Diskretne strukture UNI
Vaje 10

1. Z razširjenim Evklidovim algoritmom poišči največji skupni delitelj števil

   (a) 330 in 98, (b) 189 in 40, (c) 260 in 147, (d) 637 in 26.

   Za vsakega od parov določi še njun najmanjši skupni večkratnik.

a)
$$
\begin{aligned}
330 &= 1\cdot 330 + 0\cdot 98 \\
98 &= 0\cdot 330 + 1\cdot 98 \quad /\cdot 3 \\
36 &= 1\cdot 330 - 3\cdot 98 \quad /\cdot 2 \\
26 &= -2\cdot 330 + 7\cdot 98 \\
10 &= 3\cdot 330 - 10\cdot 98 \quad /\cdot 2 \\
6 &= -8\cdot 330 + 27\cdot 98 \\
4 &= 11\cdot 330 - 37\cdot 98 \\
2 &= -19\cdot 330 + 64\cdot 98 \quad /\cdot 2 \\
0 &= \underbrace{49}_{\frac{98}{2}}\cdot 330 - \underbrace{165}_{\frac{330}{2}}\cdot 98
\end{aligned}
$$

$98\cdot 3 = 294$

$330 - 294 = 36$

$36\cdot 2 = 72$

$98 - 72 = 26$

$11 + 2\cdot 19 = 49$

$-37 - 64\cdot 2 = -165$

$\gcd(330, 98) = \underline{\underline{2}}$

$$\mathrm{lcm}(330, 98) = \frac{330\cdot 98}{\gcd(330,98)} = 330\cdot\frac{98}{2} = 330\cdot 49 = \underline{\underline{16\,170}}$$

$$\boxed{\gcd(a,b)\cdot \mathrm{lcm}(a,b) = a\cdot b}$$

b)
$$
\begin{aligned}
189 &= 1\cdot 189 + 0\cdot 40 \\
40 &= 0\cdot 189 + 1\cdot 40 \quad /\cdot 4 \rightsquigarrow 160 = 0\cdot 189 + 4\cdot 40 \\
&\qquad 189 - 160 = 29 \\
29 &= 1\cdot 189 - 4\cdot 40 \\
11 &= -1\cdot 189 + 5\cdot 40 \quad /\cdot 2 \rightsquigarrow 22 = -2\cdot 189 + 10\cdot 40 \\
7 &= 3\cdot 189 - 14\cdot 40 \\
4 &= -4\cdot 189 + 19\cdot 40 \\
3 &= 7\cdot 189 - 33\cdot 40 \\
1 &= -11\cdot 189 + 52\cdot 40 \quad /\cdot 3 \rightsquigarrow 3 = -33\cdot 189 + 156\cdot 40 \\
0 &= 40\cdot 189 - 189\cdot 40
\end{aligned}
$$

$\gcd(189, 40) = \underline{\underline{1}}$

$\mathrm{lcm}(189, 40) = 189\cdot 40 = \underline{\underline{7560}}$

c)
$$
\begin{aligned}
260 &= 1\cdot 260 + 0\cdot 147 \\
147 &= 0\cdot 260 + 1\cdot 147 \\
113 &= 1\cdot 260 - 1\cdot 147 \\
34 &= -1\cdot 260 + 2\cdot 147 \quad /\cdot 3 \rightsquigarrow 102 = -3\cdot 260 + 6\cdot 147 \\
11 &= 4\cdot 260 - 7\cdot 147 \quad /\cdot 3 \rightsquigarrow 33 = 12\cdot 260 - 21\cdot 147 \\
1 &= -13\cdot 260 + 23\cdot 147 \quad /\cdot 11 \rightsquigarrow 11 = -143\cdot 260 + 253\cdot 147 \\
0 &= 147\cdot 260 - 260\cdot 147
\end{aligned}
$$

$\gcd(260, 147) = \underline{\underline{1}} \rightsquigarrow \mathrm{lcm}(260, 147) = 260\cdot 147 = \underline{\underline{38220}}$

d)
$$
\begin{aligned}
637 &= 1\cdot 637 + 0\cdot 26 \\
26 &= 0\cdot 637 + 1\cdot 26 \quad /\cdot 24 \rightsquigarrow 624 = 0\cdot 637 + 24\cdot 26 \\
13 &= 1\cdot 637 - 24\cdot 26 \quad /\cdot 2 \\
0 &= -\underbrace{2}_{\frac{26}{13}}\cdot 637 + \underbrace{49}_{\frac{637}{13}}\cdot 26
\end{aligned}
$$

$\gcd(637, 26) = \underline{\underline{13}}$

$$\mathrm{lcm}(637, 26) = \frac{637\cdot 26}{13} = 2\cdot 637 = \underline{\underline{1274}}$$

2. Reši linearne diofantske enačbe

(a) $15x + 33y = 6$, (b) $7x - 2y = 1$, (c) $65x + 39y = 20$.

Poišči še tiste rešitve, pri katerih je $x \geq 0$ in $y \geq 0$.

$\underline{ax+by=c}$ $\quad a,b,c \in \mathbb{Z}$

- $d = \gcd(a,b)$
- če d ne deli c, ni rešitev
- sicer eno rešitev (x_0, y_0) uganemo ali poiščemo z REA
- vse rešitve so
$$x_k = x_0 + \frac{b}{d}k$$
$$y_k = y_0 - \frac{a}{d}k$$
za $k \in \mathbb{Z}$

(a) $15x + 33y = 6$

1. način

$33 = 1 \cdot 33 + 0 \cdot 15$

$15 = 0 \cdot 33 + 1 \cdot 15 \quad / \cdot 2$

$3 = 1 \cdot 33 - 2 \cdot 15 \quad / \cdot 5$

$0 = -5 \cdot 33 + 11 \cdot 15$

$\gcd(33,15) = d = 3$, d deli $c = 6$ $\Rightarrow$ enačba je rešljiva

$\cdot 2$

$6 = \underbrace{2}_{y_0 = 2} \cdot 33 \underbrace{-4}_{x_0 = -4} \cdot 15$

$$x_k = -4 + \frac{33}{3}k, \quad y_k = 2 - \frac{15}{3}k$$

$$\underline{\underline{x_k = -4 + 11k,\ y_k = 2 - 5k}} \quad (k \in \mathbb{Z})$$

2. način: $15x + 33y = 6 \quad / :3$

$5x + 11y = 2 \rightsquigarrow d = \gcd(5,11) = 1 \rightsquigarrow 1$ deli $2 \Rightarrow$ je rešljiva

uganemo: $5 \cdot 4 - 11 \cdot 2 = -2 \rightsquigarrow 5 \cdot (-4) + 11 \cdot 2 = 2 \rightsquigarrow x_0 = -4,\ y_0 = 2$

$\Rightarrow \underline{\underline{x_k = -4 + 11k,\ y_k = 2 - 5k}} \quad (k \in \mathbb{Z})$

Nenegativne rešitve?

$x_k \geq 0$	$y_k \geq 0$
$-4 + 11k \geq 0$	$2 - 5k \geq 0$
$11k \geq 4$	$5k \leq 2$
$k \geq \frac{4}{11}$	$k \leq \frac{2}{5}$
$k \geq 1$	$k \leq 0$

k-jev, ki bi zadoščali obema pogojema, ni $\Rightarrow$ ni rešitev, kjer bi bila x in y oba nenegativna.

(b) $7x - 2y = 1$

$\gcd(7,2) = d = 1$, d deli $c = 1$ $\Rightarrow$ je rešljiva

$7 \cdot 1 - 2 \cdot 3 = 7 - 6 = 1 \rightsquigarrow x_0 = 1,\ y_0 = 3$

$x_k = 1 + \frac{(-2)}{1}k$, $\ y_k = 3 - \frac{7}{1}k \rightsquigarrow \underline{\underline{x_k = 1 - 2k,\ y_k = 3 - 7k}} \quad (k \in \mathbb{Z})$

Nenegativne rešitve?

$x_k \geq 0$	$y_k \geq 0$
$1 - 2k \geq 0$	$3 - 7k \geq 0$
$2k \leq 1$	$7k \leq 3$
$k \leq \frac{1}{2}$	$k \leq \frac{3}{7}$
$k \leq 0$	$k \leq 0$

$\underline{\underline{k \leq 0}} \rightsquigarrow$ Nenegativne rešitve dobimo za $k = 0, -1, -2, -3, \ldots$

(c) $65x + 39y = 20$

$\gcd(65, 39) = \gcd(5 \cdot 13, 3 \cdot 13) = 13$, 13 ne deli $20 \Rightarrow$ ni rešitev

3. Šolarji so šli na ekskurzijo v muzej. Vstopnica za odrasle stane 10€, za otroke pa 6€. Skupaj so plačali 156€. Koliko je bilo odraslih in koliko otrok, če veš, da je bilo otrok vsaj petkrat več?

Št. odraslih = x

št. otrok = y

$y \geq 5x$

$10x + 6y = 156 \quad /:2$

$\boxed{5x + 3y = 78}$

$\gcd(5,3) = 1$ deli $78 \Rightarrow$ rešljiva

uganemo: $78 = 60 + 18 = 5 \cdot 12 + 3 \cdot 6 \rightsquigarrow x_0 = 12,\ y_0 = 6$

$x_k = 12 + 3k$

$y_k = 6 - 5k$ $\quad (k \in \mathbb{Z})$

<u>Nenegativne rešitve?</u>

$x_k \geq 0$

$12 + 3k \geq 0$

$3k \geq -12$

$k \geq -4$

$y_k \geq 0$

$6 - 5k \geq 0$

$5k \leq 6$

$k \leq \frac{6}{5}$

$k \leq 1$

$k = -4, -3, -2, -1, 0, 1$

k	-4	-3	-2	-1	0	1
x_k	0 -3	3 -3	6 -3	9 -3	12 $+3$	15
y_k	26 $+5$	21 $+5$	16 $+5$	11 $+5$	6 -5	1
$5x_k$	0	15	30	45	60	75
$y_k > 5x_k$?	✗	✓	✗	✗	✗	✗

26 otrok ne bo šlo nikoli samih v muzej :)

V muzej je šlo 21 otrok in 3 odrasli.

4. Na tekmo bi radi z avtobusi pripeljali 1500 navijačev. Na voljo imamo avtobuse z 31 sedeži x in avtobuse s 47 sedeži. Koliko avtobusov naj naročimo, če naj bodo v vseh avtobusih zasedeni vsi sedeži? y

$31x + 47y = 1500 \qquad \gcd(31,47) = 1 \rightsquigarrow 1$ deli $1500 \rightsquigarrow$ je rešljiva

$$\begin{aligned}
47 &= 1\cdot 47 + 0\cdot 31 \\
31 &= 0\cdot 47 + 1\cdot 31 \\
16 &= 1\cdot 47 - 1\cdot 31 \\
15 &= -1\cdot 47 + 2\cdot 31 \\
1 &= 2\cdot 47 - 3\cdot 31 \quad |\cdot 15 \\
0 &= -31\cdot 47 + 47\cdot 31
\end{aligned}$$

$\rightsquigarrow \quad 1 = 2\cdot 47 - 3\cdot 31 \quad |\cdot 1500$

$$1500 = \underbrace{3000}_{y_0}\cdot 47 - \underbrace{4500}_{x_0}\cdot 31$$

$x_0 = -4500,\ y_0 = 3000 \rightsquigarrow x_k = -4500 + 47k$

$y_k = 3000 - 31k$

Nenegativne rešitve?

$$\begin{aligned}
x_k &\geq 0 & y_k &\geq 0 \\
-4500 + 47k &\geq 0 & 3000 - 31k &\geq 0 \\
47k &\geq 4500 & 31k &\leq 3000 \\
k &\geq \tfrac{4500}{47} \doteq 95.7 & k &\leq \tfrac{3000}{31} \doteq 96.7 \\
k &\geq 96 & k &\leq 96
\end{aligned}$$

$$\underline{\underline{k = 96}}$$

$x_{96} = -4500 + 47\cdot 96 = 12$

$y_{96} = 3000 - 31\cdot 96 = 24$

Naročiti moramo 12 avtobusov z 31 sedeži in 24 avtobusov s 47 sedeži.

Preverimo: $12\cdot 31 + 24\cdot 47 = 372 + 1128 = 1500$ ✓

5. Reši linearne diofantske enačbe

(a) $21x + 15y - 6z = 9$, (b) $10x + 13y + 17z = 50$, (c) $28x + 30y + 31z = 365$.

Opiši še tiste rešitve teh enačb, za katere velja $x \geq 0$, $y \geq 0$ in $z \geq 0$.

(a) $21x + 15y - 6z = 9 \quad / : 3$

$7x + 5y - 2z = 3$ → najmanjši po absolutni vrednosti

$2z = 7x + 5y - 3 \quad / : 2$

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

$\underbrace{z}_{\in \mathbb{Z}} = \underbrace{3x + 2y - 1}_{\in \mathbb{Z}} + \underbrace{\frac{1}{2}x + \frac{1}{2}y - \frac{1}{2}}$ $\Rightarrow t_1 \in \mathbb{Z}$

$t_1 = \frac{1}{2}x + \frac{1}{2}y - \frac{1}{2} \quad / \cdot 2$

$2t_1 = x + y - 1$

$x + y - 2t_1 = 1$

$y = \underbrace{2t_1 - x + 1}_{\in \mathbb{Z}}$

$x = t_2$, $y = 2t_1 - t_2 + 1$

$z = 3x + 2y - 1 + t_1 = 3t_2 + 2(2t_1 - t_2 + 1) - 1 + t_1 =$

$= 3t_2 + 4t_1 - 2t_2 + 2 - 1 + t_1$

$z = 5t_1 + t_2 + 1 \qquad (t_1, t_2 \in \mathbb{Z})$

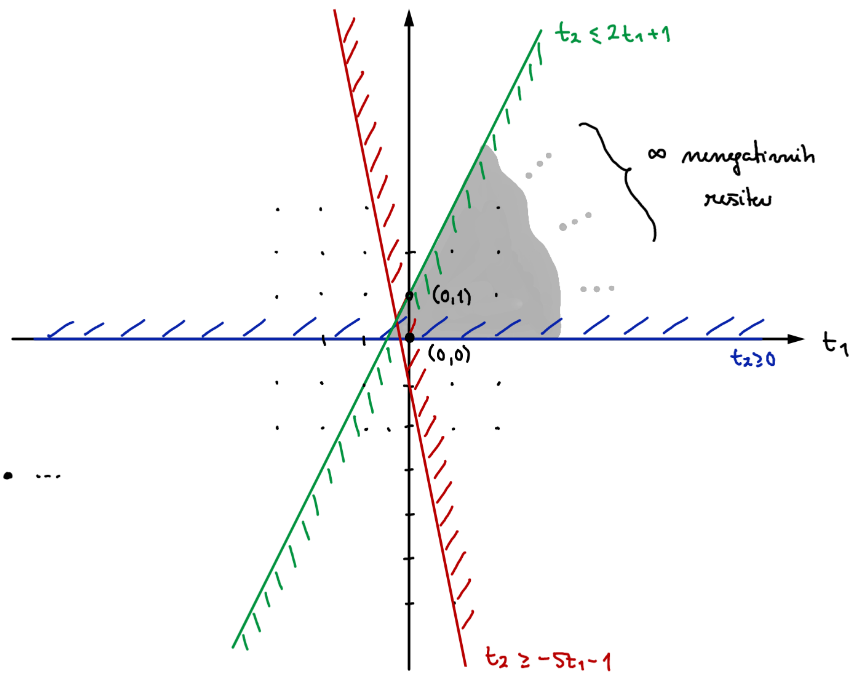
Preverimo: $7(t_2) + 5(2t_1 - t_2 + 1) - 2(5t_1 + t_2 + 1) = \overbrace{7t_2}^{0t_2} + 10t_1 - 5t_2 + 5 - \overbrace{10t_1}^{0t_1} - 2t_2 - 2 = 3$ ✓

Nenegativne rešitve?

$x \geq 0$: $t_2 \geq 0$

$y \geq 0$: $2t_1 - t_2 + 1 \geq 0$, $t_2 \leq 2t_1 + 1$

$z \geq 0$: $5t_1 + t_2 + 1 \geq 0$, $t_2 \geq -5t_1 - 1$



Primeri nenegativnih rešitev:

- $(t_1, t_2) = (0, 0)$: $x = 0$, $y = 1$, $z = 1$
- $(t_1, t_2) = (0, 1)$: $x = 1$, $y = 0$, $z = 2$
- ...

(b) $10x+13y+17z=50$ $\quad$ $\gcd(10,13,17)=1$

$$10x = 50-13y-17z \quad /:10$$
$$x = 5-\frac{13}{10}y-\frac{17}{10}z$$
$$x = 5-y-\frac{3}{10}y-z-\frac{7}{10}z$$
$$\underbrace{x}_{\in\mathbb{Z}} = \underbrace{5-y-z}_{\in\mathbb{Z}}\underbrace{-\frac{3}{10}y-\frac{7}{10}z}_{t_1}$$

$$t_1=-\frac{3}{10}y-\frac{7}{10}z \in\mathbb{Z}$$
$$10t_1=-3y-7z$$
$$10t_1+3y+7z=0$$
$$3y=-7z-10t_1 \quad /:3$$
$$y=-\frac{7}{3}z-\frac{10}{3}t_1$$
$$\underbrace{y}_{\in\mathbb{Z}}=\underbrace{-2z-3t_1}_{\in\mathbb{Z}}\underbrace{-\frac{1}{3}z-\frac{1}{3}t_1}_{t_2\in\mathbb{Z}}$$
$$t_2=-\frac{1}{3}z-\frac{1}{3}t_1$$
$$3t_2=-z-t_1$$
$$\underline{\underline{z=-t_1-3t_2}}$$
$$y=-2(-t_1-3t_2)-3t_1+t_2=$$
$$=2t_1+6t_2-3t_1+t_2$$
$$\underline{\underline{y=-t_1+7t_2}}$$

$$x=5-(-t_1+7t_2)-(-t_1-3t_2)+t_1$$
$$x=5+t_1-7t_2+t_1+3t_2+t_1$$
$$\underline{\underline{x=5+3t_1-4t_2}}$$

Preverimo: $10(5+3t_1-4t_2)+13(-t_1+7t_2)+17(-t_1-3t_2)=50+30t_1-40t_2-13t_1+91t_2-17t_1-51t_2=50$ ✓ $\quad$ ($0t_2$, $0t_1$)

Nenegativne rešitve? $\quad x\geq 0 \quad y\geq 0 \quad z\geq 0$

⋮ ⋮ ⋮

Vedno enačbe 3 polravnin.
Iščemo celoštevilske točke v preseku vseh treh.

(c) $28x+30y+31z=365$ $\quad$ $\gcd(28,30,31)=1$

Eno nenegativno rešitev znamo uganiti: $x=1, y=4, z=7$.

$$28x=365-30y-31z$$
$$x=\frac{365}{28}-\frac{30}{28}y-\frac{31}{28}z$$
$$x=13+\frac{1}{28}-y-\frac{2}{28}y-z-\frac{3}{28}z$$
$$x=13-y-z+\underbrace{\frac{1}{28}-\frac{2}{28}y-\frac{3}{28}z}_{t_1}$$

$$28t_1=1-2y-3z$$
$$28t_1+2y+3z=1$$
$$2y=1-3z-28t_1$$
$$y=\frac{1}{2}-\frac{3}{2}z-14t_1$$
$$y=-z-14t_1+\underbrace{\frac{1}{2}-\frac{1}{2}z}_{t_2}$$
$$2t_2=1-z$$
$$\underline{\underline{z=1-2t_2}}$$
$$y=-(1-2t_2)-14t_1+t_2=-1+2t_2-14t_1+t_2$$
$$\underline{\underline{y=-1-14t_1+3t_2}}$$

$$x=13-(-1-14t_1+3t_2)-(1-2t_2)+t_1=$$
$$=13+1+14t_1-3t_2-1+2t_2+t_1$$
$$\underline{\underline{x=13+15t_1-t_2}}$$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad 0\cdot t_1 \quad\quad 0\cdot t_2$

Preverimo: $28(13+15t_1-t_2)+30(-1-14t_1+3t_2)+31(1-2t_2) = 364+420t_1-28t_2-30-420t_1+90t_2+31-62t_2 = 365$ ✓

Nenegativne rešitve:

$x \geq 0$

$13+15t_1-t_2 \geq 0$

$t_2 \leq 15t_1+13$

$(0,13)\ (1,28)$
$(-1,-2)$

$y \geq 0$

$-1-14t_1+3t_2 \geq 0$

$3t_2 \geq 1+14t_1$

$t_2 \geq \frac{14}{3}t_1+\frac{1}{3}$

$(1,5)\ (-2,-9)$

$z \geq 0$

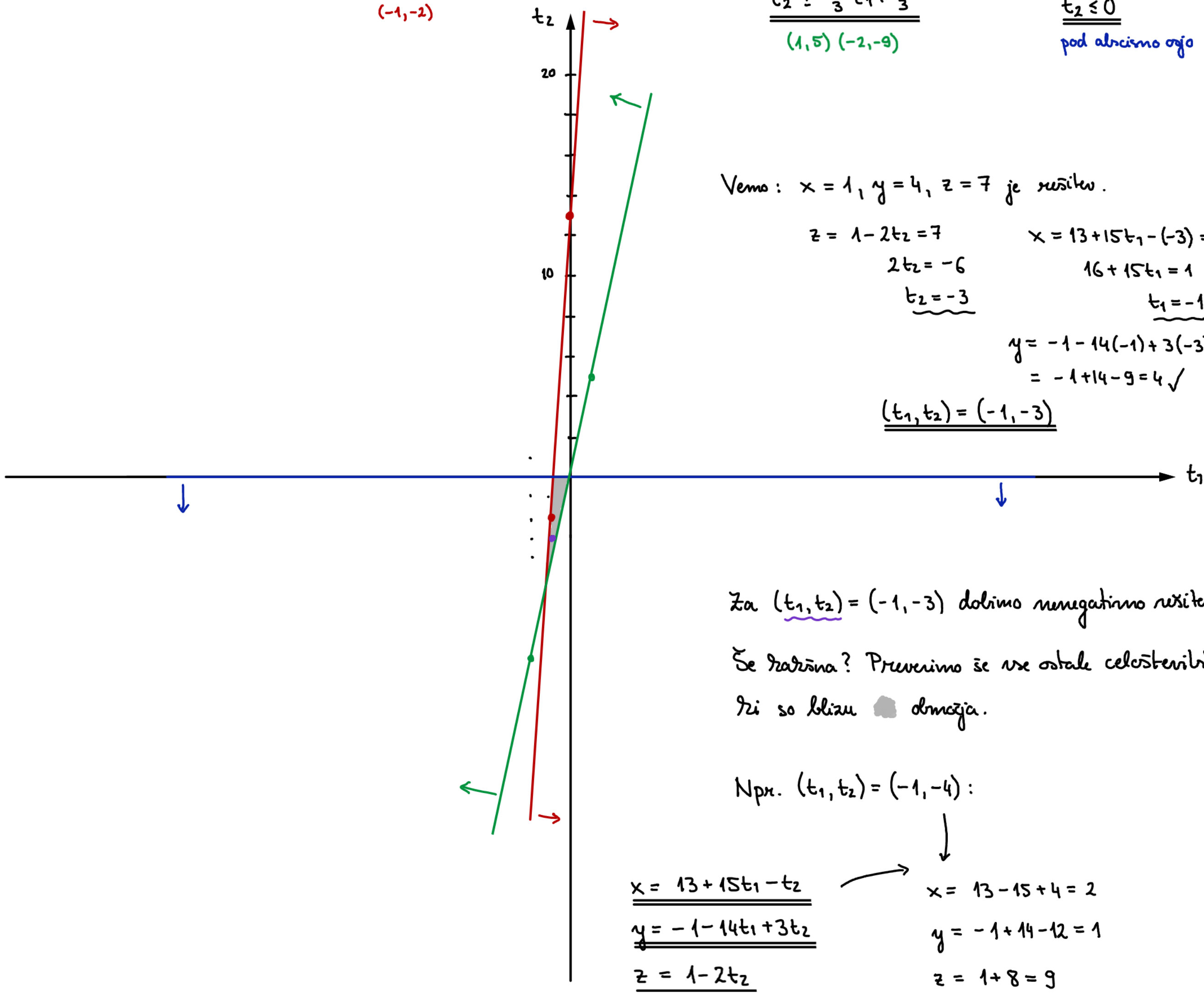
$1-2t_2 \geq 0$

$2t_2 \leq 1$

$t_2 \leq \frac{1}{2}$

$t_2 \leq 0$

pod abscisno osjo



Vemo: $x=1,\ y=4,\ z=7$ je rešitev.

$z = 1-2t_2 = 7$
$2t_2 = -6$
$t_2 = -3$

$x = 13+15t_1-(-3) = 1$
$16+15t_1 = 1$
$t_1 = -1$

$y = -1-14(-1)+3(-3) =$
$= -1+14-9 = 4$ ✓

$(t_1,t_2) = (-1,-3)$

Za $(t_1,t_2) = (-1,-3)$ dobimo nenegativno rešitev.

Še kakšna? Preverimo še vse ostale celoštevilske točke, ki so blizu območja.

Npr. $(t_1,t_2) = (-1,-4)$:

$x = 13+15t_1-t_2$ $\quad\quad x = 13-15+4 = 2$

$y = -1-14t_1+3t_2$ $\quad\quad y = -1+14-12 = 1$

$z = 1-2t_2$ $\quad\quad z = 1+8 = 9$

$2\cdot 28+1\cdot 30+9\cdot 31 = 365$

Koledar bi lahko imel 2 meseca z 28 dnevi, 1 mesec s 30 in 9 mesecev z 31.

6. Določi najmanjše naravno število x, za katerega da $157x$ ostanek 10 pri deljenju s 24.

$157x \,\%\, 24 = 10 \rightsquigarrow 157x + 24y = 10$

$157 = 1\cdot 157 + 0\cdot 24$

$24 = 0\cdot 157 + 1\cdot 24 \;/\cdot 6 \longrightarrow 144 = 0\cdot 157 + 6\cdot 24$

$13 = 1\cdot 157 - 6\cdot 24$

$11 = -1\cdot 157 + 7\cdot 24$

$2 = 2\cdot 157 - 13\cdot 24 \;/\cdot 5 \longrightarrow 10 = 10\cdot 157 - 65\cdot 24$

$1 = -11\cdot 157 + 72\cdot 24$

$\vdots$

$\gcd = 1$ → rešljiva

1. možnost

$\cdot 10$

$10 = -110\cdot 157 + 720\cdot 24$

$x_0 = -110$

$y_0 =$

$x_k = -110 + 24k$

$y_k =$

\+ iskanje najmanjšega nenegativnega x

2. možnost: malo lažje, če opazimo (manjše številke)

$10 = 10\cdot 157 - 65\cdot 24$

$x_0 = 10$

$x_k = 10 + 24k$

$x_0 = 10$ je že najmanjši

Vse rešitve so $x_k = 10 + 24k,\ k\in\mathbb{Z}$.

Najmanjša nenegativna je $x = 10$.

7. (a) Izračunaj $\varphi(1215)$ in $\varphi(1216)$.

(b) Določi $1024^{3241} \pmod{1215}$.

φ = Eulerjeva φ funkcija

$\varphi(n)$ = število števil med 1 in n, ki so tuja n

$\varphi(p) = p-1$ za $p \in \mathbb{P}$

$\varphi(p^\alpha) = (p-1)p^{\alpha-1}$ za $p \in \mathbb{P}, \alpha = 2,3,4,\dots$

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ praštevilski razcep

$\Rightarrow \varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \ldots \cdot \varphi(p_k^{\alpha_k})$

a)

$$\begin{array}{r|l} 1215 & 3 \\ 405 & 3 \\ 135 & 3 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad \begin{array}{r|l} 1216 & 2 \\ 608 & 2 \\ 304 & 2 \\ 152 & 2 \\ 76 & 2 \\ 38 & 2 \\ 19 & 19 \\ 1 & \end{array}$$

$1215 = 3^5 \cdot 5$, $\varphi(1215) = \varphi(3^5 \cdot 5) = \varphi(3^5) \cdot \varphi(5) = 2 \cdot 3^4 \cdot 4 = 2 \cdot 81 \cdot 4 = 648$

$\underline{\underline{\varphi(1215) = 648}}$

$1216 = 2^6 \cdot 19$, $\varphi(1216) = \varphi(2^6 \cdot 19) = \varphi(2^6) \cdot \varphi(19) = 1 \cdot 2^5 \cdot 18 = 32 \cdot 18 = 576$

$\underline{\underline{\varphi(1216) = 576}}$

Fermatov mali izrek:

$p \in \mathbb{P} \Rightarrow \forall a \in \mathbb{Z}: a^p \equiv a \pmod{p}$

Eulerjev izrek

a, m tuji $\Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$

b) $1024^{3241} \equiv ? \pmod{1215}$

a, n tuji $\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

$a = 1024$, $n = 1215$, $\varphi(n) = 648 \Rightarrow 1024^{648} \equiv 1 \pmod{1215}$

$648 \cdot 5 = 3240$

$$1024^{3241} \equiv 1024^{3240+1} \equiv 1024^{5 \cdot 648 + 1} \equiv \left(\underbrace{(1024)^{648}}_{\equiv 1}\right)^5 \cdot 1024 \equiv 1^5 \cdot 1024 \equiv \underline{\underline{1024}} \pmod{1215}$$