

Ecuatii diofantice de grad 1

Ec in $\mathbb{Z} \times \mathbb{Z}$ de forma $ax + by = c$. (D)

Prop: Ec. (D) are sol. $\Leftrightarrow (a, b) \mid c$.

Dem: " \Rightarrow " $d = (a, b)$; $d \mid a \wedge d \mid b$ $\left\{ \begin{array}{l} \Rightarrow d \mid ax_0 + by_0 = c \\ \exists (x_0, y_0) \in \mathbb{Z} \times \mathbb{Z} \text{ a.t. } ax_0 + by_0 = c \end{array} \right.$

" \Leftarrow " $d = (a, b)$; $d \mid c \Rightarrow c = dc'$ cu $c' \in \mathbb{Z}$
 $a = d a'$, $b = d b'$; $(a', b') = 1$

Ec. (D) devine $a'x + b'y = c'$ cu $(a', b') = 1$.

$(a', b') = 1 \Leftrightarrow \exists \alpha, \beta \in \mathbb{Z}$ s.t. $\alpha a' + \beta b' = 1$.

$(\Rightarrow (x_0 = \alpha c', y_0 = \beta c'))$ e sol a ec. (D).

In general, daca $d = (a, b)$ atunci $\exists \alpha, \beta \in \mathbb{Z}$ s.t. $\alpha a + \beta b = d$

Algorithmus von Euclid: $a, b \in \mathbb{Z}, |a| > |b| \neq 0$

$$\begin{aligned} a = b\varrho_1 + r_1, \quad 0 \leq r_1 < |b| \quad &\Rightarrow r_1 = a - b\varrho_1 \\ b = r_1\varrho_2 + r_2, \quad 0 \leq r_2 < r_1 \quad &\Rightarrow r_2 = b - (a - b\varrho_1)\varrho_2 \\ r_1 = r_2\varrho_3 + r_3, \quad 0 \leq r_3 < r_2 \quad &\Rightarrow r_3 = a - b\varrho_1 - r_2(-\varrho_2 + \\ &\vdots \\ r_{n-2} = r_{n-1}\varrho_n + r_n, \quad 0 \leq r_n < r_{n-1} \quad &+ (\varrho_1\varrho_2)\varrho_3)b \\ r_{n-1} = r_n\varrho_{n+1} + 0 \quad &= \alpha_3 a + \beta_3 b \\ \text{J.m.: } 0 \leq r_n < r_{n-1} < \dots < r_2 < r_1 < |b| \quad &\alpha_3 = 1 + \varrho_2\varrho_3 \\ &\beta_3 = (\varrho_1\varrho_2)(-\varrho_3) - \varrho_1 \\ d = r_n = (a, b) \quad &\Rightarrow d = \underbrace{\alpha_n}_{\alpha} a + \underbrace{\beta_n}_{\beta} b \end{aligned}$$

Reziproker (D) $d = (a, b) \mid c$.

Für (x_0, y_0) ein partikuläres in (x, y) allg. sol. von (D)

$$ax_0 + by_0 = ax + by = c \quad | : d$$

$$a'(x_0) + b'y_0 = a'x + b'y (= c')$$

$$\underbrace{a'(\overbrace{x - x_0})}_{\substack{| \\ a'}} = b'(\overbrace{y_0 - y}) \quad \left\{ \begin{array}{l} (a, b) = 1 \\ \Rightarrow a' \mid y_0 - y \end{array} \right. \Rightarrow$$

$$\Rightarrow \exists t \in \mathbb{Z} \quad y_0 - y = a't \Leftrightarrow y = y_0 - a't$$

$$a'(\overbrace{x - x_0}) = b'a't \quad |, a' \neq 0 \Rightarrow x = x_0 + b't$$

für gen. sol. von (D) entsteht $\begin{cases} x = x_0 + b't \\ y = y_0 - a't \end{cases}, \quad t \in \mathbb{Z}$

Example:

i) $281x - 133y = 3$

$$281 = 133 \cdot 2 + 15 \Rightarrow 15 = 281 - 133 \cdot 2$$

$$\begin{aligned} 133 &= 15 \cdot 8 + 13 \Rightarrow 13 = 133 - 15 \cdot 8 \\ &= 133 - (281 - 133 \cdot 2) \cdot 8 \\ &= -8 \cdot 281 + 17 \cdot 133 \end{aligned}$$

$$15 = 13 \cdot 1 + 2 \Rightarrow 2 = 15 - 13 = 9, 281 - 19 \cdot 133$$

$$13 = 2 \cdot 6 \rightarrow 1 \Rightarrow 1 = 13 - 6 \cdot 2 = 131 \cdot 133 - 62 \cdot 281$$

$$2 = 1 \cdot 2 + 0$$

$$\text{durch } -62 \cdot 281 + 131 \cdot 133 = 1 \mid \cdot 3 \Rightarrow$$

$$\Rightarrow x_0 = -3 \cdot 62 = -186, y_0 = -3 \cdot 131 = -393$$

ext. rel. partiz. or ec.

$$\text{fol. ffn ext. } \left\{ \begin{array}{l} x = -186 + 133t, t \in \mathbb{Z} \\ y = -393 + 281t \end{array} \right.$$

$$\boxed{281x - 133y = 3}$$

$$ii) A = \{3n-2 \mid n \in \mathbb{N}\}, B = \{1003-2m \mid m \in \mathbb{N}\}$$

$$C = \{6l+1 \mid l \in \mathbb{N} \cap [0, 166]\}$$

$$A \cap B \cap C = ?$$

lsl: $x \in A \cap B \iff \exists n, m \in \mathbb{N} \text{ and } x = 3n-2 = 1003-2m$

$$3n-2m = 1005$$

lsl part 1: $3 \cdot 3 + 2 \cdot (-4) = 1 \mid 1005 \Rightarrow \begin{cases} m_0 = 3015 \\ m_0 = -4020 \end{cases} \Rightarrow$

lsl generate $\begin{cases} n = 3015 + 2t \in \mathbb{N} \\ m = -4020 - 3t \in \mathbb{N} \end{cases} \Rightarrow t \in \mathbb{Z} \cap [-1507, -1340]$

$$x = 3n-2 = 9043 + 6t, t \in \mathbb{Z} \cap [-1507, -1340]$$

$$A \cap B = \{6t + 9043 \mid t \in \mathbb{Z} \cap [-1507, -1340]\}$$

$$= \{6z+1 \mid z \in \mathbb{Z} \cap [0, 167]\}$$

$$(z = 1507 + t)$$

$$A \cap B \cap C = \{6z+1 \mid z \in \mathbb{Z} \cap [0, 167] \} \cap \{6l+1 \mid l \in \mathbb{N} \cap [0, 166]\}$$

$$= \{6p+1 \mid p \in \mathbb{N} \cap [0, 166]\} = C$$

$$\text{Jednačina: } M = \left\{ n \in \mathbb{Z} \mid n = \frac{n^2 + 3}{n^2 + n}, n \in \mathbb{N} \cap [1, 50] \right\}$$

$$|M| = ?$$

Rešenje:

$$1) A = \{2, 3, 6, 8\}, B = \{1, 3, 5, 7\}$$

$$f = \{(x, y) \mid x > 6 \vee y \leq 1\} \subseteq A \times B$$

Explicativno rješenje:

$$\text{Rješenje: } f = \{(x, y) \mid x \in \{6, 8\} \vee y = 1\}$$

$$= \{(6, 1), (8, 1)\} \cup \{(1, 1), (1, 3), (1, 5), (1, 7)\} \subseteq A \times B$$

$$2) A = B = \mathbb{N}; f = \{(3, 5), (15, 3), (3, 3), (15, 5)\}$$

$$\sigma = \{(x, y) \mid x \leq y\} \subseteq \mathbb{N} \times \mathbb{N}$$

$$g = h(x, y) \mid y - x = 12 \subseteq \mathbb{N} \times \mathbb{N}$$

$$a) f^{-1}, g^{-1}, \tau^{-1}$$

$$f^{-1} = \{(5, 3), (3, 5), (3, 3), (15, 5)\} = f$$

$$\tau^{-1} = \{(x, y) \mid (y, x) \in \tau\} = \{(x, y) \mid y \leq x\}$$

$$g^{-1} = \{(x, y) \mid (y, x) \in g\} = \{(x, y) \mid x - y = 12\}$$

$$= \{(y+12, y) \mid y \in \mathbb{N}\}.$$

$$b) f^2, \sigma \circ f, f \circ \sigma = ?$$

$$f^2 = f \circ f = \{(a, c) \mid \exists b \text{ s.t. } (a, b) \in f, (b, c) \in f\}$$

$$= \{(3, 3), (3, 5), (15, 3), (15, 5)\} = f \begin{matrix} 3, 5 \\ 5, 3 \\ 5, 5 \end{matrix} \begin{matrix} 5, 3, 5 \\ 3, 3, 5 \\ 5, 3, 5 \end{matrix}$$

$$f^2 = f \Rightarrow f^m = f, \forall m \in \mathbb{N}^*$$

$$\tau \circ f = \{(a, c) \mid \exists b \text{ s.t. } (a, b) \in f, (b, c) \in \tau\}$$

$$= \{(3, c) \mid c \geq 5\} \cup \{(5, c) \mid c \geq 3\}$$

$$\cup \{(3, 0) \mid c \geq 3\} \cup \{(15, c) \mid c \geq 5\}$$

$$= \{(3, c) \mid c \geq 3\} \cup \{(5, c) \mid c \geq 3\}.$$

$$f \circ \tau = \{(a, c) \mid \exists b \text{ s.t. } (a, b) \in \tau, (b, c) \in f\}$$

$$= \{(a, c) \mid a \leq 3 \} \cup \{(a, 3) \mid a \leq 5\} \cup \{(a, 3) \mid a \leq 3\} \cup \{(a, 5) \mid a \leq 5\}$$

$$= \{(a, 3) \mid a \leq 5\} \cup \{(15, 5) \mid a \leq 5\} \neq \sigma \circ f$$

$$3) \quad S = \{(3,5), (15,3), (3,3), (5,5)\} \subseteq N \times N$$

$$T = \{(x,y) \mid y - x = 12\} \subseteq N \times N$$

$$\sigma = \{(x,y) \mid x \leq y\} \subseteq N \times N$$

$$T \circ S, \sigma \circ T = ?$$

Lös: $T \circ S = \{(x,z) \mid \exists y \text{ s.t. } (x,y) \in S, (y,z) \in T\}$

$$\begin{array}{ccc} 35 & & 5, 17 \\ 53 & & 3, 15 \\ 33 & & 3, 15 \\ & 55 & 5, 17 \\ & & \end{array}$$

$$= \{(3,17), (5,15), (3,15), (5,17)\}.$$

$$\sigma \circ T = \{(a,c) \mid \exists b \text{ s.t. } (a,b) \in T, (b,c) \in \sigma\}$$

$$\begin{array}{c} \| \\ a+12 \end{array} \quad a+12 \leq c$$

$$= \{(a,c) \mid a+12 \leq c\}$$

$$4) \quad \rho = \{ (2a, 3b) \mid a, b \in \mathbb{Z} \} \subseteq \mathbb{Z} \times \mathbb{Z}$$

$$\rho^n = ?, \quad n \in \mathbb{N}^* \quad (\rho^0 \stackrel{\text{def}}{=} \Delta_{\mathbb{Z}})$$

$$\rho^2 = \left\{ (x, z) \mid \exists y \text{ a.r. } \begin{matrix} (x, y) \in \rho, \\ \underset{2a}{\underset{\parallel}{\underset{\parallel}{(y, z)}}} \end{matrix} \underset{3b}{\underset{\parallel}{\underset{\parallel}{(y, z)}}} \in \rho \right\}$$

$$= \left\{ (2a, z) \mid \exists c \text{ a.r. } \begin{matrix} (6c, z) \in \rho \end{matrix} \right\} = \left\{ (2a, 3d) \mid a, d \in \mathbb{Z} \right\}$$

$\underset{(b=2c)}{\underset{\parallel}{\underset{\parallel}{(2, 3c)}}} \quad \underset{\parallel}{\underset{\parallel}{(3d, z)}} = \rho$

$$\Rightarrow \rho^n = \rho, \quad \forall n \in \mathbb{N}^*.$$

Tarea $\rho = \{ (a, a+3) \mid a \in \mathbb{N} \} \subseteq \mathbb{N} \times \mathbb{N}$,

calcular $\rho^n, \quad n \in \mathbb{N}^*$.

Indicación: $\rho^2 = \left\{ (a, c) \mid \exists b \text{ a.r. } \begin{matrix} (a, b), (b, c) \in \rho \end{matrix} \right\}$

$a \rightarrow 3 \quad a+3 \quad a+6$

$$= \left\{ (a, a+6) \mid a \in \mathbb{N} \right\} \neq \rho.$$