3 - 2 \cdot 1 = 3 - 1 \cdot (5 - 3 \cdot 1) = 3 - (5 - 3) \\ &= 3 - 5 + 3 = 2 \cdot 3 + (-1) \cdot 5 \end{aligned}$$

Дакле,

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

Ми хотимо
да ове буде
1001

Због тога помножимо и леву и десну страну
са 1001.

$$\begin{aligned} 2 \cdot 3 + (-1) \cdot 5 &= 1 \quad | \cdot 1001 \\ 2002 \cdot 3 + (-1001) \cdot 5 &= 1001 \end{aligned}$$

$\Rightarrow (x_0, y_0) = (2002, -1001)$ је једно парти-
куларно решење наше ј-не, па је опште решење
(према формулама (2)) облика

-8-

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

итд.

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

Напомена. Можемо наћи и било које друго партикуларно решење (не мора то да буде $(2002, -1001)$), можемо користити и неки други начин за то.

Нпр. за прелиходну једначину се види да је $(332, 1)$ ~~једно~~ једно њено решење, па ће ~~о~~ опште решење бити облика

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

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

- Ојлерова метода

Ову методу ћемо приказати кроз пример.

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

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

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

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

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

Како $y \in \mathbb{Z}$ и $x \in \mathbb{Z}$, среди да и $\frac{17x - 10}{22}$ мора

бити цео број, па ставимо да је $\frac{17x - 10}{22} = z \in \mathbb{Z}$.
~~Бг~~ ($y = x + z$)

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

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

$$= z + \left(\frac{5z + 10}{17} \right) = z + m$$

$m \in \mathbb{Z}$ (из истог разлога)

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

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

-10-

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

$$\begin{aligned} \left(\begin{array}{c} \in \mathbb{Z} \\ \mathbb{Z} \end{array} \right) = \begin{array}{c} \in \mathbb{Z} \\ \mathbb{Z} \end{array} \left(3m-2 \right) + \frac{2m}{5} &\Rightarrow \frac{2m}{5} \in \mathbb{Z} \Rightarrow 5 \mid 2m \quad \left. \begin{array}{l} (2,5)=1 \\ \Rightarrow 5 \mid m \\ \Rightarrow m=5n \\ n \in \mathbb{Z} \end{array} \right\} \end{aligned}$$

$$\Rightarrow z = 3m-2 + \frac{2 \cdot 5n}{5} = 3m-2 + 2n = 3 \cdot (5n) - 2 + 2n = 17n - 2$$

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

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

$\Rightarrow$ Решения системы облика $(x, y) = (22n - 2, 39n - 4), n \in \mathbb{Z}$
(их бесконечно много)

Можно и иначе записать

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

$\downarrow$
система решения