## 1. Soustavy lineárních rovnic v analytické geometrii

**1.1.** Uvažujme v $\mathbb{R}^2$ přímku $p$ s parametrickým vyjádřením

$$p = \{(1,2) + t \cdot (1,1) |\ t \in \mathbb{R}\}.$$

(a) Určete obecné vyjádření přímky $p$,
(b) najděte průsečíky přímky $p$ s osou x a osou y,
(c) rozhodněte, které z bodů $(2,3)$, $(3,2)$ a $(-1,1)$ leží na $p$.

(a) Spočítáme normálový vektor $(1,-1)$, který je právě kolmý na směrový vektor přímky $(1,1)$. To znamená, že rovnice přímky má tvar $x - y = c$, a nyní dosazením bodu $(x,y) = (1,2)$ z parametrického zadání dostaneme $c = 1 - 2 = -1$, tedy dostáváme obecné vyjádření přímky $p = \{(x,y) \in \mathbb{R}^2 |\ x - y = -1\}$. Poznamenejme, že vyjádření je určeno jednoznačně až na násobek celé rovnice nenulovým reálným číslem.

(b) Stačí dosadit za x a y nulu do rovnice obecného vyjádření. Pro $y = 0$ dostáváme $x - 0 = -1$ a pro $x = 0$ máme $0 - y = -1$, tudíž hledané průsečíky jsou $(-1,0)$ a $(0,1)$.

(c) Opět využijeme obecné vyjádření, abychom zjistili, že $2-3 = -1$, $3-2 \neq -1$ a $-1 - 1 \neq -1$, a proto bod $(2,3)$ na přímce leží, zatímco body $(3,2)$ a $(-1,1)$ nikoli. $\square$

**1.2.** Uvažujme v $\mathbb{R}^2$ přímku $q$ s obecným vyjádřením

$$q = \{(x,y) \in \mathbb{R}^2 |\ x + 2y = 3\}.$$

(a) Určete parametrické vyjádření přímky $q$,
(b) najděte průsečík přímky $q$ s přímkou $p$ z předchozí úlohy.

(a) Tentokrát známe z obecného tvaru normálový vektor $(1,2)$ a snadno tedy určíme směrový vektor $(2,-1)$, který je na něj kolmý. Například dosazením $y = 0$ najdeme bod $(3,0)$ přímky $q$, proto je $q = \{(3,0) + t \cdot (2,-1) |\ t \in \mathbb{R}\}$ jedno z možných parametrických vyjádření přímky $q$.

(b) Řešíme soustavu rovnic o dvou neznámých $\begin{array}{ccccc} x & + & 2y & = & 3 \\ x & - & y & = & -1 \end{array}$, kterou můžeme také zapsat maticově (to znamená pozičně bez přepisování symbolů, x a y) do matice soustavy $\left(\begin{array}{cc|c} 1 & 2 & 3 \\ 1 & -1 & -1 \end{array}\right)$. Nyní některým ze známých způsobů upravíme jednu rovnici pomocí druhé tak, abychom jednu z proměnných odstranili. Vyberme si například odčítací metodu a odečtěme od první rovnice druhou. V maticovém zápisu to bude vypadat následovně:

$$\left(\begin{array}{cc|c} 1 & 2 & 3 \\ 1 & -1 & -1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & -3 & -4 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & 1 & \frac{4}{3} \end{array}\right),$$

kde symbol $\sim$ znamená, že soustava napravo i nalevo mají stejnou množinu řešení. Třetí úprava odpovídá tomu, že rovnici $-3y = -4$ vydělíme hodnotou $-3$ a získáme tak $y = \frac{4}{3}$. Nyní snadno například z původní druhé rovnice dopočítáme $x = -1 + \frac{4}{3} = \frac{1}{3}$. Hledaným průsečíkem přímek $p$ a $q$ je bod $(\frac{1}{3}, \frac{4}{3})$. $\square$

**1.3.** Najděte všechna (a) reálná, (b) racionální, (c) komplexní řešení soustavy rovnic $\begin{array}{ccccc} x & + & 2y & = & 3 \\ x & - & y & = & -1. \end{array}$

Všechna reálná řešení jsme našli v předchozí úloze. Díky geometrickému náhledu přitom bylo zjevné, že existuje právě jedno řešení soustavy $(\frac{1}{3}, \frac{4}{3})$.

Nalezené řešení je zjevně racionální, tedy jde o jediné racionální řešení Navíc aritmetický postup z předchozí úlohy, který nezávisel na tom, zda počítáme v reálném či komplexním oboru (všechna zúčastněná čísla byla dokonce jen racionální), zajišťuje, že bod $(\frac{1}{3}, \frac{4}{3})$ je i jediným komplexním řešením dané soustavy. □

**1.4.** Najděte v $\mathbb{R}^2$ obecné i parametrické vyjádření přímky $u$ obsahující body $(3, -1)$ a $(2, 1)$.

Nejprve snadno určíme vektor posunutí jednoho bodu do druhého, tedy například $(1, -2) = (3, -1) - (2, 1)$. Protože známe hned dva body přímky můžeme okamžitě napsat parametrické vyjádření $u = \{(2, 1) + t \cdot (1, -2) |\ t \in \mathbb{R}\}$.

Obecné vyjádření získáme stejně jako v úloze 1.1 z parametrického vyjádření pomocí normálového vektoru a dosazení: $u = \{(x, y) \in \mathbb{R}^2 |\ 2x + y = 5\}$ □

**1.5.** Uvažujme v $\mathbb{R}^3$ rovinu $r$ s obecným vyjádřením

$$r = \{(x, y, z) \in \mathbb{R}^3 |\ x + y - z = 1\}.$$

(a) Určete parametrické vyjádření roviny $r$,
(b) rozhodněte, které z bodů $(1, 1, 1)$ a $(2, 2, 2)$ leží v rovině $r$.

(a) Postupujeme obdobně jako ve dvoudimenzionálním prostoru. Potřebujeme nejprve najít jeden bod roviny. Pro volbu $y = z = 0$ dopočítáme bod $(1, 0, 0)$. Nyní musíme najít dva vektory určující rovinu, tedy vektory, které jsou kolmé na normálový vektor $(1, 1, -1)$. Snadno spočítáme, že kolmé jsou například vektory $(1, 0, 1)$ a $(0, 1, 1)$, proto dostáváme parametrické vyjádření roviny

$$r = \{(1, 0, 0) + s \cdot (1, 0, 1) + t \cdot (0, 1, 1) |\ s, t \in \mathbb{R}\}$$

.

(b) Stejně jako v 1.1(c) prostým dosazením do obecného vyjádření zjistíme, že bod $(1, 1, 1)$ leží a bod $(2, 2, 2)$ neleží v rovině $r$. □

**1.6.** Uvažujme v $\mathbb{R}^3$ rovinu $v$ s parametrickým vyjádřením

$$v = \{(3, -1, 1) + s \cdot (1, 1, 2) + t \cdot (1, 0, -1) |\ s, t \in \mathbb{R}\}.$$

(a) Určete obecné vyjádření roviny $v$,
(b) najděte parametrické vyjádření přímky dané průsečíkem roviny $v$ s rovinou $r$ z předchozího příkladu.

(a) Opět stačí najít normálový vektor kolmý na vektory $(1, 1, 2)$ a $(1, 0, -1)$, kterým je (až na nenulový reálný násobek právě) vektor $(1, -3, 1)$ a dosazením do výrazu $x - 3y + z$ bodu $(3, -1, 1)$ získat konstantu 7. Tedy hledané obecné vyjádření roviny má tvar$v = \{(x, y, z) \in \mathbb{R}^3 |\ x - 3y + z = 7\}$.

(b) Podobně jako 1.2(b) řešíme soustavu rovnic tentokrát o třech neznámých $\begin{array}{ccccccc} x & + & y & - & z & = & 1 \\ x & - & 3y & + & z & = & 7 \end{array}$, kterou si opět zapíšeme maticově a budeme ji odčítací metodou upravovat:

$$\left(\begin{array}{ccc|c} 1 & 1 & -1 & 1 \\ 1 & -3 & 1 & 7 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & -1 & 1 \\ 0 & -4 & 2 & 6 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & -1 & 1 \\ 0 & -2 & 1 & 3 \end{array}\right).$$

Druhou rovnici jsme tedy nahradili rovnicí $-2y+z=3$ tak, že soustavy mají stejnou množinu řešení. Nyní jednak po volbě $y=0$ jednoznačně dopočítáme souřadnice bodu přímky $z=3$ a $x=7-0+3=10$ a dále najdeme směrový vektor, který musí být kolmý na normálové vektory $(1,1,-1)$ a $(0,2,-1)$, jímž je vektor $(1,1,2)$. Našli jsme parametrický popis přímky $r\cap v=\{(10,0,3)+t\cdot(1,1,2)|\ t\in\mathbb{R}\}$. $\square$

**1.7.** Spočítejte v komplexních číslech $\mathbb{C}$ hodnotu výrazů:

(a) $1-2i+2+3i$,
(b) $\frac{1}{3+i}$ a $\frac{2+3i}{1-2i}$,
(c) $(1+i)^{50}$.

(a) Reálná a komplexní hodnota se po složkách sečtou: $1-2i+2+3i=3+i$.

(b) Obvyklým způsobem rozšíříme zlomky komplexně sdruženou hodnotou a dostaneme

$$\frac{1}{3+i}=\frac{1}{3+i}\cdot\frac{3-i}{3-i}=\frac{3}{10}-\frac{1}{10}i$$

a

$$\frac{2+3i}{1-2i}=\frac{2+3i}{1-2i}\cdot\frac{1+2i}{1+2i}=-\frac{4}{5}+\frac{7}{5}i.$$

(c) Využijeme goniometrický zápis komplexních čísel a Moivreovu větu:

$$(1+i)^{50}=(\sqrt{2}(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}))^{50}=2^{25}(\cos\frac{50\pi}{4}+i\sin\frac{50\pi}{4})=$$
$$=2^{25}(\cos(6\pi+\frac{\pi}{4})+i\sin(6\pi+\frac{\pi}{4}))=2^{25}(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4})=2^{25}i.$$

$\square$

## 2. Řešení soustav lineárních rovnic

**2.1.** Najděte všechna reálná řešení soustavy rovnic:

$$\begin{array}{rcrcrcr} x & + & 2y & + & z & = & 1\\ -2x & + & y & + & 2z & = & 2\\ x & + & 3y & - & z & = & 0 \end{array}$$

Nejprve si soustavu zapíšeme do rozšířené matice a poté ji pomocí elementárních úprav upravujeme do odstupňovaného tvaru. Vše si budeme zapisovat pomocí maticového zápisu. Připomeňme, že soustava rovnic nalevo od symbolu $\sim$ má stejnou množinu řešeni jako soustava rovnic napravo od něj:

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1\\ -2 & 1 & 2 & 2\\ 1 & 3 & -1 & 0 \end{array}\right)\sim\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1\\ 0 & 5 & 4 & 4\\ 0 & 1 & -2 & -1 \end{array}\right)\sim$$
$$\sim\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1\\ 0 & 1 & -2 & -1\\ 0 & 5 & 4 & 4 \end{array}\right)\sim\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1\\ 0 & 1 & -2 & -1\\ 0 & 0 & 14 & 9 \end{array}\right)$$

Druhý řádek první upravené matice, který odpovídá rovnici $5y+4z=4$, jsme dostali přičtením dvojnásobku rovnice $x+2y+z=1$ k rovnici $-2x+y+2z=2$ (tedy přičtením dvojnásobku řádku $\left(\begin{array}{ccc|c}1 & 2 & 1 & 1\end{array}\right)$ k řádku $\left(\begin{array}{ccc|c}-2 & 1 & 2 & 2\end{array}\right)$) a podobně třetí řádek vznikl z původního třetího řádku odečtením prvního. V dalším kroku jsme jen přehodili řádky (tedy rovnice) a poté jsme odečetli pětinásobek druhého řádku od třetího. Nyní už výsledek získáme zpětnou substitucí. Z poslední rovnice $14z = 9$ okamžitě dostáváme $z = \frac{9}{14}$ a dále dopočítáme

$$y = -1 + 2z = -1 + \frac{9}{7} = \frac{2}{7} \quad \text{a} \quad x = 1 - 2y - z = 1 - \frac{4}{7} - \frac{9}{14} = -\frac{3}{14}.$$

Vidíme, že jediné řešení soustavy je $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -\frac{3}{14} \\ \frac{2}{7} \\ \frac{9}{14} \end{pmatrix}$.

Uvědomme si, že můžeme k výsledku dospět i v maticovém zápisu, tj. můžeme levou stranu matice posloupností elementárních úprav převést až na jednotkovou matici: :

$$\sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 1 & -2 & -1 \\ 0 & 0 & 1 & \frac{9}{14} \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 0 & 1 & 0 & \frac{4}{14} \\ 0 & 0 & 1 & \frac{9}{14} \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 0 & -\frac{3}{14} \\ 0 & 1 & 0 & \frac{2}{7} \\ 0 & 0 & 1 & \frac{9}{14} \end{array}\right).$$

□

**2.2.** Najděte všechna reálná řešení soustavy rovnic:

$$\begin{array}{rcrcrcr} x & + & 2y & + & z & = & 1 \\ -2x & + & y & + & 2z & = & 2 \end{array}$$

Znovu si soustavu zapíšeme do matice a poté ji pomocí přičtení vhodného násobku jedné rovnice k rovnici druhé upravíme stejně jako v předchozí úloze:

$$\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ -2 & 1 & 2 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|c} \mathbf{1} & 2 & 1 & 1 \\ 0 & \mathbf{5} & 4 & 4 \end{array}\right),$$

Vidíme, že se pivoty (v druhé matici vyznačeny tučně) nachází v prvním a druhém sloupci a volná proměnná je tedy ta, která odpovídající třetímu sloupci. Nyní si snadno uvědomíme (a na přednášce byl tento fakt vysloven v pozorování 2.16), že dosadíme-li za $z$ libovolnou hodnotu, pak jednoznačně dopočítáme $y$ a $x$. Položíme-li například $z = 0$, pak z rovnice $5y + 4 \cdot 0 = 4$ dostáváme, že $y = \frac{4}{5}$ a z rovnice $x + 2 \cdot \frac{4}{5} + 0 = 1$ spočítáme, že $x = -\frac{3}{5}$. Našli jsme tedy jedno řešení dané soustavy, které můžeme zapsat do trojice $(x, y, z)^T = (-\frac{3}{5}, \frac{4}{5}, 0)^T$. Dosadíme-li za $z$ obecný reálný prvek $t$ můžeme zpětnou substitucí dopočítat $y$:

$$5y + 4 \cdot t = 4 \Rightarrow y = \frac{4}{5} - \frac{4}{5}t$$

a poté stejným způsobem i $x$:

$$x + 2 \cdot y + z = 1 \Rightarrow x = 1 - 2 \cdot (\frac{4}{5} - \frac{4}{5}t) - t = -\frac{3}{5} + \frac{3}{5}t.$$

Obecné řešení má tedy tvar $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -\frac{3}{5} + \frac{3}{5}t \\ \frac{4}{5} - \frac{4}{5}t \\ t \end{pmatrix} = \begin{pmatrix} -\frac{3}{5} \\ \frac{4}{5} \\ 0 \end{pmatrix} + t \begin{pmatrix} \frac{3}{5} \\ -\frac{4}{5} \\ 1 \end{pmatrix}$ a množina všech řešení soustavy je právě $\{ \begin{pmatrix} -\frac{3}{5} \\ \frac{4}{5} \\ 0 \end{pmatrix} + t \begin{pmatrix} \frac{3}{5} \\ -\frac{4}{5} \\ 1 \end{pmatrix} \mid t \in \mathbb{R}\}$.

Na závěr si připomeňme geometrický význam řešení dané soustavy: každou z rovnic chápeme jako rovinu v $\mathbb{R}^3$ (tvořenou všemi trojicemi $(x, y, z)$, které rovnici řeší) a množina řešení celé soustavy je průnik těchto dvou rovin. Všimneme-li si navíc, že roviny zjevně nejsou rovnoběžné, musí množinu všech řešení tvořit přímka, jejíž jeden bod $(-\frac{3}{5}, \frac{4}{5}, 0)$ už jsme našli a jejíž směr je dán vektorem $(3, -4, 5)$, který je právě o netriviální řešení soustav rovnic se stejnými levými a nulovými pravými stranami. Z geometrického náhledu tedy vidíme, že množin všechna řešení je přímka, kterou můžeme vyjádřit ve tvaru $\{(-\frac{3}{5} + 3t, \frac{4}{5} - 4t, 5t)^T \mid t \in \mathbb{R}\}$. $\square$

**2.3.** Najděte všechna reálná řešení soustavy rovnic:

$$\begin{array}{rcrcrcl} x_1 & + & x_2 & - & x_4 & = & 1 \\ x_2 & + & x_3 & + & x_4 & = & 3 \\ & - & x_3 & + & 2x_4 & = & 0 \\ & & x_3 & + & 3x_4 & = & 5 \end{array}$$

Soustavu si opět můžeme zapsat do matice a poté ji (jedinou elementární řádkovou úpravou) upravíme na odstupňovanou matici:

$$\left(\begin{array}{cccc|c} 1 & 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 & 3 \\ 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 1 & 3 & 5 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 1 & 0 & -1 & 1 \\ 0 & 1 & 1 & 1 & 3 \\ 0 & 0 & -1 & 2 & 0 \\ 0 & 0 & 0 & 5 & 5 \end{array}\right)$$

Nyní už snadno jednoznačně dopočítáme neznámé zpětnou substitucí. Z posledního řádku $5x_4 = 5$ dostáváme, že $x_4 = 1$, z předposledního řádku $-x_3 + 2x_4 = 0$ vidíme, že $-x_3 + 2 = 0$, tedy $x_3 = 2$. Dále z druhé rovnice $x_2 + x_3 + x_4 = 3$ obdržíme $x_2 = 0$ a konečně z rovnice $x_1 + x_2 - x_4 = 1$ dostaneme $x_1 = 2$. Vidíme, že existuje jediné řešení soustavy $(x_1, x_2, x_3, x_4)^T = (2, 0, 2, 1)^T$. $\square$

**2.4.** Najděte všechna reálná řešení soustavy rovnic s maticí *a)* $\left(\begin{array}{ccc|c} 0 & 1 & 1 & 2 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 1 \end{array}\right)$,

*b)* $\left(\begin{array}{cccc|c} 1 & 1 & 3 & 2 & 2 \\ 1 & 0 & 1 & 1 & 1 \\ 2 & 1 & -1 & 1 & 0 \\ 2 & 2 & 1 & 2 & 1 \end{array}\right)$, *c)* $\left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 2 & -1 & 1 \\ 2 & 2 & 1 & 0 & -1 & 1 & 3 \end{array}\right)$.

Ve všech případech postupujeme standardně posloupností elementárních úprav:
a)

$$\left(\begin{array}{ccc|c} 0 & 1 & 1 & 2 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 1 \end{array}\right), \sim \left(\begin{array}{ccc|c} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 \end{array}\right), \sim \left(\begin{array}{ccc|c} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 2 \end{array}\right),$$

Vidíme, že původní soustava je ekvivalentní se soustavou požadující rovnost $0 = 2$, tedy množina řešení je prázdná.
b)

$$\left(\begin{array}{cccc|c} 1 & 1 & 3 & 2 & 2 \\ 1 & 0 & 1 & 1 & 1 \\ 2 & 1 & -1 & 1 & 0 \\ 2 & 2 & 1 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 3 & 2 & 2 \\ 2 & 1 & -1 & 1 & 0 \\ 2 & 2 & 1 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 1 & -3 & -1 & -2 \\ 0 & 2 & -1 & 0 & -1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & -5 & -2 & -3 \\ 0 & 0 & -5 & -2 & -3 \end{array}\right) \sim \left(\begin{array}{cccc|c} \mathbf{1} & 0 & 1 & 1 & 1 \\ 0 & \mathbf{1} & 2 & 1 & 1 \\ 0 & 0 & \mathbf{5} & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Obdrželi jsme matici hodnosti 3 s čtvrtým volným sloupcem (pivoty jsme opět vyznačili tučně). Zvolíme-li opět za čtvrtou neznámou $u$ parametr libovolnou reálnou hodnotu $t$, dopočítáme zpětnou substitucí:

$$z = \frac{3}{5} - \frac{2}{5}t,\ y = -\frac{1}{5} - \frac{1}{5}t,\ x = \frac{2}{5} - \frac{3}{5}t$$

Zjistili jsme, že $\{ \begin{pmatrix} \frac{2}{5} \\ -\frac{1}{5} \\ \frac{3}{5} \\ 0 \end{pmatrix} + t \begin{pmatrix} -\frac{3}{5} \\ -\frac{1}{5} \\ -\frac{2}{5} \\ 1 \end{pmatrix} \mid t \in \mathbb{R}\}$ je množina všech řešení dané soustavy.

Protože čtveřice $(1, 0, 1, -1)^T$ rovněž řeší danou soustavu a vektor $(3, 1, 2, -5)$ řeší homogenní variantu naší soustavy, snadno můžeme nahlédnout, že množinu všech řešení také můžeme popsat ve tvaru $\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ -1 \end{pmatrix} + t \begin{pmatrix} 3 \\ 1 \\ 2 \\ -5 \end{pmatrix} \mid t \in \mathbb{R}\}$.

c)

$$\left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 2 & -1 & 1 \\ 2 & 2 & 1 & 0 & -1 & 1 & 3 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 2 & -1 & 1 \\ 0 & 0 & 1 & -2 & -5 & 3 & 1 \end{array}\right).$$

Získali jsme odstupňovanou matici, v níž jsou bez pivotů 2., 4., 5. a 6. sloupec, tedy volné jsou jim odpovídající proměnné. Označíme-li si neznámé postupně $x_1, \ldots, x_6$, pak pro libovolná $t_2, t_4, t_5, t_6 \in \mathbb{R}$ položíme

$$x_2 = t_2,\ x_4 = t_4,\ x_5 = t_5,\ x_6 = t_6$$

a zpětnou substitucí dopočítáme

$$x_3 = 1 + 2t_4 + 5t_5 - 3t_6 \text{ a poté } x_1 = 1 - t_2 - t_4 - 2t_5 + t_6.$$

Nyní obvyklým způsobem popíšeme množinu všech řešení soustavy:

$$\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t_2 \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t_4 \begin{pmatrix} -1 \\ 0 \\ 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t_5 \begin{pmatrix} -2 \\ 0 \\ 5 \\ 0 \\ 1 \\ 0 \end{pmatrix} + t_6 \begin{pmatrix} 1 \\ 0 \\ -3 \\ 0 \\ 0 \\ 1 \end{pmatrix} + \mid t_2, t_4, t_5, t_6 \in \mathbb{R}\}$$

□

**2.5.** Najděte všechna racionální řešení soustavy rovnic z úlohy 2.2.

Stačí si rozmyslet, že z množiny řešení úlohy 2.2 musíme vybrat ta, která jsou ve všech složkách racionální. Není těžké nahlédnout, že součin, součet i rozdíl racionálních čísel je opět racionální, proto množina $M = \{(-\frac{3}{5} + 3t, \frac{4}{5} - 4t, 5t)^T \mid t \in \mathbb{Q}\}$ jistě obsahuje racionální řešení soustavy. Protože součin, součet a rozdíl nenulového racionálního a iracionálního čísla je zjevně iracionální, obsahuje vektor $(-\frac{3}{5} + 3t, \frac{4}{5} - 4t, 5t)^T$ pro každé iracionální $t$ iracionální hodnoty, tudíž množina $M$ je právě množinou všech racionálních řešení soustavy. □

**2.6.** Najděte v závislosti na parametru $a \in \mathbb{R}$ všechna reálná řešení soustavy rovnic:

$$\begin{array}{rcrcrcl} x & + & y & + & 3z & = & a \\ 2x & - & ay & + & z & = & 1 \end{array}$$

Soustavu si nejprve napíšeme v maticovém tvaru a upravíme na odstupňovaný tvar:

$$\left(\begin{array}{ccc|c} 1 & 1 & 3 & a \\ 2 & -a & 1 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 3 & a \\ 0 & -a-2 & -5 & 1-2a \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 3 & a \\ 0 & a+2 & 5 & 2a-1 \end{array}\right).$$

Protože levá strana poslední rovnice je vždy nenulová, má soustava pro všechna $a$ řešení. musí jen rozlišit situaci, kdy $a+2=0$, tedy $a=-2$ a situaci, kdy $a \neq -2$.

Nechť nejprve $\mathbf{a = -2}$. Pak je $y$ volná proměnná a řešíme soustavu s maticí:

$$\left(\begin{array}{ccc|c} 1 & 1 & 3 & -2 \\ 0 & 0 & 5 & -5 \end{array}\right)$$

Položíme tedy $y = 0$ a dopočítáme $z = -1$ a $x = -2 - 3 \cdot (-1) = 1$. Pro $y = 1$ a dopočítáme hodnoty homogenní soustavy $z = 0$ a $x = -1$, tedy množina všech řešení je tvaru $\{(1, 0, -1)^T + t(-1, 1, 0)^T |\ t \in \mathbb{R}\}$

Nyní nechť $\mathbf{a \neq -2}$. Potom je volná proměnná $z$ a řešíme soustavu s maticí:

$$\left(\begin{array}{ccc|c} 1 & 1 & 3 & a \\ 0 & a+2 & 5 & 2a-1 \end{array}\right)$$

Položíme tedy $z = 0$ a dopočítáme $y = \frac{2a-1}{a+2}$ a $x = a - \frac{2a-1}{a+2} = \frac{a^2+1}{a+2}$. Konečně dopočítáme-li pro $z = 1$ hodnoty řešení homogenní soustavy $y = -\frac{5}{a+2}$ a $x = -(3 - \frac{5}{a+2}) = -\frac{3a+1}{a+2}$ a množina všech řešení je proto tvaru

$$\{ \begin{pmatrix} \frac{a^2+1}{a+2} \\ \frac{2a-1}{a+2} \\ 0 \end{pmatrix} + t \begin{pmatrix} -\frac{3a+1}{a+2} \\ -\frac{5}{a+2} \\ 1 \end{pmatrix} |\ t \in \mathbb{R}\} = \{ \begin{pmatrix} \frac{a^2+1}{a+2} \\ \frac{2a-1}{a+2} \\ 0 \end{pmatrix} + t \begin{pmatrix} 3a+1 \\ 5 \\ -a-2 \end{pmatrix} |\ t \in \mathbb{R}\}$$

□

## 3. Soustavy rovnic nad obecnými tělesy

Sčítání a násobení v tělese $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ pro prvočíslo $p$ budeme vždy zapisovat obvyklými symboly $+$ a $\cdot$.

**3.1.** Najděte nad tělesem $\mathbb{Z}_2$ řešení soustavy rovnic:

$$\begin{array}{rcrcrcl} & & x_3 & + & x_4 & = & 1 \\ x_1 & + & x_3 & + & x_4 & = & 0 \\ & & x_1 & + & x_4 & = & 1 \\ x_1 & + & x_2 & + & x_3 & = & 1 \end{array}$$

Uvědomíme si, že počítání v tělese obsahující jen (ve všech tělesech přítomné) prvky 0 a 1 je velmi snadné, soustavu zapíšeme do matice a s počítáním v $\mathbb{Z}_2$ ji budeme přímočaře upravovat posloupností elementárních úprav:

$$\left(\begin{array}{cccc|c} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right).$$

Nejprve jsme přehodili první a třetí řádek, a poté přičetli (nový) první řádek k druhému a čtvrtému. Dále jsme třetí řádek přičetli ke čtvrtému, pak druhý k třetímu a nakonec jsme zpřeházeli řádku a dostali jsme jediné řešení soustavy $x_1 = x_2 = x_3 = 1$ a $x_4 = 0$.

Poznamenejme, že jsme ke stejnému výsledku mohli dospět i jinou posloupností elementárních úprav, například standardním použitím Gaussovy eliminace a zpětné substituce. □

**3.2.** Spočítejte v tělesech:

(a) $\mathbb{Z}_3$ hodnoty $1^{-1}$, $2^{-1}$ a $2^{-1} \cdot (2+2)$,
(b) $\mathbb{Z}_5$ hodnoty $2^{-1}$, $3^{-1}$, $4^{-1}$ a $(-2)^{-1} \cdot ((2+4) \cdot (4+4)^{-1}) + 3$,
(c) $\mathbb{Z}_7$ hodnoty $2^{-1}$, $3^{-1}$, $4^{-1}$, $5^{-1}$,$6^{-1}$ a $(-2)^{-1} \cdot ((2+4) \cdot (4+4)^{-1}) + 3$,
(d) $\mathbb{Z}_p$ pro liché prvočíslo $p$ hodnoty $2^{-1}$ a $(p-1)^{-1}$.

(a) Stačí uvážit definice operací na $\mathbb{Z}_3$ (tedy modulo 3). Protože $1 \cdot 1 = 1$ a $2 \cdot 2 = 1$, dostáváme $1^{-1} = 1$ a $2^{-1} = 2$. Podobně snadno spočteme, že

$$2^{-1} \cdot (2+2) = 2 \cdot 1 = 2.$$

(b) Uvažujeme stejně jako v (a). Vidíme, že v $\mathbb{Z}_5$ máme $2 \cdot 3 = 1$, proto $2^{-1} = 3$ a $3^{-1} = 2$, a ¨protože $4 \cdot 4 = 1$, vidíme, že $4^{-1} = 4$. Dále

$$(-2)^{-1} \cdot ((2+4) \cdot (4+4)^{-1}) + 3 = 3^{-1} \cdot (1 \cdot 3^{-1}) + 3 = 2 \cdot 2 + 3 = 2.$$

(c) Podobně dostáváme nad $\mathbb{Z}_7$, že $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$ a $6^{-1} = 6$, neboť $2 \cdot 4 = 3 \cdot 5 = 6 \cdot 6 = 1$ a dále

$$(-2)^{-1} \cdot ((2+4) \cdot (4+4)^{-1}) + 3 = 5^{-1} \cdot (6 \cdot 1^{-1}) + 3 = 3 \cdot 6 + 3 = 0.$$

(d) Protože je $p$ liché , vidíme, že $\frac{p+1}{2} \in \mathbb{Z}_p$ a v tělese $\mathbb{Z}_p$ platí, že $2 \cdot \frac{p+1}{2} = 1$, tudíž $2^{-1} = \frac{p+1}{2}$.

Víme z přednášky, že v jakémkoli tělese je $(-1) \cdot (-1) = 1$, tedy $(-1)^{-1} = (-1)$. Protože v tělese $\mathbb{Z}_p$ máme $(p-1)+1 = 0$, je $p-1$ číslo opačné k číslu 1. To znamená, že $-1 = p-1$ a podle předchozí úvahy tedy $(p-1)^{-1} = p-1$. □

**3.3.** Najděte v tělese $\mathbb{Z}_5$:

(a) $x$ splňující rovnici $3x + 4 = 1$,
(b) všechna $x$ a $y$ splňující rovnici $4x - 3y + 1 = 2$.

(a) Budeme způsobem, na nějž jsme zvyklí například z tělese reálných čísel upravovat rovnici ekvivalentním úpravami. Nejprve od obou stran odečteme hodnotu 4, což v $\mathbb{Z}_5$ znamená přičíst hodnotu 1 (vždyť $-4 = 1$) a dostaneme ekvivalentní rovnici $3x = 2$. Nyní vydělíme trojkou tj. vynásobíme číslem $\frac{1}{3} = 3^{-1} = 2$ a dostaneme jediné řešení $x = 4$.

(b) Postupujeme jako v úloze (a). Nejprve odečteme od obou stran 1 a uvědomíme si, že $-3 = 2$. Obdržíme rovnici $4x + 2y = 1$, kde vezmeme $y = s \in \mathbb{Z}_5$ libovolně a zpětnou substitucí za dalšího využití ekvivalentních úprav dopočítáme

$$4x = 1 - 2s = 1 + 3s \Rightarrow x = 4^{-1}(1+3s) = 4(1+3s) = 4 + 2s.$$

Množina všech řešení je pětiprvková tvaru

$$\{\begin{pmatrix}4\\0\end{pmatrix}+s\begin{pmatrix}2\\1\end{pmatrix} \mid s\in\mathbb{Z}_5\}=\{\begin{pmatrix}4\\0\end{pmatrix},\begin{pmatrix}1\\1\end{pmatrix},\begin{pmatrix}3\\2\end{pmatrix},\begin{pmatrix}0\\3\end{pmatrix},\begin{pmatrix}2\\4\end{pmatrix}\}.$$

□

**3.4.** Najděte nad tělesem $\mathbb{Z}_7$ všechna řešení soustavy rovnic s maticí

a) $\left(\begin{array}{cccc|c}3&1&5&2&1\\3&2&4&6&1\\2&5&6&0&1\end{array}\right)$, b) $\left(\begin{array}{cccc|c}3&1&5&2&1\\3&2&4&6&2\\2&5&6&0&5\end{array}\right)$.

Opět upravíme rozšířené matici soustavy na odstupňované matici.

a)

$$\left(\begin{array}{cccc|c}3&1&5&2&1\\3&2&4&6&1\\2&5&6&0&1\end{array}\right)\sim\left(\begin{array}{cccc|c}3&1&5&2&1\\0&1&6&4&0\\0&2&5&1&5\end{array}\right)\sim\left(\begin{array}{cccc|c}3&1&5&2&1\\0&1&6&4&0\\0&0&0&0&5\end{array}\right)$$

Protože poslední řádek představuje rovnici $0=5$, která neplatí pro žádný vektor neznámých, je množina všech řešení soustavy prázdná.

b)

$$\left(\begin{array}{cccc|c}3&1&5&2&1\\3&2&4&6&2\\2&5&6&0&5\end{array}\right)\sim\left(\begin{array}{cccc|c}3&1&5&2&1\\0&1&6&4&1\\0&2&5&1&2\end{array}\right)\sim\left(\begin{array}{cccc|c}3&1&5&2&1\\0&1&6&4&1\\0&0&0&0&0\end{array}\right)$$

Tentokrát řešení soustavy existuje a my ho obvyklým způsobem nalezneme zpětnou substitucí pro volbu za volné proměnné $x_3=r$ a $x_4=s$:

$$x_2+6x_3+4x_4=1\Rightarrow x_2=1+x_3+3x_4=1+r+3s,$$

$$3x_1+x_2+5x_3+2x_4=1\Rightarrow x_1=3^{-1}(1+6x_2+2x_3+5x_4)=$$
$$=5(1+6(1+r+3s)+2r+5s)=5(r+2s)=5r+3s$$

Našli jsme množinu všech řešení soustavy:

$$\{\begin{pmatrix}0\\1\\0\\0\end{pmatrix}+r\cdot\begin{pmatrix}5\\1\\1\\0\end{pmatrix}+s\cdot\begin{pmatrix}3\\3\\0\\1\end{pmatrix} \mid r,s\in\mathbb{Z}_7\}.$$

□

**3.5.** Najděte nad tělesem $\mathbb{Z}_5$ všechna řešení soustavy rovnic s maticí

$$\left(\begin{array}{ccccc|c}3&1&1&2&4&1\\1&2&1&2&1&2\\4&3&0&1&3&4\end{array}\right).$$

Postupujeme stejně jako v předchozích úlohách. Nejprve rozšířenou matici stejnými elementárními úpravami upravíme na odstupňovanou matici a poté najdeme všechna řešení zpětnou substitucí:

$$\left(\begin{array}{ccccc|c}3&1&1&2&4&1\\1&2&1&2&1&2\\4&3&0&1&3&4\end{array}\right)\sim\left(\begin{array}{ccccc|c}3&1&1&2&4&1\\0&0&4&3&3&0\\0&0&1&3&4&1\end{array}\right)\sim\left(\begin{array}{ccccc|c}3&1&1&2&4&1\\0&0&1&3&4&1\\0&0&0&1&2&1\end{array}\right).$$

Položíme za volné proměnné $x_2 = s$ a $x_5 = t$, kde $s, t \in$ a obvyklým způsobem dopočítáme $x_4 = 1 + 3t$, $x_3 = 3 + 2t$ a $x_1 = 2 + 3s + t$. Nyní zbývá shrnout množinu všech dvaceti pěti řešení soustavy do množiny

$$\{\begin{pmatrix}2\\0\\3\\1\\0\end{pmatrix} + s\cdot\begin{pmatrix}3\\1\\0\\0\\0\end{pmatrix} + t\cdot\begin{pmatrix}1\\0\\2\\3\\1\end{pmatrix} \mid s, t \in \mathbb{Z}_5\}$$

□

**3.6.** Najděte nad tělesem komplexních čísel množinu všech řešení soustavy s maticí

$$\left(\begin{array}{ccc|c}1+i & i & 0 & i-1\\ 1 & 1-i & 2 & i\end{array}\right).$$

I tentokrát nejprve převedeme matici na odstupňovaný tvar:

$$\left(\begin{array}{ccc|c}1+i & i & 0 & i-1\\ 1 & 1-i & 2 & i\end{array}\right) \sim \left(\begin{array}{ccc|c}1 & 1-i & 2 & i\\ 1+i & i & 0 & i-1\end{array}\right) \sim$$

$$\left(\begin{array}{ccc|c}1 & 1-i & 2 & i\\ 0 & i-2 & -2-2i & 0\end{array}\right) \sim \left(\begin{array}{ccc|c}1 & 1-i & 2 & i\\ 0 & 5 & 2+6i & 0\end{array}\right).$$

Pro volnou proměnnou $z = t \in \mathbb{C}$ dostáváme $y = -(\frac{2}{5} + \frac{6}{5}i)t$ a

$$x = i - (1-i)y - 2z = i + (1-i)(\frac{2}{5} + \frac{6}{5}i)t - 2t = i + (-\frac{2}{5} + \frac{4}{5}i)t$$

Spočítali jsme, že množina všech řešení soustavy je právě

$$\{\begin{pmatrix}i\\0\\0\end{pmatrix} + t\begin{pmatrix}-\frac{2}{5}+\frac{4}{5}i\\ -\frac{2}{5}-\frac{6}{5}i\\ 1\end{pmatrix} \mid t \in \mathbb{C}\} = \{\begin{pmatrix}i\\0\\0\end{pmatrix} + t\begin{pmatrix}-2+4i\\ -2-6i\\ 5\end{pmatrix} \mid t \in \mathbb{C}\}.$$

□

**3.7.** Najděte v závislosti na parametru $a$ nad tělesem a) $\mathbb{Z}_5$, b) $\mathbb{Z}_7$ c) $\mathbb{Z}_{11}$ řešení soustavy rovnic z úlohy 2.6.

Stejně jako v úloze 2.6 převedeme soustavu do ekvivalentního odstupňovaného tvaru

$$\left(\begin{array}{ccc|c}1 & 1 & 3 & a\\ 2 & -a & 1 & 1\end{array}\right) \sim \left(\begin{array}{ccc|c}1 & 1 & 3 & a\\ 0 & a+2 & 5 & 2a-1\end{array}\right)$$

a provedeme obdobnou diskusi.

Nechť $\mathbf{a} = \mathbf{-2}$. Pak je $y$ volná proměnná a řešíme soustavu s maticí:

$$\left(\begin{array}{ccc|c}1 & 1 & 3 & -2\\ 0 & 0 & 5 & -5\end{array}\right)$$

V případech b) a c), kdy pracujeme s tělesem charakteristiky různé od pěti je postup stejný jako v 2.6, proto je množina všech řešení opět tvaru $\{(1,0,-1)^T + t(-1,1,0)^T \mid t \in \mathbf{T}\}$ pro těleso $\mathbf{T} = \mathbb{Z}_7, \mathbb{Z}_{11}$. V případě a), kdy pracujeme s tělesem $\mathbb{Z}_5$ se nám modulo 5 druhý řádek soustavy vynuluje:

$$\left(\begin{array}{ccc|c}1 & 1 & 3 & -2\\ 0 & 0 & 5 & -5\end{array}\right) = \left(\begin{array}{ccc|c}1 & 1 & 3 & 3\\ 0 & 0 & 0 & 0\end{array}\right)$$

Výše spočítané partikulární řešení po úpravě modulo 5 zůstává v platnosti (a bude tedy tvaru $(1,0,4)^T$), snadno lze ovšem také najít kanonické partikulární řešení pro nulové hodnoty obou volných proměnných $(3,0,0)^T$. Při výpočtu řešení homogenní soustavy máme dvě volné proměnné $x_2$ a $x_3$. Obvyklým postupem nyní najdeme nad $\mathbb{Z}_5$ dvě řešení $(4,1,0)^T$ a $(2,0,1)^T$ (jednočlenné) homogenní soustavy, všechna řešení jsou tedy tvaru

$$(1,0,4)^T + t\cdot(4,1,0)^T + s\cdot(2,0,1)^T \quad \text{pro} \quad s,t \in \mathbb{Z}_5.$$

Zjistili jsme , že všechna řešení tvoří pro $a=-2$ množina:

$$\text{a)}\{\begin{pmatrix}1\\0\\4\end{pmatrix} + t\begin{pmatrix}4\\1\\0\end{pmatrix} + s\begin{pmatrix}2\\0\\1\end{pmatrix} \mid s,t\in\mathbb{Z}_5\},$$

$$\text{b)}\{\begin{pmatrix}1\\0\\6\end{pmatrix} + t\begin{pmatrix}6\\1\\0\end{pmatrix} \mid t\in\mathbb{Z}_7\}, \qquad \text{c)}\{\begin{pmatrix}1\\0\\10\end{pmatrix} + t\begin{pmatrix}10\\1\\0\end{pmatrix} \mid t\in\mathbb{Z}_{11}\}.$$

V případě $\mathbf{a \neq -2}$, je volná proměnná $z$ a stačí využít výsledky úlohy 2.6:

$$\text{a)}\{\begin{pmatrix}\frac{a^2+1}{a+2}\\ \frac{2a+4}{a+2}\\ 0\end{pmatrix} + t\begin{pmatrix}3a+1\\0\\4a+3\end{pmatrix} \mid t\in\mathbb{Z}_5\}, \quad \text{b)}\{\begin{pmatrix}\frac{a^2+1}{a+2}\\ \frac{2a+6}{a+2}\\ 0\end{pmatrix} + t\begin{pmatrix}3a+1\\5\\6a+5\end{pmatrix} \mid t\in\mathbb{Z}_7\},$$

$$\text{c)}\begin{pmatrix}\frac{a^2+1}{a+2}\\ \frac{2a-1}{a+2}\\ 0\end{pmatrix} + t\begin{pmatrix}3a+1\\5\\10a+9\end{pmatrix} \mid t\in\mathbb{Z}_{11}\}$$

Závěrem poznamenejme, že symbol $\frac{c}{d}$ je v tělese $\mathbb{Z}_p$ výraz, který je třeba dopočítat, tedy že $\frac{c}{d} = c\cdot d^{-1}$. □

## 4. Počítání s maticemi

**4.1.** Uvažujme matice $\mathbf{A} = \begin{pmatrix}1&2\\3&5\end{pmatrix}$, $\mathbf{B} = \begin{pmatrix}1&0&-1\\1&2&1\end{pmatrix}$ a $\mathbf{C} = \begin{pmatrix}1&2&0\\3&5&1\end{pmatrix}$ nad tělesem $\mathbb{R}$, $\mathbb{Z}_7$ a $\mathbb{Z}_{11}$.

(a) Spočítejte součty $\mathbf{B}+\mathbf{C}$, $\mathbf{C}+\mathbf{B}$, $\mathbf{B}^T+\mathbf{C}^T$.
(b) Spočítejte součiny $\mathbf{A}\cdot\mathbf{B}$, $\mathbf{B}^T\cdot\mathbf{A}^T$, $\mathbf{B}^T\cdot\mathbf{A}$, $\mathbf{B}^T\cdot\mathbf{C}$, $\mathbf{C}^T\cdot\mathbf{B}$ a $5\cdot\mathbf{C}\cdot$.
(c) Spočítejte $\mathbf{A}\cdot(\mathbf{A}-\mathbf{B}\cdot\mathbf{C}^T) + (\mathbf{C}\cdot\mathbf{B}^T\cdot\mathbf{A}^T)^T - \mathbf{A}$.

Ve všech případech úlohu vyřešíme nejprve v tělese charakteristiky 0, tedy v reálných číslech a poté, obdobně jako tomu bylo v Příkladu 2.6 výsledek pouze upravíme modulu příslušné prvočíslo.

(a) Postupujeme nejprve přímo podle definice součtu matic:

$$\mathbf{B}+\mathbf{C} = \begin{pmatrix}1&0&-1\\1&2&1\end{pmatrix} + \begin{pmatrix}1&2&0\\3&5&1\end{pmatrix} = \begin{pmatrix}1+1&0+2&-1+0\\1+3&2+5&1+1\end{pmatrix} = \begin{pmatrix}2&2&-1\\4&7&2\end{pmatrix}.$$

Na přednášce bylo ukázáno, že je sčítání matic komutativní, nemusíme samozřejmě druhý součet počítat a přímo vidíme, že $\mathbf{C}+\mathbf{B} = \mathbf{B}+\mathbf{C} = \begin{pmatrix}2&2&-1\\4&7&2\end{pmatrix}$ nad $\mathbb{R}$ a

$\mathbf{C}+\mathbf{B} = \mathbf{B}+\mathbf{C} = \begin{pmatrix}2&2&6\\4&0&2\end{pmatrix}$ nad $\mathbb{Z}_7$ a $\mathbf{C}+\mathbf{B} = \mathbf{B}+\mathbf{C} = \begin{pmatrix}2&2&10\\4&7&2\end{pmatrix}$ nad $\mathbb{Z}_{11}$.

Podobně bylo na přednášce ověřeno, že $\mathbf{B}^T+\mathbf{C}^T=(\mathbf{B}+\mathbf{C})^T$, tedy nám stačí jen bez dalšího počítání transponovat matici $\mathbf{B}+\mathbf{C}$, abychom dostali $\mathbf{B}^T+\mathbf{C}^T=\begin{pmatrix}2&4\\2&7\\-1&2\end{pmatrix}$ nad tělesem reálných čísel,

$$\mathbf{B}^T+\mathbf{C}^T=\begin{pmatrix}2&4\\2&0\\6&2\end{pmatrix}\ \text{nad}\ \mathbb{Z}_7,\quad \text{a}\quad \mathbf{B}^T+\mathbf{C}^T=\begin{pmatrix}2&4\\2&7\\10&2\end{pmatrix}\ \text{nad}\ \mathbb{Z}_{11}.$$

(b) Opět nejprve postupujme bezprostředně podle definice, tentokrát se jedná o definici násobení matic: $\mathbf{A}\cdot\mathbf{B}=$

$$\begin{pmatrix}1&2\\3&5\end{pmatrix}\cdot\begin{pmatrix}1&0&-1\\1&2&1\end{pmatrix}=\begin{pmatrix}1\cdot1+2\cdot1&1\cdot0+2\cdot2&-1\cdot1+2\cdot1\\3\cdot1+5\cdot1&3\cdot0+5\cdot2&-3\cdot1+5\cdot1\end{pmatrix}=\begin{pmatrix}3&4&1\\8&10&2\end{pmatrix}.$$

Protože bylo na přednášce ověřeno, že $(\mathbf{A}\cdot\mathbf{B})^T=\mathbf{B}^T\cdot\mathbf{A}^T$, vidíme, že

$$\mathbf{B}^T\cdot\mathbf{A}^T=\begin{pmatrix}3&4&1\\8&10&2\end{pmatrix}^T=\begin{pmatrix}3&8\\4&10\\1&2\end{pmatrix}.$$

To nám ovšem nepomůže pro výpočet $\mathbf{B}^T\cdot\mathbf{A}$, který opět provedeme podle definice:

$$\mathbf{B}^T\cdot\mathbf{A}=\begin{pmatrix}1&1\\0&2\\-1&1\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&5\end{pmatrix}=\begin{pmatrix}4&7\\6&10\\2&3\end{pmatrix}.$$

Při výpočtu součinu $\mathbf{B}^T\cdot\mathbf{C}$ nám pomůže rozklad matice $\mathbf{C}$ na dva bloky $\mathbf{C}=(\mathbf{A}|\mathbf{S})$, kde $\mathbf{A}$ je matice s kterou pracujeme a $\mathbf{S}=\begin{pmatrix}0\\1\end{pmatrix}$. Výpočet nám usnadní jednak to, že jsme již spočítali součin $\mathbf{B}^T\cdot\mathbf{A}$ a dále pozorování, že součin $\mathbf{B}^T\cdot\mathbf{S}$ právě vybere z matice $\mathbf{B}^T$ druhý sloupec:

$$\mathbf{B}^T\cdot\mathbf{C}=(\mathbf{B}^T\cdot\mathbf{A}|\mathbf{B}^T\cdot\mathbf{S})=\begin{pmatrix}1&1\\0&2\\-1&1\end{pmatrix}\cdot\left(\begin{array}{cc|c}1&2&0\\3&5&1\end{array}\right)=\begin{pmatrix}4&7&1\\6&10&2\\2&3&1\end{pmatrix}.$$

Konečně $\mathbf{C}^T\cdot\mathbf{B}=\mathbf{C}^T\cdot(\mathbf{B}^T)^T=(\mathbf{B}^T\cdot\mathbf{C})^T=\begin{pmatrix}4&6&2\\7&10&3\\1&2&1\end{pmatrix}$ a

$$5\cdot\mathbf{C}=\begin{pmatrix}5\cdot1&5\cdot2&5\cdot0\\5\cdot3&5\cdot5&5\cdot1\end{pmatrix}=\begin{pmatrix}5&10&0\\15&25&5\end{pmatrix}.$$

Našli jsme výsledky v tělese reálných čísel a nyní je upravíme nad oběma konečnými tělesy:

$$\mathbf{A}\cdot\mathbf{B}=\begin{pmatrix}3&4&1\\1&3&2\end{pmatrix},\quad \mathbf{B}^T\cdot\mathbf{A}=\begin{pmatrix}4&0\\6&3\\2&3\end{pmatrix},\quad \mathbf{B}^T\cdot\mathbf{C}=\begin{pmatrix}4&0&1\\6&3&2\\2&3&1\end{pmatrix},$$

a $\mathbf{C}^T \cdot \mathbf{B} = \begin{pmatrix} 4 & 6 & 2 \\ 0 & 3 & 3 \\ 1 & 2 & 1 \end{pmatrix}$ a $5 \cdot \mathbf{C} = \begin{pmatrix} 5 & 3 & 0 \\ 1 & 4 & 5 \end{pmatrix}$ vše nad tělesem $\mathbb{Z}_7$. Obdobně

$$\mathbf{A} \cdot \mathbf{B} = \begin{pmatrix} 3 & 4 & 1 \\ 8 & 10 & 2 \end{pmatrix}, \quad \mathbf{B}^T \cdot \mathbf{A} = \begin{pmatrix} 4 & 7 \\ 6 & 10 \\ 2 & 3 \end{pmatrix}, \quad \mathbf{B}^T \cdot \mathbf{C} = \begin{pmatrix} 4 & 7 & 1 \\ 6 & 10 & 2 \\ 2 & 3 & 1 \end{pmatrix},$$

$\mathbf{C}^T \cdot \mathbf{B} = \begin{pmatrix} 4 & 6 & 2 \\ 7 & 10 & 3 \\ 1 & 2 & 1 \end{pmatrix}$ a $5 \cdot \mathbf{C} = \begin{pmatrix} 5 & 10 & 0 \\ 4 & 3 & 5 \end{pmatrix}$ vše nad tělesem $\mathbb{Z}_{11}$.

(c) Využijeme početních pravidel a nejprve upravíme:

$$\mathbf{A} \cdot (\mathbf{A} - \mathbf{B} \cdot \mathbf{C}^T) + (\mathbf{C} \cdot \mathbf{B}^T \cdot \mathbf{A}^T)^T - \mathbf{A} = \mathbf{A} \cdot \mathbf{A} - \mathbf{A} \cdot \mathbf{B} \cdot \mathbf{C}^T + (\mathbf{A}^T)^T \cdot (\mathbf{B}^T)^T \cdot \mathbf{C}^T - \mathbf{A} =$$
$$= \mathbf{A} \cdot (\mathbf{A} - \mathbf{I}_2) - \mathbf{A} \cdot \mathbf{B} \cdot \mathbf{C}^T + \mathbf{A} \cdot \mathbf{B} \cdot \mathbf{C}^T = \mathbf{A} \cdot (\mathbf{A} - \mathbf{I}_2).$$

Nyní snadno dopočítáme

$$\mathbf{A} \cdot (\mathbf{A} - \mathbf{I}_2) = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 15 & 26 \end{pmatrix} \text{ nad } \mathbb{R}$$

$$\mathbf{A} \cdot (\mathbf{A} - \mathbf{I}_2) = \begin{pmatrix} 6 & 3 \\ 1 & 5 \end{pmatrix} \text{ nad } \mathbb{Z}_7, \quad \text{a} \quad \mathbf{A} \cdot (\mathbf{A} - \mathbf{I}_2) = \begin{pmatrix} 6 & 10 \\ 4 & 4 \end{pmatrix} \text{ nad } \mathbb{Z}_{11}.$$

$\square$

**4.2.** Najděte nad tělesem $\mathbb{Z}_7$ všechny matice $\mathbf{X}$ splňující rovnost $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$, jestliže

$$\text{(a)} \ \mathbf{A} = \begin{pmatrix} 4 & 5 \\ 1 & 3 \end{pmatrix}, \ \mathbf{B} = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}, \quad \text{(b)} \ \mathbf{A} = \begin{pmatrix} 5 & 5 \\ 2 & 3 \end{pmatrix}, \ \mathbf{B} = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 1 & 1 \end{pmatrix},$$

(a) Hledaná matice $\mathbf{X}$ musí být zřejmě typu $2 \times 2$ tvaru $\mathbf{X} = (\mathbf{x}, \mathbf{y})$ pro dva sloupcové vektory, $\mathbf{x}, \mathbf{y} \in \mathbb{Z}_7^2$. Užitím definice násobení matic snadno nahlédneme, že pro $\mathbf{X}$ platí, že splňuje rovnost $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$, právě tehdy když

$$\mathbf{A}\mathbf{x} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{a} \quad \mathbf{A}\mathbf{y} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

Protože mají obě soustavy touž matici levých stran, můžeme soustavy zapsat do jedné matice s oběma vektory pravých stran vpravo a levé strany upravíme posloupností elementárních úprav na odstupňovanou matici:

$$\left(\begin{array}{cc|cc} 4 & 5 & 0 & 1 \\ 1 & 3 & 0 & 2 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 3 & 0 & 2 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Dostali jsme tedy dvě soustavy s rozšířenými maticemi

$$\left(\begin{array}{cc|c} 1 & 3 & 0 \\ 0 & 0 & 0 \end{array}\right) \quad \text{a} \quad \left(\begin{array}{cc|c} 1 & 3 & 2 \\ 0 & 0 & 0 \end{array}\right).$$

Nyní snadno obvyklým způsobem dopočítáme, že první soustavu řeší právě vektory $c \cdot (4,1)^T$ pro všechna $c \in \mathbb{Z}_7$ druhou soustavu řeší právě vektory $(2,0)^T + d \cdot (4,1)^T$ pro všechna $d \in \mathbb{Z}_7$. Zbývá všechna řešení soustav sepsat do řešení maticové rovnice. Tedy $\mathbf{X}$ je řešením maticové rovnice $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$, právě když $\mathbf{X}$ leží v množině $\{(\mathbf{x}, \mathbf{y}) | \exists c, d \in \mathbb{Z}_7 : \mathbf{x} = c \cdot \begin{pmatrix} 4 \\ 1 \end{pmatrix}, \mathbf{y} = \begin{pmatrix} 2 \\ 0 \end{pmatrix} d \cdot \begin{pmatrix} 4 \\ 1 \end{pmatrix}\} =$

$$= \{ \begin{pmatrix} 4c & 2 + 4d \\ c & d \end{pmatrix} \mid c, d \in \mathbb{Z}_7 \}.$$

(b) I tentokrát nejprve snadno zjistíme, že hledaná matice je typu $2 \times 3$, sestává ze tří sloupcových vektorů $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{Z}_7^2$ tak, že $\mathbf{X} = (\mathbf{x}, \mathbf{y}, \mathbf{z})$ a platí

$$\mathbf{Ax} = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \quad \mathbf{Ay} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \quad \text{a} \quad \mathbf{Az} = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$$

Stejně jako v (a) budeme hledat řešení všech soustav najednou:

$$\sim \left(\begin{array}{cc|ccc} 5 & 5 & 1 & 2 & 5 \\ 0 & 1 & 4 & 3 & 6 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 5 & 0 & 2 & 1 & 3 \\ 0 & 1 & 4 & 3 & 6 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 1 & 0 & 6 & 3 & 2 \\ 0 & 1 & 4 & 3 & 6 \end{array}\right).$$

Matici levých stran se nám postupně podařilo upravit na jednotkovou matici, z níž okamžitě odečteme řešení jednotlivých neznámých:

$$\mathbf{x} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mathbf{x} = \begin{pmatrix} 6 \\ 4 \end{pmatrix}, \quad \mathbf{y} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mathbf{y} = \begin{pmatrix} 3 \\ 3 \end{pmatrix} \quad \text{a} \quad \mathbf{z} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mathbf{z} = \begin{pmatrix} 2 \\ 6 \end{pmatrix}$$

Zjistili jsme, že existuje právě jedno řešení rovnice $\mathbf{X} = \begin{pmatrix} 6 & 3 & 2 \\ 4 & 3 & 6 \end{pmatrix}$. □

**4.3.** Uvažujme matice $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$ a $\mathbf{B} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ nad tělesem $\mathbb{Z}_5$ a definujme zobrazení $f_\mathbf{A} : \mathbb{Z}_5^2 \to \mathbb{Z}_5^2$ a $f_\mathbf{B} : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ předpisy $f_\mathbf{A}(\mathbf{v}) = \mathbf{Av}$ a $f_\mathbf{B}(\mathbf{v}) = \mathbf{Bv}$

(a) Rozhodněte, zda je $f_\mathbf{A}$ či $f_\mathbf{B}$ prosté zobrazení.
(b) Rozhodněte, zda je $f_\mathbf{A}$ či $f_\mathbf{B}$ zobrazení na.
(c) Najděte všechny vektory $\mathbf{v} \in \mathbb{Z}_5^3$, pro něž je $f_\mathbf{B}(\mathbf{v}) = (0,0)^T$
(d) Najděte všechny vektory $\mathbf{v} \in \mathbb{Z}_5^3$, pro něž je $f_\mathbf{B}(\mathbf{v}) = (1,2)^T$

(a) Připomeňme, že je zobrazení $f_\mathbf{A}$ prosté, jestliže $f_\mathbf{A}(\mathbf{u}) = f_\mathbf{A}(\mathbf{v}) \implies \mathbf{u} = \mathbf{v}$. Protože $f_\mathbf{A}(\mathbf{u}) = f_\mathbf{A}(\mathbf{v})$, právě když $f_\mathbf{A}(\mathbf{u} - \mathbf{v}) = f_\mathbf{A}(\mathbf{u}) - f_\mathbf{A}(\mathbf{v}) = 0$, lze ekvivalentně prostotu zobrazení $f_\mathbf{A}$ vyjádřit podmínkou $f_\mathbf{A}(\mathbf{u}) = 0 \implies \mathbf{u} = 0$. Tedy nám stačí zjistit, zda mají soustavy rovnic $\mathbf{Ax} = (0,0)^T$ a $\mathbf{Bx} = (0,0)^T$ nějaké nenulové řešení. V obou případech po jediné ekvivalentní úpravě vidíme, že nenulové řešení existují, v prvním případě například $f_\mathbf{A}((3,1)^T) = (0,0)^T = f_\mathbf{A}((0,0)^T)$ a v druhém příkladě například $f_\mathbf{B}((4,1,1)^T) = (0,0)^T = f_\mathbf{B}((0,0,0)^T)$, proto zobrazení $f_\mathbf{A}$ ani $f_\mathbf{B}$ není podle definice prosté.

(b) Opět se úloha redukuje na otázku řešení soustavy rovnic s danou maticí. Tentokrát se ptáme, zda pro každou pravou stranu existuje řešení. V prvním případě vidíme, že nikoli, například pro pravou stranu $(1,0)^T$ vidíme, že řešení soustavy $\mathbf{Ax} = (1,0)^T$ neexistuje. V druhém případě vidíme, že odstupňovaný tvar matice $\mathbf{B}$ nemá žádný nulový řádek, tedy pivoty každé soustavy s maticí levých stran $\mathbf{B}$ leží v části matice odpovídající levým stranám, proto řešení vždy existuje. Tedy $f_\mathbf{A}$ není na, zatímco $f_\mathbf{B}$ je zobrazení na $\mathbb{Z}_5^2$.

(c) Stačí, abychom obvyklým způsobem vyřešili homogenní soustavu rovnic s maticí

$$\mathbf{B} \sim \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 4 \end{pmatrix}.$$

Obvyklým způsobem zjistíme, že vektor $\mathbf{v}$ splňuje $f_\mathbf{B}(\mathbf{v}) = (0,0)^T$, právě když leží v množině $\{t \cdot \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix} \mid t \in \mathbb{Z}_5\}$.

(d) Tentokrát standardně řešíme soustavu rovnic tvaru $\mathbf{Bx} = (1,2)^T$ s maticovým zápisem

$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & 1 & 1 \\ 0 & 1 & 4 & 1 \end{array}\right).$$

Spočítáme jedno partikulární řešení $(1,1,0)^T$ a využijeme výsledku (c), vidíme, že $\mathbf{v}$ splňuje $f_{\mathbf{B}}(\mathbf{v}) = (0,0)^T$, právě když leží v množině $\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix} \mid t \in \mathbb{Z}_5 \}$. □

**4.4.** Definujme zobrazení $f_{\mathbf{A}} : \mathbb{Q}^2 \to \mathbb{Q}^2$ předpisem $f_{\mathbf{A}}(\mathbf{v}) = \mathbf{Av}$ pro racionální matici $\mathbf{A} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$.

(a) Spočítejte jádro matice $\mathbf{A}$,
(b) dokažte, že je $f_{\mathbf{A}}$ bijekce,
(c) existuje-li, najděte racionální matici $\mathbf{X}$, pro níž $\mathbf{AX} = \mathbf{I}_2$,
(d) existuje-li, najděte matici $\mathbf{B}$, pro niž platí $f_{\mathbf{B}} \circ f_{\mathbf{A}} = f_{\mathbf{A}} \circ f_{\mathbf{B}} = \mathrm{Id}$, tedy $f_{\mathbf{B}} = f_{\mathbf{A}}^{-1}$, kde je $f_{\mathbf{B}}$ definováno předpisem $f_{\mathbf{B}}(\mathbf{v}) = \mathbf{Bv}$.
(e) spočítejte součin $\mathbf{X} \cdot \mathbf{A}$.

(a) Jádro matice je právě množina všech řešení homogenní soustavy rovnic s danou maticí, tj. $\mathrm{Ker}\,\mathbf{A} = \{\mathbf{x} \in \mathbb{Q}^2 |\ \mathbf{A}\,\mathbf{x} = \mathbf{0}\}$. Standardním postupem v jediném kroku upravíme matici $\mathbf{A}$ na odstupňovanou

$$\begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 \\ 0 & \frac{-1}{2} \end{pmatrix}$$

a vidíme, že matice levých stran neobsahuje žádný sloupec odpovídající volné proměnné, tudíž jediné řešení soustavy je triviální a $\mathrm{Ker}\,\mathbf{A} = \{\mathbf{0}\}$.

(b) Máme dokázat, že je zobrazení dané maticí $\mathbf{A}$ prosté a na, tedy máme ukázat, že pro každý vektor $\mathbf{v} \in \mathbb{Q}^2$ existuje právě jeden vektor $\mathbf{x} \in \mathbb{Q}^2$, pro který $f_{\mathbf{A}}(\mathbf{x}) = \mathbf{A}\,\mathbf{x} = \mathbf{v}$. Opět tedy řešíme soustavy rovnic. Uvědomíme-li si, že podle Věty 4.33 z přednášky je každé řešení soustavy rovnic s maticí $\mathbf{A}$ tvaru $\mathbf{u} + \mathrm{Ker}\,\mathbf{A}$ pro nějaké partikulární řešení, stačí pro ověření prostoty zobrazení zjistit, zda je jádro $\mathrm{Ker}\,\mathbf{A}$ jednoprvkové. To jsme ovšem už spočítali v úloze (a). Navíc jsme v (a) zjistili, že odstupňovaný tvar matice $\mathbf{A}$ neobsahuje žádný nulový řádek, tedy pro každou pravou stranu $\mathbf{v}$ umíme soustavu $\mathbf{A}\,\mathbf{x} = \mathbf{v}$ vyřešit. Tím máme ověřeno, že je zobrazení $f_{\mathbf{A}}$ prosté i na.

(c) Budeme postupovat stejně jako v úloze 4.2, tj řešíme dvě soustavy rovnic se stejnou maticí levých stran

$$\mathbf{A}\,\mathbf{x} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \mathbf{A}\,\mathbf{y} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

a hledanou maticí (existují-li obě řešení) sestavíme ze sloupců $\mathbf{X} = (\mathbf{x}, \mathbf{y})$. Obě soustavy přitom upravujeme společně v jedné rozšířené matici.

$$\left(\begin{array}{cc|cc} 2 & 3 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} -1 & -1 & 1 & -1 \\ 3 & 4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} -1 & -1 & 1 & -1 \\ 0 & 1 & 3 & -2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cc|cc} 1 & 1 & -1 & 1 \\ 0 & 1 & 3 & -2 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & -4 & 3 \\ 0 & 1 & 3 & -2 \end{array}\right).$$

Postupně jsme odčítali druhý řádek od prvního, přičítali trojnásobek prvního řádku ke druhému, vynásobili první řádek hodnotou $-1$ a odečetli druhý řádek od prvního, abychom zjistili, že $\mathbf{X} = \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix}$. Všimněme si, že upravením levé strany matice na jednotkovou znamená, že už nemusíme dopočítávat sloupce matice $\mathbf{X}$, protože se na levé straně upravené matice hledaná matice $\mathbf{X}$ objeví.

(d) Využitím definice zobrazení $f_{\mathbf{A}}$ a $f_{\mathbf{B}}$ pro každý vektor $\mathbf{v} \in \mathbb{Q}^2$ dostaneme

$$f_{\mathbf{A}} \circ f_{\mathbf{B}}(\mathbf{v}) = f_{\mathbf{A}}(\mathbf{B} \cdot \mathbf{v}) = \mathbf{A} \cdot \mathbf{B} \cdot \mathbf{v}\,.$$

položíme-li tedy $\mathbf{B} = \mathbf{X} = \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix}$, tj. vezmeme matici nalezenou v úloze (c), obdržíme pro každé $\mathbf{v} \in \mathbb{Q}^2$

$$f_{\mathbf{A}} \circ f_{\mathbf{B}}(\mathbf{v}) = \mathbf{A} \cdot (\mathbf{X} \cdot \mathbf{v}) = (\mathbf{A} \cdot \mathbf{X}) \cdot \mathbf{v} = \mathbf{I}_2 \cdot \mathbf{v} = \mathbf{v}\,.$$

Tím jsme dokázali, že $f_{\mathbf{A}} \circ f_{\mathbf{B}} = \mathrm{Id}$. Protože je $f_{\mathbf{A}}$ bijekce, víme že existuje $f_{\mathbf{A}}^{-1}$, proto

$$f_{\mathbf{A}}^{-1} = f_{\mathbf{A}}^{-1} \circ \mathrm{Id} = f_{\mathbf{A}}^{-1} \circ (f_{\mathbf{A}} \circ f_{\mathbf{B}}) = (f_{\mathbf{A}}^{-1} \circ f_{\mathbf{A}}) \circ f_{\mathbf{B}} = \mathrm{Id} \circ f_{\mathbf{B}} = f_{\mathbf{B}},$$

proto i $f_{\mathbf{B}} \circ f_{\mathbf{A}} = \mathrm{Id}$.

(e) Přímým výpočtem lze snadno zjistit, že $\mathbf{X} \cdot \mathbf{A} = \mathbf{I}_2$. Stejný závěr ovšem plyne také z pozorování úlohy (d), že $f_{\mathbf{B}} \circ f_{\mathbf{A}} = \mathrm{Id}$. □

**4.5.** Uvažujme matici $\mathbf{B}$ a zobrazení $f_{\mathbf{B}} : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ z úlohy 4.3. nad tělesem $\mathbb{Z}_5$ a definujme zobrazení $f_{\mathbf{A}} : \mathbb{Z}_5^2 \to \mathbb{Z}_5^2$ a $f_{\mathbf{B}} : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ předpisy $f_{\mathbf{A}}(\mathbf{v}) = \mathbf{A}\mathbf{v}$ a $f_{\mathbf{B}}(\mathbf{v}) = \mathbf{B}\mathbf{v}$

(a) Najděte všechny matice $\mathbf{X}$ nad $\mathbb{Z}_5$, pro níž $\mathbf{B}\mathbf{X} = \mathbf{I}_2$,
(b) najděte všechny matice $\mathbf{Y}$ nad $\mathbb{Z}_5$, pro níž $\mathbf{Y}\mathbf{B} = \mathbf{I}_3$.

(a) Postupujeme obdobně jako v předchozí úloze. Nejprve řešíme soustavy rovnic se společnou maticí levých stran $\mathbf{B}\,\mathbf{x} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \mathbf{B}\,\mathbf{y} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ :

$$\left(\begin{array}{ccc|cc} 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 4 & 4 & 1 \end{array}\right).$$

Zpětnou substitucí pro hodnotu třetí proměnné 0 získáme dvě partikulární řešení soustav, které umístíme do sloupců matice $\mathbf{X} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \\ 0 & 0 \end{pmatrix}$. Využijeme-li jádro

$$\mathrm{Ker}\,\mathbf{B} = \{t \cdot \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix} \mid t \in \mathbb{Z}_5\}$$

nalezené v úloze 4.3, snadno popíšeme množinu všech matic $\mathbf{X}$ splňující $\mathbf{B}\mathbf{X} = \mathbf{I}_2$:

$$\{\begin{pmatrix} 1 & 0 \\ 4 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 4s & 4t \\ s & t \\ s & t \end{pmatrix} \mid s,t \in \mathbb{Z}_5\} = \{\begin{pmatrix} 4s+1 & 4t \\ s+4 & t+1 \\ s & t \end{pmatrix} \mid s,t \in \mathbb{Z}_5\}$$

(b) Tentokrát můžeme buď pomocí transpozice a řešení soustav rovnic přímočaře, byť poněkud těžkopádně spočítat, že požadované matice $\mathbf{Y}$ žádná neexistuje, nebo lze zopakovat úvahu úlohy 4.4(d). Kdyby totiž matice $\mathbf{Y}$ existovala, muselo by pro indukované zobrazení $f_{\mathbf{Y}}$ platit, že $f_{\mathbf{Y}} \circ f_{\mathbf{B}} = \mathrm{Id}$. Zobrazení $f_{\mathbf{B}}$ ovšem není prosté, tedy žádné zobrazení $g$ splňující $g \circ f_{\mathbf{B}} = \mathrm{Id}$ nemůže existovat, tedy množina všech matic $\mathbf{Y}$ je prázdná □

**4.6.** Existuje-li, najděte matici $\mathbf{X}$ splňující

(a) $\begin{pmatrix} 1 & 2 & 1 \\ -2 & -3 & 1 \\ 2 & 4 & 3 \end{pmatrix} \cdot \mathbf{X} = \mathbf{I}_3$ nad tělesem racionálních čísel,

(b) $\begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix} \cdot \mathbf{X} = \mathbf{I}_2$ nad tělesem $\mathbb{Z}_5$,

(c) $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \cdot \mathbf{X} = \mathbf{I}_4$ nad tělesem $\mathbb{Z}_2$.

(a) Počítáme obdobně jako v úloze 4.4:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ -2 & -3 & 1 & 0 & 1 & 0 \\ 2 & 4 & 3 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 1 & -2 & 0 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 2 & 0 & 3 & 0 & -1 \\ 0 & 1 & 0 & 8 & 1 & -3 \\ 0 & 0 & 1 & -2 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -13 & -2 & 5 \\ 0 & 1 & 0 & 8 & 1 & -3 \\ 0 & 0 & 1 & -2 & 0 & 1 \end{array}\right).$$

Vidíme, že $\mathbf{X} = \begin{pmatrix} -13 & -2 & 5 \\ 8 & 1 & -3 \\ -2 & 0 & 1 \end{pmatrix}$.

(b) Opět upravujeme řádky rozšířené matice nad tělesem $\mathbb{Z}_5$:

$$\left(\begin{array}{cc|cc} 2 & 2 & 1 & 0 \\ 3 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 2 & 2 & 1 & 0 \\ 0 & 3 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 1 & 3 & 0 \\ 0 & 1 & 2 & 2 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 1 & 3 \\ 0 & 1 & 2 & 2 \end{array}\right)$$

Postupně jsme 1) přičetli 1. řádek ke 2. (protože $-3 = 2$ v $\mathbb{Z}_5$), 2) vynásobili 1. řádek číslem 3 a 2. řádek číslem 2 (protože $2^{-1} = 3$ a $3^{-1} = 2$ v $\mathbb{Z}_5$), 3) odečetli 2. řádek od 1. nebo ekvivalentně řečeno přičetli 4-násobek 2. řádku k 1. (protože $-4 = 1$ v $\mathbb{Z}_5$).

Nyní vidíme, že $\mathbf{X} = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$ nad tělesem $\mathbb{Z}_5$.

(c) Postupujeme standardně, přičemž nejprve přičteme všechny níže položené řádky k prvnímu a poté první řádek přičteme k níže položeným řádkům:

$$\left(\begin{array}{cccc|cccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right).$$

Spočítali jsme, že $\mathbf{X} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$. $\square$

**4.7.** Rozhodněte, které z následujících matic jsou regulární. K regulárním maticím najděte jejich inverzní matice.

(a) $\mathbf{B} = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$ nad tělesem racionálních čísel,

(b) $\mathbf{C} = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$ nad tělesem reálných čísel a nad tělesem $\mathbb{Z}_5$,

(c) $\mathbf{D} = \begin{pmatrix} 1+i & 1 \\ 2 & 3-i \end{pmatrix}$ nad tělesem komplexních čísel.

(f) $\mathbf{G} = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 2 & 6 \\ 1 & 0 & 5 \end{pmatrix}$ nad tělesem $\mathbb{Z}_7$,

(g) $\mathbf{G}^T$ nad tělesem $\mathbb{Z}_7$

Potřebujeme nejprve zjistit, zda odstupňovaná matice každé ze uvedených čtvercových matic obsahuje či neobsahuje nulový řádek. V prvním případě jde o singulární a v druhém o regulární matici. Inverzní matice potom počítáme stejně jako v příkladu 4.6.

(a) Jedinou úpravou dostaneme $\mathbf{B} \sim \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$, tudíž matice $\mathbf{B}$ není regulární.

(b) Opět jedinou elementární úpravou dostaneme, že $\mathbf{C} \sim \begin{pmatrix} 1 & 2 \\ 0 & -5 \end{pmatrix}$ nad tělesem reálných čísel, což znamená, že je matice regulární. Nad tělesem $\mathbb{Z}_5$ matici upravíme modulo 5, tedy $\mathbf{C} \sim \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ a matice $\mathbf{C}$ je nad $\mathbb{Z}_5$ singulární. Zbývá najít inverzní matici $\mathbf{C}$ nad $\mathbb{R}$:

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -5 & -3 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & -\frac{1}{5} & \frac{2}{5} \\ 0 & 1 & \frac{3}{5} & -\frac{1}{5} \end{array}\right) \sim$$

Dostali jsme, že $\mathbf{C}^{-1} = \frac{1}{5} \cdot \begin{pmatrix} -1 & 2 \\ 3 & -1 \end{pmatrix}$.

(c) Postupujeme jako v (b) s využitím aritmetiky komplexních čísel, během výpočtu přitom zjistíme, že inverz existuje:

$$\left(\begin{array}{cc|cc} 1+i & 1 & 1 & 0 \\ 2 & 3-i & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1+i & 1 & 1 & 0 \\ 0 & 2 & -1+i & 1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cc|cc} 1 & \frac{1-i}{2} & \frac{1-i}{2} & 0 \\ 0 & 1 & \frac{i-1}{2} & \frac{1}{2} \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & \frac{1-2i}{2} & \frac{i-1}{4} \\ 0 & 1 & \frac{i-1}{2} & \frac{1}{2} \end{array}\right)$$

Spočítali jsme, že $\mathbf{D}^{-1} = \begin{pmatrix} \frac{1-2i}{2} & \frac{i-1}{4} \\ \frac{i-1}{2} & \frac{1}{2} \end{pmatrix} = \frac{1}{4} \begin{pmatrix} 2-4i & i-1 \\ 2i-2 & 2 \end{pmatrix}$.

(d) Počítáme tentokrát nad $\mathbb{Z}_7$:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 4 & 1 & 0 & 0 \\ 3 & 2 & 6 & 0 & 1 & 0 \\ 1 & 0 & 5 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 5 & 0 & 0 & 1 \\ 0 & 2 & 5 & 0 & 1 & 4 \\ 0 & 2 & 6 & 1 & 0 & 6 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2 & 5 & 5 \\ 0 & 1 & 0 & 1 & 3 & 4 \\ 0 & 0 & 1 & 1 & 6 & 2 \end{array}\right).$$

Dostali jsme $\mathbf{G}^{-1} = \begin{pmatrix} 2 & 5 & 5 \\ 1 & 3 & 4 \\ 1 & 6 & 2 \end{pmatrix}$.

(e) Tentokrát pouze využijeme předchozí výsledek a tvrzení z přednášky, které říká, že $(\mathbf{G}^T)^{-1} = (\mathbf{G}^{-1})^T = \begin{pmatrix} 2 & 5 & 5 \\ 1 & 3 & 4 \\ 1 & 6 & 2 \end{pmatrix}^T = \begin{pmatrix} 2 & 1 & 1 \\ 5 & 3 & 6 \\ 5 & 4 & 2 \end{pmatrix}$. □

**4.8.** Napište všechny regulární matice z předchozí úlohy jako součin elementárních matic.

Využijeme postup důkazu Věty 4.66. Stačí nám tedy zaznamenat inverzní elementární úpravy k těm, které jsme prováděli při převodu matice na inverzní, do elementárních matic:

Matici $\mathbf{C} = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$ nad tělesem reálných čísel jsme převedli na jednotkovou tak, že jsme nejprve odečetli trojnásobek prvního řádku k druhému, poté vydělili druhý řádek číslem $-5$ a nakonec odečetli dvojnásobek druhého řádku od prvního. To znamená, že

$$\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & \frac{-1}{5} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

proto hledané elementární matice dostáváme přenásobením rovnosti zleva příslušnými inverzními elementárními maticemi, které jsou samozřejmě také elementární:

$$\mathbf{C} = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 0 & \frac{-1}{5} \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

V případě matice $\mathbf{D} = \begin{pmatrix} 1+i & 1 \\ 2 & 3-i \end{pmatrix}$ nad tělesem komplexních čísel jsme postupně upravovali: 1) $(1-i)$-násobek prvního řádku jsme odečetli od druhého, 2) prvního řádek jsme vynásobili hodnotou $\frac{1}{1+i}$ a druhý řádek hodnotou $\frac{1}{2}$ 3) $\frac{1-i}{2}$-násobek druhého řádku jsme odečetli od prvního. Nyní zbývá elementární matice opačných elementárních úprav sepsat do matic

$$\begin{pmatrix} 1+i & 1 \\ 2 & 3-i \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1-i & 1 \end{pmatrix} \cdot \begin{pmatrix} 1+i & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1-i}{2} \\ 0 & 1 \end{pmatrix}.$$

Podobně pro matici $\mathbf{G} = \begin{pmatrix} 1 & 2 & 4 \\ 3 & 2 & 6 \\ 1 & 0 & 5 \end{pmatrix}$ nad tělesem $\mathbb{Z}_7$ stačí zaznamenat provedené elementární úpravy do inverzních elementárních matic $\mathbf{G} =$

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Konečně pro matici transponovanou ke $\mathbf{G}$ stačí transponovat celý součin elementárních matic, tedy $\mathbf{G}^T =$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 5 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

□

**4.9.** Rozhodněte, pro která $a$ z tělesa je matice $\mathbf{A}_a$ regulární a pro tato $a$ spočítejte matici $\mathbf{A}_a^{-1}$.

(a) $\mathbf{A}_a = \begin{pmatrix} 2 & a \\ 3 & 0 \end{pmatrix}$ nad tělesem $\mathbb{Z}_7$,

(b) $\mathbf{A}_a = \begin{pmatrix} 1 & a \\ a & 2a-1 \end{pmatrix}$ nad tělesem $\mathbb{Q}$,

(c) $\mathbf{A}_a = \begin{pmatrix} a & 1 & 0 \\ 1 & 0 & a \\ 1 & 2 & a \end{pmatrix}$ nad tělesem $\mathbb{Z}_5$.

Budeme obvyklým způsobem počítat inverzní matice a přitom zároveň provedeme diskusi, pro která $a$ inverzní matice existuje.

(a)

$$\left(\begin{array}{cc|cc} 2 & a & 1 & 0 \\ 3 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 3 & 0 & 0 & 1 \\ 2 & a & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 0 & 5 \\ 0 & a & 1 & 4 \end{array}\right)$$

Vidíme, že $\mathbf{A}_a$ regulární, právě když $a \neq 0$ a tehdy $\mathbf{A}_a^{-1} = \begin{pmatrix} 0 & 5 \\ a^{-1} & 4a^{-1} \end{pmatrix}$.

(b) Postupujeme stejně jako v (a):

$$\left(\begin{array}{cc|cc} 1 & a & 1 & 0 \\ a & 2a-1 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & a & 1 & 0 \\ 0 & 2a-1-a^2 & -a & 1 \end{array}\right)$$

Tentokrát je zřejmě matice $\mathbf{A}_a$ regulární, právě když $2a - 1 - a^2 = -(a-1)^2 \neq 1$, tedy právě když $a \neq 1$. Pro $a \in \mathbb{Q} \setminus \{1\}$ pokračujeme v úpravách:

$$\sim \left(\begin{array}{cc|cc} 1 & a & 1 & 0 \\ 0 & 1 & \frac{a}{(a-1)^2} & \frac{-1}{(a-1)^2} \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & \frac{1-2a}{(a-1)^2} & \frac{a}{(a-1)^2} \\ 0 & 1 & \frac{a}{(a-1)^2} & \frac{-1}{(a-1)^2} \end{array}\right)$$

Zjistili jsme, že $\mathbf{A}_a^{-1} = \frac{1}{(a-1)^2}\begin{pmatrix} 1-2a & a \\ a & -1 \end{pmatrix}$.

(c) Nejprve si všimněme, že pro $a = 0$ je poslední sloupec matice nulový, tedy matice $\mathbf{A}_0$ je singulární. Dále uvažujme jen $a \in \mathbb{Z}_5 \setminus \{0\}$:

$$\left(\begin{array}{ccc|ccc} a & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & a & 0 & 1 & 0 \\ 1 & 2 & a & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & a & 0 & 1 & 0 \\ 1 & 2 & a & 0 & 0 & 1 \\ a & 1 & 0 & 1 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & a & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 4 & 1 \\ 0 & 1 & 4a^2 & 1 & 4a & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|ccc} 1 & 0 & a & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 2 & 3 \\ 0 & 0 & 4a^2 & 1 & 4a+3 & 2 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & a^{-1} & 3a^{-1} & 2a^{-1} \\ 0 & 1 & 0 & 0 & 2 & 3 \\ 0 & 0 & 4a^2 & 1 & 4a+3 & 2 \end{array}\right) \sim$$

Nyní snadno dopočítáme, že $\mathbf{A}_a^{-1} = \begin{pmatrix} a^{-1} & 3a^{-1} & 2a^{-1} \\ 0 & 2 & 3 \\ \frac{4}{a^2} & \frac{a+2}{a^2} & \frac{3}{a^2} \end{pmatrix}$ pro $a \in \mathbb{Z}_5 \setminus \{0\}$. □

**4.10.** Spočítejte součiny reálných matic

(a) $\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 3 & 1 & -1 \\ 2 & 0 & -1 & 2 \end{pmatrix}$, (b) $\begin{pmatrix} 2 & 0 \\ -1 & 3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^{-1}$.

(a) Označme $\mathbf{A} = \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}$ a $\mathbf{B} = \begin{pmatrix} 1 & 3 & 1 & -1 \\ 2 & 0 & -1 & 2 \end{pmatrix}$. Rozšíříme-li matici $\mathbf{A}$ o matici $\mathbf{B}$ a budeme-li vzniklou matici $(\mathbf{A}|\mathbf{B})$ upravovat stejně jako v předchozích úlohách takovými elementárními úpravami, abychom vlevo obdrželi jednotkovou matici, snadno nahlédneme, že

$$(\mathbf{A}|\mathbf{B}) \sim \mathbf{A}^{-1} \cdot (\mathbf{A}|\mathbf{B}) = (\mathbf{I}_2|\mathbf{A}^{-1}\mathbf{B}),$$

Tedy vpravo dostaneme hledaný součin $\mathbf{A}^{-1}\mathbf{B}$. Počítejme:

$$\left(\begin{array}{cc|cccc} 2 & 3 & 1 & 3 & 1 & -1 \\ 1 & 1 & 2 & 0 & -1 & 2 \end{array}\right) \sim \left(\begin{array}{cc|cccc} 1 & 1 & 2 & 0 & -1 & 2 \\ 2 & 3 & 1 & 3 & 1 & -1 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cc|cccc} 1 & 1 & 2 & 0 & -1 & 2 \\ 0 & 1 & -3 & 3 & 3 & -5 \end{array}\right) \sim \left(\begin{array}{cc|cccc} 1 & 0 & 5 & -3 & -4 & 7 \\ 0 & 1 & -3 & 3 & 3 & -5 \end{array}\right).$$

Spočítali jsme, že $\begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 3 & 1 & -1 \\ 2 & 0 & -1 & 2 \end{pmatrix} = \begin{pmatrix} 5 & -3 & -4 & 7 \\ -3 & 3 & 3 & -5 \end{pmatrix}$. □

(b) Označme $\mathbf{C} = \begin{pmatrix} 2 & 0 \\ -1 & 3 \\ 1 & 2 \end{pmatrix}$ a $\mathbf{D} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$. Využijeme-li Tvrzení 4.20 a 4.65, dostaneme $(\mathbf{C} \cdot \mathbf{D}^{-1})^T = (\mathbf{D}^{-1})^T \cdot \mathbf{C}^T = (\mathbf{D}^T)^{-1} \cdot \mathbf{C}^T$, a proto můžeme postupovat stejným způsobem jako v bodu (a), ovšem pro součin transponovaných matic v obráceném pořadí:

$$\left(\begin{array}{cc|ccc} 3 & 2 & 2 & -1 & 1 \\ 4 & 3 & 0 & 3 & 2 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 12 & 8 & 8 & -4 & 4 \\ 12 & 9 & 0 & 9 & 6 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 3 & 2 & 2 & -1 & 1 \\ 0 & 1 & -8 & 13 & 2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{cc|ccc} 3 & 0 & 18 & -27 & -3 \\ 0 & 1 & -8 & 13 & 2 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 1 & 0 & 6 & -9 & -1 \\ 0 & 1 & -8 & 13 & 2 \end{array}\right).$$

Zjistili jsme, že $(\mathbf{D}^T)^{-1} \cdot \mathbf{C}^T = \begin{pmatrix} 6 & -9 & -1 \\ -8 & 13 & 2 \end{pmatrix}$, a proto $\mathbf{C} \cdot \mathbf{D}^{-1} = \begin{pmatrix} 6 & -8 \\ -9 & 13 \\ -1 & 2 \end{pmatrix}$. □

**4.11.** Existuje-li, najděte LU rozklad reálné matice:

(a) $\mathbf{A} = \begin{pmatrix} 2 & 2 \\ 4 & 9 \end{pmatrix}$, (b) $\mathbf{B} = \begin{pmatrix} 1 & 1 & 2 \\ -4 & -1 & 1 \\ 2 & 5 & -1 \end{pmatrix}$, (c) $\mathbf{C} = \begin{pmatrix} 2 & 1 & -2 \\ -2 & 2 & 3 \\ 2 & 7 & 2 \end{pmatrix}$,

(d) $\mathbf{D} = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 3 & 1 & 2 & 1 \\ 1 & 1 & 1 & 3 \\ 0 & 0 & 0 & 3 \end{pmatrix}$.

(a) Všimněme si, že stačí provést jedinou elementární úpravu třetího typu, abychom z matice $\mathbf{A}$ dostali odstupňovanou matici $\begin{pmatrix} 2 & 2 \\ 0 & 5 \end{pmatrix}$, což můžeme zapsat v maticové podobě pomocí násobení zleva příslušnou elementární maticí:

$$\begin{pmatrix} 2 & 2 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 4 & 9 \end{pmatrix}$$

Uvědomíme-li si, že inverzní matice $\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ je rovněž dolní trojúhelníková s jednotkami na diagonále a přenásobíme-li výše uvedenou rovnost zleva maticí

$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}^{-1}$, dostáváme

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 4 & 9 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 4 & 9 \end{pmatrix},$$

odkud vidíme, že LU rozklad matice $\mathbf{A}$ je $\mathbf{A} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 0 & 5 \end{pmatrix}$.

(b) I tentokrát budeme matici $\mathbf{B}$ upravovat elementárními úpravami. Příslušné úpravy si budeme pamatovat a poté si je přepíšeme v maticovém zápisu jako součin elementárních matic:

$$\mathbf{B} = \begin{pmatrix} 1 & 1 & 2 \\ -4 & -1 & 1 \\ 2 & 5 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 9 \\ 0 & 3 & -5 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 9 \\ 0 & 0 & -14 \end{pmatrix} = \mathbf{U}.$$

Při upravování jsme nepotřebovali přehazovat řádky (ani násobit řádek nenulovým skalárem), tedy dostali jsme $\mathbf{L}_k \dots \mathbf{L}_1 \mathbf{B} = \mathbf{U}$, kde $\mathbf{L}_i$ jsou všechno elementární transformační matice odpovídající přičtení výše položeného řádku k řádku níže položenému:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 4 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 2 \\ -4 & -1 & 1 \\ 2 & 5 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 9 \\ 0 & 0 & -14 \end{pmatrix}.$$

Matice $\mathbf{L}_i$ jsou zřejmě dolní trojúhelníkové s jednotkami na diagonále a okamžitě vidíme, že součin $\mathbf{L} = \mathbf{L}_1^{-1} \dots \mathbf{L}_k^{-1}$ rovněž dolní trojúhelníková matice s jednotkami na diagonále. Navíc $\mathbf{B} = \mathbf{LU}$. Tudíž jsme našli LU rozklad matice $\mathbf{B}$. Vidíme, že součin matic $\mathbf{L}_1^{-1} \dots \mathbf{L}_k^{-1}$ obsahuje na příslušných pozicích hodnoty jednotlivých elementárních matic (tj. $i$-tý řádek a $j$-tý sloupec, $i > j$, obsahuje hodnotu $c_{ij}$, právě když jsme během Gaussovy eliminace odečítali od $i$-tého řádku matice $\mathbf{B}$ a $c_{ij}$-násobek jejího $j$-tého řádku):

$$\mathbf{L} = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 2 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Našli jsme tedy (jednoznačně určený) LU rozklad

$$\begin{pmatrix} 1 & 1 & 2 \\ -4 & -1 & 1 \\ 2 & 5 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 2 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 0 & 3 & 9 \\ 0 & 0 & -14 \end{pmatrix}.$$

Všimněme si, že výsledná matice $\mathbf{L}$ obsahuje na $i$-tém řádku a $j$-tém sloupci právě opačnou hodnotu k násobku, jímž jsme násobili $j$-tý řádek při jeho přičítání k $i$-tému sloupci během elementárních úprav (tedy během Gaussovy eliminace). To, že se jedná o obecný způsob, jak nalézt dolní trojúhelníkovou matici LU rozkladu matice ukazuje důkazu Věty 4.69 z přednášky a na témže místě je ukázáno, že horní trojúhelníková matice LU rozkladu je právě odstupňovaná matice, kterou získáme Gaussovou eliminací.

(c) Tentokrát budeme postupovat jako v důkazu Věty 4.69, tedy stačí gaussovsky upravovat matici $\mathbf{C}$ a příslušné (opačné) hodnoty sestavovat do matice $\mathbf{L}$:

$$\begin{pmatrix} 2 & 1 & -2 \\ -2 & 2 & 3 \\ 2 & 7 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & -2 \\ 0 & 3 & 1 \\ 0 & 6 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & -2 \\ 0 & 3 & 1 \\ 0 & 0 & 2 \end{pmatrix},$$

kde jsme postupně odečetli 1) $-1$-násobek 1. řádku od 2., 2) 1-násobek 1. řádku od 3. a 3) 2-násobek 2. řádku od 3. Tedy dostáváme tedy LU rozklad

$$\begin{pmatrix} 2 & 1 & -2 \\ -2 & 2 & 3 \\ 2 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & -2 \\ 0 & 3 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

(d) Opět upravujeme gaussovou eliminací matici $\mathbf{D}$:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 3 & 1 & 2 & 1 \\ 1 & 1 & 1 & 3 \\ 0 & 0 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Provedené úpravy zaznamenáme do matice $\mathbf{L}$ a dostaneme hledaný LU rozklad

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 3 & 1 & 2 & 1 \\ 1 & 1 & 1 & 3 \\ 0 & 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \frac{3}{2} & 1 & 0 & 0 \\ \frac{1}{2} & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & -1 & 2 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

□

**4.12.** Pomocí LU rozkladu reálné matice $\mathbf{A} = \begin{pmatrix} 2 & 1 & -2 \\ -2 & 2 & 3 \\ 2 & 7 & 2 \end{pmatrix}$ spočítejte všechna řešení soustavy rovnic $\mathbf{Ax} = \mathbf{y}$ pro vektor pravých stran $\mathbf{y} = (-3, 2, -1)^{\mathrm{T}}$.

Máme-li LU rozklad matice $\mathbf{A} = \mathbf{LU}$ a uvažujeme-li nehomogenní soustavu rovnic $\mathbf{Ax}^{\mathrm{T}} = \mathbf{y}^{\mathrm{T}}$, potom můžeme úlohu rozdělit na dva jednodušší úkoly, najít nejprve řešení soustavy $\mathbf{Lz}^{\mathrm{T}} = \mathbf{y}^{\mathrm{T}}$ a poté soustavy $\mathbf{Ux}^{\mathrm{T}} = \mathbf{z}^{\mathrm{T}}$. V obou případech počítáme s trojúhelníkovými maticemi, takže při výpočtu už jen dosazujeme, aniž musíme matice jakkoli dále gaussovsky upravovat.

LU rozklad matice jsme už spočítali: $\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 & -2 \\ 0 & 3 & 1 \\ 0 & 0 & 2 \end{pmatrix}$. Potom pro pro vektor pravých stran $\mathbf{y} = (-3, 2, -1)$ spočítáme neznámé $\mathbf{z} = (z_1, z_2, z_3)$ přímou substitucí $z_1 = y_1 = -3$, dále $-1z_1 + z_2 = 3 + z_2 = y_2 = 2$, tedy $z_2 = -1$ a konečně $z_3 = -1 - 1 \cdot (-3) - 2 \cdot (-1) = 4$.

Nyní počítáme soustavu $\mathbf{Ux}^{\mathrm{T}} = \mathbf{z}^{\mathrm{T}}$ a tentokrát tedy postupujeme zpětnou substitucí: $2x_3 = z_3$, tedy $x_3 = 2$, dále $x_2 = \frac{-1-1\cdot 2}{3} = -1$ a $x_1 = \frac{-3-1\cdot(-1)+2\cdot 2}{2} = 1$. □

**4.13.** Existuje-li, najděte LU rozklad matic:

(a) $\mathbf{A} = \begin{pmatrix} 2 & 2 \\ 1 & 4 \end{pmatrix}$ nad tělesem $\mathbf{Z}_5$, (b) $\mathbf{B} = \begin{pmatrix} 2 & 1 & 2 \\ 3 & 1 & 4 \\ 1 & 0 & 3 \end{pmatrix}$ nad tělesem $\mathbf{Z}_5$,

(c) $\mathbf{B}$ nad tělesem $\mathbf{Z}_7$,

Postupujeme v 4.11 s počítáním v tělesech $\mathbf{Z}_5$ a $\mathbf{Z}_7$, tedy gaussovsky upravíme matici na matici $\mathbf{U}$ a příslušné hodnoty sepíšeme do matice $\mathbf{L}$:

(a) $\begin{pmatrix} 2 & 2 \\ 1 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 2 \\ 0 & 3 \end{pmatrix}$ a dostáváme LU rozklad $\begin{pmatrix} 2 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 2 \\ 0 & 3 \end{pmatrix}$.

(b)

$$\begin{pmatrix}2&1&2\\3&1&4\\1&0&3\end{pmatrix}\sim\begin{pmatrix}2&1&2\\0&2&1\\0&2&2\end{pmatrix}\sim\begin{pmatrix}2&1&2\\0&2&1\\0&0&1\end{pmatrix}.$$

Spočítali jsme LU rozklad matice $\mathbf{B}=\begin{pmatrix}1&0&0\\4&1&0\\3&1&1\end{pmatrix}\cdot\begin{pmatrix}2&1&2\\0&2&1\\0&0&1\end{pmatrix}$ nad tělesem $\mathbf{Z}_5$.

(c)

$$\begin{pmatrix}2&1&2\\3&1&4\\1&0&3\end{pmatrix}\sim\begin{pmatrix}2&1&2\\0&3&1\\0&3&2\end{pmatrix}\sim\begin{pmatrix}2&1&2\\0&3&1\\0&0&1\end{pmatrix}.$$

Spočítali jsme nad $\mathbf{Z}_7$ LU rozklad matice $\mathbf{B}=\begin{pmatrix}1&0&0\\5&1&0\\4&1&1\end{pmatrix}\cdot\begin{pmatrix}2&1&2\\0&3&1\\0&0&1\end{pmatrix}$. □

**4.14.** Pro reálnou matici $\mathbf{A}=\begin{pmatrix}1&1&2&2\\-1&-1&-2&1\\2&1&0&1\\2&2&-1&1\end{pmatrix}$ ověřte, že nemá LU-rozklad, najděte permutační matici $\mathbf{P}$ tak, aby matice $\mathbf{PA}$ měla LU rozklad a ten spočítejte.

Budeme matici postupně upravovat Gaussovu eliminaci, tj. budeme kanonickým způsobem, používat pouze přehazování řádků a přičítání násobku výše položeného k níže položenému řádku. Oba typy úprav budeme zaznamenávat (pravý sloupec jen čísluje řádky):

$$\left(\begin{array}{cccc|c}1&1&2&2&\mathit{1}\\-1&-1&-2&1&\mathit{2}\\2&1&0&1&\mathit{3}\\2&2&-1&1&\mathit{4}\end{array}\right)\sim\left(\begin{array}{cccc|c}1&1&2&2&\mathit{1}\\0&0&0&3&\mathit{2}\\0&-1&-4&-3&\mathit{3}\\0&0&-5&-3&\mathit{4}\end{array}\right)\sim\left(\begin{array}{cccc|c}1&1&2&2&\mathit{1}\\0&-1&-4&-3&\mathit{3}\\0&0&-5&-3&\mathit{4}\\0&0&0&3&\mathit{2}\end{array}\right).$$

Tedy permutační matice, kterou potřebujeme změnit původní matici $\mathbf{A}$, odpovídá permutaci řádků zachycené v pravém sloupci, čili $\mathbf{P}=\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&0&0&1\\0&1&0&0\end{pmatrix}$. Původním transformacím typu přičtení výše položeného řádku k níže položenému odpovídala matice $\mathbf{L}'=\begin{pmatrix}1&0&0&0\\-1&1&0&0\\2&0&1&0\\2&0&0&1\end{pmatrix}$, my ale musíme adekvátně matici $\mathbf{P}$, jako jsme to udělali i v průběhu důkazu Věty 5.4, změnit polohu upravovaných řádků, takže dostáváme LU rozklad matice $\mathbf{PA}$:

$$\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&0&0&1\\0&1&0&0\end{pmatrix}\begin{pmatrix}1&1&2&2\\-1&-1&-2&1\\2&1&0&1\\2&2&-1&1\end{pmatrix}=\begin{pmatrix}1&0&0&0\\2&1&0&0\\2&0&1&0\\-1&0&0&1\end{pmatrix}\begin{pmatrix}1&1&2&2\\0&-1&-4&-3\\0&0&-5&-3\\0&0&0&3\end{pmatrix}.$$

□

**4.15.** Existuje-li, najděte nad tělesem $\mathbb{Z}_3$ všechny matice $\mathbf{X}$ splňující

(a) $\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix} \cdot \mathbf{X} = \mathbf{I}_2$,

(b) $\mathbf{X} \cdot \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \mathbf{I}_3$.

(a) Počítáme obdobně jako v úlohách 4.2 a 4.6:

$$\left(\begin{array}{ccc|cc} 1 & 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 2 & 1 & 1 & 0 \\ 0 & 2 & 0 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 & 2 \end{array}\right)$$

Nyní zpětnou substitucí snando zjistíme, že $\mathbf{X} \in \{ \begin{pmatrix} 2+2s & 2+2t \\ 1 & 2 \\ s & t \end{pmatrix} \mid s, t \in \mathbb{Z}_3 \}$.

(b) Nyní buď můžeme zjistit, že hledaná matice $\mathbf{X}$ neexistuje, stejnými prostředky jako v předchozí úloze, nebo si všimneme, že otázka je ekvivalentní podmínce

$$\mathbf{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \mathbf{e}_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \in f_{\mathbf{A}^T}(\mathbb{Z}_3^2)$$

kde $\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ a zobrazení $f_{\mathbf{A}^T} : \mathbb{Z}_3^2 \to \mathbb{Z}_3^3$ je dáno předpisem $f_{\mathbf{A}^T}(\mathbf{v}) = \mathbf{A}^T\mathbf{v}$. Ovšem $f_{\mathbf{A}^T}(\mathbb{Z}_3^2)$ je právě řádkový vekltorový prostor matice $\mathbf{A}$, tedy má (nejvýše) devět prvků, zatímco podprostor, který by obsahoval všechny vektory $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ by musel obsahovat všechny jejich lineární kombinace, tedy všechny vektory lineárního prostoru $\mathbb{Z}_3^3$, tedy 27 různých vektorů, což není možné. Požadovaná matice tudíž neexistuje. $\square$

**4.16.** Najděte čtvercovou matici $\mathbf{A}$ nad tělesem $T$ řádu $n$ splňující podmínky $\mathbf{A}^2 = \mathbf{I}_n$ a $\mathbf{A} \neq \mathbf{I}_n$, jestliže

(a) $n = 1$ a $T = \mathbb{R}$,
(b) $n = 2$ a $T = \mathbb{R}$,
(c) $n = 2$ a $T = \mathbb{Z}_5$,
(d) $n = 3$ a $T = \mathbb{R}$,
(e) $n = 4$ a $T = \mathbb{Z}_2$.

(a) Čtvercové matice řádu 1 odpovídají prvkům těles, tedy se ptáme, kdy $a^2 = 1$ a $a \neq 1$ nad reálnými čísly. Okamžitě vidíme, že podmínku splňuje pouze matice $(-1)$.

(b) V úloze nám může pomoct geometrický náhled. Uvážíme-li matici zobrazení $f_{\mathbf{A}}$, hledáme taková zobrazení, která jsou sama k sobě inverzní. Ta ovšem snadno najdeme mezi symetriemi, například osová souměrnost podle osy x či y nebo souměrnost podle průsečíku os jsou zobrazení sama k sobě inverzní. Nyní stačí nahlédnout, že $\mathbf{A}_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ je maticí souměrnosti podle osy x, $\mathbf{A}_y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ je maticí souměrnosti podle osy y a $\mathbf{A}_o = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ je maticí souměrnosti podle počátku souřadnic, a že $\mathbf{A}_x^2 = \mathbf{A}_y^2 = \mathbf{A}_o^2 = \mathbf{I}_2$.

(c) V tomto případě nám sice geometrická představa chybí, ale algebraické důvody ukazují, že předchozí příklady matic

$$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 4\end{pmatrix},\quad \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}4 & 0\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}=\begin{pmatrix}4 & 0\\ 0 & 4\end{pmatrix}.$$

i nad tělesem $\mathbb{Z}_5$ splňují podmínku $\mathbf{A}^2=\mathbf{I}_2$. Poznamenejme ovšem, že existují i další matice splňují $\mathbf{A}^2=\mathbf{I}_2$ například matice $\begin{pmatrix}2 & 2\\ 1 & 3\end{pmatrix}$.

(d) Tentokrát můžeme použít geometrickou úvahu z (b), abychom si uvědomili, že osové souměrnosti s maticemi

$$\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix},\quad \begin{pmatrix}-1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix},\quad \begin{pmatrix}-1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 1\end{pmatrix},$$

symetrie podle rovin určených dvojicí os s maticemi

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -1\end{pmatrix},\quad \begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 1\end{pmatrix},\quad \begin{pmatrix}-1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},$$

stejně jako středová symetrie s maticí $\begin{pmatrix}-1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix}$ naši podmínku splňují.

(e) Nad tělesem $\mathbb{Z}_2$ platí, že $-1=1$, tedy úvahu z (b) využít nemůžeme. Přesto například matice $\mathbf{H}=\begin{pmatrix}0 & 1 & 1 & 1\\ 1 & 0 & 1 & 1\\ 1 & 1 & 0 & 1\\ 1 & 1 & 1 & 0\end{pmatrix}$ z úlohy 4.7(h) podmínku $\mathbf{H}^2=\mathbf{I}_4$ splňuje.

□

**4.17.** Najděte aspoň 4 reálné čtvercové matice $\mathbf{A}$ řádu 3, aby $\mathbf{A}^2=\mathbf{A}$ a $\mathbf{A}\neq\mathbf{I}_3$.

Podobně jako v předchozí úloze může využít geometrického náhledu. Uvážíme-li matici zobrazení $f_{\mathbf{A}}$, hledáme geometrická zobrazení, která se dvojí aplikací nezmění. Takovou podmínku splňují jistě kolmé projekce na rovinu či přímku, matice projekcí na rovinu určenou dvojicí os jsou potom tvaru

$$\begin{pmatrix}0 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{pmatrix},$$

zatímco matice projekcí na osy jsou

$$\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix},\quad \begin{pmatrix}0 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{pmatrix},\quad \begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}.$$

□

**4.18.** Mějme reálnou matici $\mathbf{M}=\begin{pmatrix}2 & 0\\ 1 & 3\end{pmatrix}$ řádu $n>1$. Najděte příklady (nekonečně mnoha) matic, které s $\mathbf{M}$ komutují.

Uvědomíme-li si, že je skalární násobení komutativní, dostaneme třídu matic $c\mathbf{I}_2 = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$ pro , které zřejmě komutují se všemi maticemi. D8le připomeňme, že $\mathbf{M} \cdot d\mathbf{M}^{-1} = c\mathbf{I}_2 = d\mathbf{M}^{-1} \cdot \mathbf{M}$. Tedy matice $d\mathbf{M}^{-1}$ pro každé $d \in \mathbb{R}$ komutuje s $\mathbf{M}$, vezmeme-li $c = 6d$ snadno spočítáme, že s $\mathbf{M}$ komutují matice $\begin{pmatrix} 3c & 0 \\ -c & 2c \end{pmatrix}$ pro každé $c \in \mathbb{R}$.

Dále pro každé přirozené $n$ máme $\mathbf{M} \cdot \mathbf{M}^n = \mathbf{M}^{n+1} = \mathbf{M}^n \cdot \mathbf{M}$ a $\mathbf{M} \cdot (\mathbf{M}^{-1})^n = (\mathbf{M}^{-1})^{n-1} = (\mathbf{M}^{-1})^n \cdot \mathbf{M}$, tedy matice $\mathbf{M}^n$ i $(\mathbf{M}^{-1})^n$ s $\mathbf{M}$ komutují. □

Připomeňme, že *Jordanova buňka* je matice tvaru $\mathbf{J}_\lambda = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & \dots & 0 & \lambda \end{pmatrix}$.

**4.19.** Je-li $\mathbf{J}_\lambda$ Jordanova buňka řádu $n$ nad obecným tělesem, dokažte, že

$$\mathbf{J}_\lambda^k = \begin{pmatrix} \lambda^k & \binom{k}{1}\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \dots & \binom{k}{n-1}\lambda^{k-n+1} \\ 0 & \lambda^k & \binom{k}{1}\lambda^{k-1} & \dots & \binom{k}{n-2}\lambda^{k-n+2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^k & \binom{k}{1}\lambda^{k-1} \\ 0 & 0 & \dots & 0 & \lambda^k \end{pmatrix},$$

kde definitoricky položíme $\binom{k}{r}\lambda_i^{k-r} = 0$ pro $r > k$.

Postupujeme indukcí. Pro $k = 1$ tvrzení zřejmě platí. Předpokládejme, že vzorec platí pro $k$ a dokažme ho pro $k + 1$. Budeme násobit $\mathbf{J}_\lambda^{k+1} = \mathbf{J}_\lambda \cdot \mathbf{J}_\lambda^k =$

$$= \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & \dots & 0 & \lambda \end{pmatrix} \cdot \begin{pmatrix} \lambda^k & \binom{k}{1}\lambda^{k-1} & \binom{k}{2}\lambda^{k-2} & \dots & \binom{k}{n-1}\lambda^{k-n+1} \\ 0 & \lambda^k & \binom{k}{1}\lambda^{k-1} & \dots & \binom{k}{n-2}\lambda^{k-n+2} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^k & \binom{k}{1}\lambda^{k-1} \\ 0 & 0 & \dots & 0 & \lambda^k \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda^{k+1} & (\binom{k}{1}+1)\lambda^k & (\binom{k}{2}+\binom{k}{1})\lambda^{k-1} & \dots & (\binom{k}{n-1}+\binom{k}{n-2})\lambda^{k-n+2} \\ 0 & \lambda^{k+1} & (\binom{k}{1}+1)\lambda^k & \dots & (\binom{k}{n-2}+\binom{k}{n-3})\lambda^{k-n+3} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{k+1} & (\binom{k}{1}+1)\lambda^k \\ 0 & 0 & \dots & 0 & \lambda^{k+1} \end{pmatrix} =$$

$$= \begin{pmatrix} \lambda^{k+1} & \binom{k+1}{1}\lambda^k & \binom{k+1}{2}\lambda^{k-1} & \dots & \binom{k+1}{n-1}\lambda^{k-n+2} \\ 0 & \lambda^{k+1} & \binom{k+1}{1}\lambda^k & \dots & \binom{k+1}{n-2}\lambda^{k-n+3} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda^{k+1} & \binom{k+1}{1}\lambda^k \\ 0 & 0 & \dots & 0 & \lambda^{k+1} \end{pmatrix},$$

kde jsme využili známého vztahu $\binom{k}{r} + \binom{k}{r-1} = \binom{k+1}{r}$. □

**4.20.** Spočítejte $\mathbf{A}^n$ pro

(a) $n = 45$ a $\mathbf{A} = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}$ nad tělesem $\mathbb{R}$,

(b) $n = 45$ a $\mathbf{A} = \begin{pmatrix} 1 & \frac{1}{3} & 0 \\ 0 & 1 & \frac{1}{3} \\ 0 & 0 & 1 \end{pmatrix}$ nad tělesem $\mathbb{R}$,

(c) $n = 13$ a $\mathbf{A} = \begin{pmatrix} 8 & 1 & 0 & 0 \\ 0 & 8 & 1 & 0 \\ 0 & 0 & 8 & 1 \\ 0 & 0 & 0 & 8 \end{pmatrix}$ nad tělesem $\mathbb{Z}_{13}$.

(a) Použijeme vzorečku odvozeného v úloze 4.19:

$$\mathbf{A}^{45} = \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}^{45} = \begin{pmatrix} 3^{45} & 45 \cdot 3^{44} & 990 \cdot 3^{43} \\ 0 & 3^{45} & 45 \cdot 3^{44} \\ 0 & 0 & 3^{45} \end{pmatrix}$$

(b) Všimněme si, že $\mathbf{A} = \frac{1}{3} \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}$, proto

$$\mathbf{A}^{45} = \frac{1}{3^{45}} \cdot \begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}^{45} = \frac{1}{3^{45}} \cdot \begin{pmatrix} 3^{45} & 45 \cdot 3^{44} & 990 \cdot 3^{43} \\ 0 & 3^{45} & 45 \cdot 3^{44} \\ 0 & 0 & 3^{45} \end{pmatrix} = \begin{pmatrix} 1 & 15 & 110 \\ 0 & 1 & 15 \\ 0 & 0 & 1 \end{pmatrix}.$$

(c) Uvědomíme-li si, že pro každé prvočíslo $p$ a přirozené číslo $r \leq p$ je nad tělesem $\mathbb{Z}_p$ hodnota kombinačního čísla $\binom{p}{r} = \frac{p!}{r! \cdot (p-r)!} \equiv 0 \pmod{p}$ a spočítáme-li $8^{13} \equiv 8 \pmod{13}$ (Malá Fermatova věta nám dokonce obecně říká, že $\lambda^p \equiv \lambda \pmod{p}$ pro každé $\lambda \in \mathbb{Z}_{13} \setminus \{0\}$), dostáváme díky 4.19

$$\mathbf{A}^{13} = \begin{pmatrix} 8 & 1 & 0 & 0 \\ 0 & 8 & 1 & 0 \\ 0 & 0 & 8 & 1 \\ 0 & 0 & 0 & 8 \end{pmatrix}^{13} = \begin{pmatrix} 8 & 0 & 0 & 0 \\ 0 & 8 & 0 & 0 \\ 0 & 0 & 8 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix}.$$

□

## 5. Lineární prostory a lineární nezávislost

**5.1.** Rozhodněte, zda vektor a) $(1,1,4)^T$ a b) $(4,1,1)^T$ leží v podprostoru $U = \langle (1,4,3)^T, (3,1,1)^T \rangle$ vektorového prostoru $\mathbb{Z}_5^3$ nad tělesem $\mathbb{Z}_5$.

Ptáme se, zda existují hodnoty $x, y \in \mathbb{Z}_5$, které řeší vektorovou rovnici $x \cdot (1,4,3)^T + y \cdot (3,1,1)^T = \mathbf{v}$, tedy chceme zjistit, zda existuje řešení soustavy 3 rovnic o 2 neznámých (pro každou souřadnici dostáváme jednu rovnici) s maticemi, které snadno upravíme na odstupňovaný tvar.

a)

$$\left(\begin{array}{cc|c} 1 & 3 & 1 \\ 4 & 1 & 1 \\ 3 & 1 & 4 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 4 & 2 \\ 0 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{array}\right)$$

Vidíme, že hodnost matice homogenní soustavy i matice rozšířené se shodují, tedy podle Frobeniovy věty (5.80) řešení existuje a vektor $(1,1,4)^T$ je lineární kombinací vektorů $(1,4,3)^T$, $(3,1,1)^T$, proto $(1,1,4)^T \in U$.

b)

$$\left(\begin{array}{cc|c} 1 & 3 & 4 \\ 4 & 1 & 1 \\ 3 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 4 & 0 \\ 0 & 2 & 4 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{array}\right)$$

Tentokrát soustava zjevně řešení nemá, tedy $(4,1,1)^T \notin U$. □

**5.2.** Rozhodněte, zda je množina $U$ podprostorem aritmetického vektorového prostoru $\mathbb{Z}_5^3$ nad tělesem $\mathbb{Z}_5$, jestliže

(a) $U = \{(0,0,0)^T\}$, (b) $U = \{(0,0,0)^T, (1,2,3)^T\}$, (c) $|U| = 4$,
(d) $U = \{(0,0,0)^T, (1,2,3)^T, (2,4,1)^T, (3,1,4)^T, (4,3,2)^T\}$,
(e) $|U| = 6$, (f) $|U| = 125$, (g) $|U| = \emptyset$,

(a) Protože $(0,0,0)^T + (0,0,0)^T = (0,0,0)^T$ a $t(0,0,0)^T = (0,0,0)^T$ pro každé $t \in T$, je podle Tvrzení 5.6 z přednášky množina $\{(0,0,0)^T\}$ podprostorem $\mathbb{Z}_5^3$.

(b) Vidíme, že $(1,2,3)^T + (1,2,3)^T = 2(1,2,3)^T = (2,4,1)^T \notin U$, proto podle Tvrzení 5.6 $U$ není podprostorem.

(c) Je-li $\mathbf{u} = (u_1, u_2, u_3)$ nenulový vektor, potom množina $\langle \mathbf{u} \rangle = \{a\,\mathbf{u} \mid a \in \mathbb{Z}_5\}$ obsahuje právě tolik různých vektorů,kolik prvků obsahuje těleso $\mathbb{Z}_5$. Proto čtyřprvkový podprostor (který by nutně obsahoval nenulový vektor) nad tělesem $\mathbb{Z}_5$ nemůže existovat.

(d) Snadno pomocí Tvrzení 5.14 z přednášky nahlédneme, že $U = \langle (1,2,3)^T \rangle$, tedy se jedná o podprostor.

(e) Kdyby existoval šestiprvkový podprostor nad tělesem $\mathbb{Z}_5$, pak obsahoval nějaký nenulový vektor $\mathbf{u}$ a pak ještě jeden vektor $\mathbf{v} \in U \setminus \langle \mathbf{u} \rangle$. Podle Tvrzení 5.26 by množin $\{\mathbf{u}, \mathbf{v}\}$ byla lineárně nezávislá, a proto by vektor $2\,\mathbf{u} \notin \langle \mathbf{u} \rangle \cup \{\mathbf{v}\}$, což je spor s předpokladem $|U| = 6$. Tudíž žádný šestiprvkový podprostor nad tělesem $\mathbb{Z}_5$ neexistuje.

(f) Všimneme-li si, že 125 prvků má celý aritmetický prostor $\mathbb{Z}_5^3$, vidíme, že $U = \mathbb{Z}_5^3$ je podprostorem $\mathbb{Z}_5^3$.

(g) Prázdná množina sice triviálně splňuje podmínku uzavřenosti na operace, ale za podprostor ji nepovažujeme. □

**5.3.** Dokažte, že množina komplexních čísel $\mathbb{C}$ tvoří s obvyklým sčítáním a násobením vektorový prostor nad tělesem reálných čísel $\mathbb{R}$.

Je třeba zcela přímočaře ověřit platnost axiomatiky vektorového prostoru. Přitom víme, že $\mathbf{C}$ je se sčítáním a násobením těleso, odkud okamžitě dostáváme asociativitu a komutativitu sčítání, stejně jako existenci nulového vektoru (0). Protože $r(c+d) = rc + rd$ pro všechna komplexní $r, c, d$ platí tato rovnost i v případě, že zvolíme $r \in \mathbf{R}$. Stejný argument ukazuje, že pro každé $r, s \in \mathbf{R}$ a $c \in \mathbf{C}$ máme $(r+s)c = rc + sc$ a $(rs)c = r(sc)$. Konečně zřejmě $1c = c$. □

**5.4.** Rozhodněte, zda je posloupnost vektorů $X$ aritmetického vektorového prostoru $T^n$ nad nad tělesem $T$ lineárně závislá či nezávislá, jestliže

(a) $X = ((1,0,2,1)^T, (2,0,1,1)^T, (1,0,1,-1)^T)$, $n = 4$ a $T = \mathbb{Q}$,
(b) $X = ((1,1,2)^T, (2,0,1)^T, (2,1,1)^T)$, $n = 3$ a $T = \mathbb{Z}_3$,
(c) $U = ((1,1)^T, (1,0)^T, (3,4)^T)$ pro $T = \mathbb{Z}_7$.

(a) Stačí zjistit, zda existuje (a v takovém případě půjde o lineárně závislé vektory) či neexistuje (což by znamenalo, že dané vektory by byly lineárně nezávislé) netriviální řešení vektorové rovnice

$$x_1 \cdot (1,0,2,1)^T + x_2 \cdot (2,0,1,1)^T + x_3 \cdot (1,0,1,-1)^T = (0,0,0,0)$$

Úlohu převedeme na otázku, zda existuje jednoznačné (tedy pouze triviální) řešení homogenní soustavy rovnic s maticí $\mathbf{A}$:

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 2 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & -3 & -1 \\ 0 & -1 & -2 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 5 \\ 0 & 0 & 0 \end{pmatrix}$$

Z upravené soustavy dostáváme jednoznačné řešení $x_1 = x_2 = x_3 = 0$, tedy vektory $(1,0,2,1)^T$, $(2,0,1,1)^T$, $(1,0,1,-1)^T$ jsou lineárně nezávislé.

(b) stejně jako v (a) se ptáme, jakou má hodnost hodnost matice $\begin{pmatrix} 1 & 2 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix}$.

Protože $\begin{pmatrix} 1 & 2 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 2 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$, vidíme, že má tato matice hodnost 2, tedy existuje netriviální řešení homogenní soustavy s touto maticí, a proto je posloupnost vektorů lineárně nezávislá.

(c) Tentokrát nemusíme nic počítat, protože hodnost matice $\begin{pmatrix} 1 & 1 & 3 \\ 1 & 0 & 4 \end{pmatrix}$ určitě nemůže být 3 (na to má málo řádků), tudíž existuje netriviální řešení homogenní soustavy s takovou maticí a posloupnost vektorů je lineárně závislá. □

**5.5.** Najděte nějakou bázi podprostoru $U$ aritmetického vektorového prostoru $T^4$ nad nad tělesem $T$, jestliže

(a) $U = \{(0,0,0,0)^T\}$ pro libovolné těleso $T$,
(b) $U = T^4$ pro libovolné těleso $T$,
(c) $U = \langle (1,0,2,1)^T, (2,0,1,1)^T, (1,0,1,-1)^T \rangle$ pro $T = \mathbf{Q}$,
(d) $U = \langle (2,1,1,1)^T, (4,2,1,3)^T, (3,4,3,0)^T, (1,3,4,2)^T \rangle$ pro $T = \mathbb{Z}_5$,
(e) $U = \langle (2,0,3,4)^T, (3,3,1,2)^T, (3,1,1,2)^T \rangle$ pro $T = \mathbb{Z}_5$,
(f) $U = \langle (1,1,3,6)^T, (5,5,1,0)^T, (3,3,2,6)^T \rangle$ pro $T = \mathbb{Z}_7$.

(a) Protože podprostor $\{(0,0,0,0)^T\}$ generuje prázdná posloupnost, je právě prázdná posloupnost $\emptyset$ báze $U$.

(b) Snadno nahlédneme, že bázi celého aritmetického vektorového prostoru $T^4$ tvoří například kanonická báze, tedy posloupnost sloupcových vektorů obsažených ve sloupcích jednotkové matice.

(c) Protože množina $X = \{(1,0,2,1)^T, (2,0,1,1)^T, (1,0,1,-1)^T\}$ podle definice generuje $U$ a v předchozím příkladu jsme dokázali, že jde o lineárně nezávislou množinu aritmetických vektorů, tvoří množina $X$ bázi $U$.

(d) Seřadíme si vektory generující podprostor $U$ do řádků matice, již upravíme na odstupňovanou, a využijeme Tvrzení 5.27 a 5.37 z přednášky, která nám říkají, že nenulové řádky matice tvoří lineárně nezávislou generující množinu vektorů:

$$\mathbf{A} = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 4 & 2 & 1 & 3 \\ 3 & 4 & 3 & 0 \\ 1 & 3 & 4 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 4 & 2 \\ 2 & 1 & 1 & 1 \\ 4 & 2 & 1 & 3 \\ 3 & 4 & 3 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 4 & 2 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 4 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 & 4 & 2 \\ 0 & 0 & 3 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Zjistili jsme, že posloupnost $((1,3,4,2)^T, (0,0,3,2)^T)$ je báze podprostoru $U$. Závěrem poznamenejme, že $U = \mathrm{Im}\mathbf{A}$.

(e) Stejně jako v (d) si podprostor $U$ vyjádříme jako řádkový vektorový prostor jisté matice $\mathbf{B}$, kterou upravíme na odstupňovaný tvar:

$$\mathbf{B} = \begin{pmatrix} 2 & 0 & 3 & 4 \\ 3 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 3 & 4 \\ 0 & 3 & 4 & 1 \\ 0 & 1 & 4 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 3 & 4 \\ 0 & 3 & 4 & 1 \\ 0 & 0 & 1 & 4 \end{pmatrix}.$$

Tedy například posloupnost $((2,0,3,4)^T, (0,3,4,1)^T, (0,0,1,4)^T)$ tvoří bázi podprostoru $U = \mathrm{Im}\mathbf{B}$.

(f) Opět upravujme matici do jejíž řádku jsme sepsali generující vektory podprostoru $U$:

$$\begin{pmatrix} 1 & 1 & 3 & 6 \\ 5 & 5 & 1 & 0 \\ 3 & 3 & 2 & 6 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 3 & 6 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 3 & 6 \\ 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Vidíme, že bázi $U$ tvoří například posloupnost $((1,1,3,6)^T, (0,0,0,5)^T)$. □

**5.6.** Spočítejte dimenzi podprostorů z předchozí úlohy.

Podle definice stačí spočítat počty vektorů báze, kterou jsme našli v předchozím příkladu:

(a) $\dim U = 0$,
(b) $\dim U = 4$,
(c) $\dim U = 3$,
(d) $\dim U = 2$,
(e) $\dim U = 3$,
(f) $\dim U = 2$.

□

**5.7.** Najděte nějakou bázi a určete dimenzi $\mathbb{C}$ jako vektorového prostoru nad tělesem $\mathbb{R}$.

Protože $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$, okamžitě vidíme, že posloupnost $1, i$ generuje $\mathbb{C}$ nad $\mathbb{R}$. Předpokládáme-li, že $a \cdot 1 + b \cdot i = 0$ pro nějaká reálná $a, b \in \mathbb{R}$, pak nutně $a = b = 0$, čímž jsme ověřili, že $1, i$ je báze $\mathbb{C}$ nad $\mathbb{R}$, tedy $\dim_{\mathbb{R}}(\mathbb{C}) = 2$. □

**5.8.** Rozhodněte, zda dvojice komplexních čísel $3 - i$, $2 + 3i$ tvoří bázi vektorového prostoru $\mathbb{C}$ nad tělesem $\mathbb{R}$.

Díky tomu, že jsme v předchozím příkladu spočítali, že $\dim_{\mathbf{R}}(\mathbb{C}) = 2$, stačí zjistit, zda je dvojice $3 - i$, $2 + 3i$ lineárně nezávislá nebo generující, zbývající vlastnost je totiž podle Věty 2.19 důsledkem každé z nich. Ukážeme například, že jde o lineárně nezávislou množinu. Jestliže $0 = a(3-i) + b(2+3i) = (3a+2b) + (-a+3b)i$, tedy z reálné i imaginární části dostáváme jednu rovnici:

$$\begin{aligned} 3a &+ 2b &= 0 \\ -a &+ 3b &= 0 \end{aligned}$$ a řešíme homogenní soustavu s maticí $\begin{pmatrix} 3 & 2 \\ -1 & 3 \end{pmatrix}$, která má zjevně hodnost 2, tedy pouze triviální řešení.

Tím jsme dokázali, že je dvojice $3-i$, $2+3i$ lineárně nezávislá, tedy jde o bázi $\mathbb{C}$ nad $\mathbb{R}$. $\square$

**5.9.** Vyberte z posloupností $X = ((2,1,1,1)^T, (4,2,1,3)^T, (3,4,3,0)^T, (1,3,4,2)^T)$, resp. $Y = ((2,0,3,4)^T, (1,3,1,2)^T, (1,0,1,2)^T)$ báze podprostorů $\mathbf{U} = \langle X \rangle$, resp. $\mathbf{V} = \langle Y \rangle$ aritmetického vektorového prostoru $\mathbb{Z}_5^4$.

Nejprve si všimněme, že už jsme v Příkladu 5.5(d),(e) báze $U$ i $V$ hledali. Nešlo ovšem o báze vybrané. Využijme tedy spočítaných dimenzi a hledáme dvouprvkovou lineárně nezávislou množinu v $\mathbf{U}$, tedy dvojici vektorů, které nejsou svými násobky, což zřejmě splňuje například dvojice vektorů $(2,1,1,1)^T, (3,4,3,0)^T$ nebo $(3,4,3,0)^T, (1,3,4,2)^T$ a tříprvkovou generující množinu $\mathbf{U}$, jíž je zřejmě celé $Y$. $\square$

**5.10.** Vyberte z posloupnosti

$$X = ((2,4,0,1,4)^T, (4,3,0,2,3)^T, (1,2,3,4,0)^T, (3,1,1,1,2)^T, (4,3,4,0,2)^T)$$

bázi podprostoru $U = \langle X \rangle$ vektorového prostoru $\mathbb{Z}_5^5$ nad tělesem $\mathbb{Z}_5$.

Potřebujeme si uvědomit, které vektory z daného seznamu jsou lineární kombinací předchozích. Seřadíme si tedy vektory do posloupnosti a budeme zjišťovat, které vektory jsou lineární kombinací předchozích členů posloupnosti. Nejprve si tedy seřadíme vektory do řádků matice, čímž máme dánu posloupnost vektorů, a tu budeme upravovat Gaussovou eliminací dokud nezískáme odstupňovanou matici. Jedná se tedy o posloupnost elementárních úprav, kdy k níže položeným řádkům přičítáme výše položené řádky, případně nelze-li nějakým řádkem upravit níže položené řádky, pak takový vektor) vyměníme z níže položeným vektorem přehazujeme násob tvar. Přitom si řádky původní matice označíme římskými číslicemi a budeme zaznamenávat všechna přehazování řádků a stačí zjistit, kterým řádkům původní matice odpovídají nenulové řádky Gaussovy matice.

Poznamenejme, že je podstatné, abychom neměnili pořadí těch vektorů, pomocí nichž jsme upravovali všechny následující, tj. těch řádků matice, které už jsme použili k eliminaci následujících. Takový řádek už totiž odpovídá vektoru, který je lineárně nezávislý na předchozích a jeho případná záměna za některý z následujících vektorů pro něj samozřejmě podmínku lineární nezávislosti na předchozích řádcích nemusí zachovat. V daném případě nejprve přičteme vhodné násobky prvního řádku k ostatním a poté přehodíme druhý a třetí řádek, jímž stejným způsobem vynulujeme pátý a šestý řádek:

$$\left(\begin{array}{ccccc|c} 2 & 4 & 0 & 1 & 4 & i \\ 4 & 3 & 0 & 2 & 3 & ii \\ 1 & 2 & 3 & 4 & 0 & iii \\ 3 & 1 & 1 & 1 & 2 & iv \\ 4 & 3 & 4 & 0 & 2 & v \end{array}\right) \sim \left(\begin{array}{ccccc|c} 2 & 4 & 0 & 1 & 4 & i \\ 0 & 0 & 0 & 0 & 0 & ii \\ 0 & 0 & 3 & 1 & 3 & iii \\ 0 & 0 & 1 & 2 & 1 & iv \\ 0 & 0 & 4 & 3 & 4 & v \end{array}\right) \sim \left(\begin{array}{ccccc|c} 2 & 4 & 0 & 1 & 4 & i \\ 0 & 0 & 3 & 1 & 3 & iii \\ 0 & 0 & 0 & 0 & 0 & ii \\ 0 & 0 & 0 & 0 & 0 & iv \\ 0 & 0 & 0 & 0 & 0 & v \end{array}\right).$$

Ukázalo se, že řádek ii je násobkem řádku i a řádky iv a v jsou lineární kombinací řádků i a iii. Naopak řádek iii není lineární kombinací řádku i. Hledanou bázi tvoří například první a třetí vektor posloupnosti $X$, tedy posloupnost $\left(\begin{pmatrix}2\\4\\0\\1\\4\end{pmatrix}, \begin{pmatrix}1\\2\\3\\4\\0\end{pmatrix}\right)$. □

**5.11.** Doplňte lineárně nezávislou množinu $B = \{(2,4,0,1,4)^T, (1,2,1,0,3)^T\}$ na bázi aritmetického vektorového prostoru $\mathbb{Z}_5^5$.

Připomeňme, že podle Důsledku 5.27 se řádkový vektorový prostor matice nezmění, upravíme-li ji posloupností elementárních řádkových úprav. Seřadíme-li vektory množiny $B$ do řádků matice, kterou upravíme na odstupňovanou matici, vidíme, že

$$\langle B\rangle = \mathrm{Im}(\begin{pmatrix}2&4&0&1&4\\1&2&1&0&3\end{pmatrix})^T = \mathrm{Im}(\begin{pmatrix}2&4&0&1&4\\0&0&1&2&1\end{pmatrix})^T$$

Nyní snadno doplníme matici na odstupňovanou čtvercovou matici, jejíž všechny řádky jsou nenulové, například vektory standardní báze (i-tý přidáme, právě když i-tý sloupec matice není bázový) a přitom si všimneme, že:

$$\begin{pmatrix}2&4&0&1&4\\0&1&0&0&0\\0&0&1&2&1\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix} \sim \begin{pmatrix}2&4&0&1&4\\0&0&1&2&1\\0&1&0&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix} \sim \begin{pmatrix}2&4&0&1&4\\1&2&1&0&3\\0&1&0&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix} = \mathbf{A}.$$

Zřejmě má řádkový prostor matice $\mathbf{A}$ dimenzi 5, proto je roven $\mathbb{Z}_5^5$. Tedy množina $\{(0,1,0,0,0)^T, (0,0,0,1,0)^T, (0,0,0,0,1)^T\}$ doplňuje množinu $B$ na bázi $\mathbb{Z}_5^5$. □

**5.12.** Ověřte, že $B = ((1,4,3)^T, (3,1,1)^T)$ je báze podprostoru $U = \langle (1,4,3)^T, (3,1,1)^T\rangle$ vektorového prostoru $\mathbb{Z}_5^3$ nad tělesem $\mathbb{Z}_5$ a najděte souřadnice vektoru $(1,1,4)^T$ vzhledem k bázi $B$. $(1,4,3)^T$, $(3,1,1)^T$

Okamžitě z definice vidíme, že posloupnost $B$ je lineárně nezávislá, tedy jde o bázi $U$. Nyní hledáme hodnoty $x, y \in \mathbb{Z}_5$, které řeší vektorovou rovnici $x\cdot(1,4,3)^T + y\cdot(3,1,1)^T = (1,1,4)^T$, kterou jsme řešili už v minulé úloze. Zbývá tedy zpětnou substitucí dopočítat (jednoznačné) řešení:

$$\left(\begin{array}{cc|c}1&3&1\\4&1&1\\3&1&4\end{array}\right) \sim \left(\begin{array}{cc|c}1&3&1\\0&1&3\\0&0&0\end{array}\right)$$

Spočítali jsme, že souřadnice $(1,1,4)^T$ vzhledem k bázi $B$ jsou $\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}2\\3\end{pmatrix}$. □

**5.13.** Rozhodněte, zda je posloupnost vektorů $M = \left(\begin{pmatrix}1\\0\\2\end{pmatrix}, \begin{pmatrix}2\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}\right)$ báze vektorového prostoru $\mathbf{Q}^3$ nad tělesem $\mathbf{Q}$.

Podle pozorování 5.61 z přednášky stačí ověřit, zda je posloupnost lineárně nezávislá či zda generuje celý prostor $\mathbf{Q}^3$ a to nastává právě tehdy, když je matice $\mathbf{A} = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ regulární. Budeme tedy matici $\mathbf{A}$ upravovat:

$$\begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -3 \\ 0 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -3 \\ 0 & 0 & 2 \end{pmatrix}.$$

Zjistili jsme, že $M$ je bází $\mathbf{Q}^3$. □

**5.14.** Najděte souřadnice vektoru $\mathbf{v}$ vzhledem k bázi $M$ z předchozího příkladu, jestliže (a) $\mathbf{v} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ (b) $\mathbf{v} = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$ (c) $\mathbf{v} = \begin{pmatrix} 4 \\ 1 \\ 3 \end{pmatrix}$.

Hledáme aritmetický vektor $[\mathbf{v}]_M = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$, aby $\mathbf{v} = a \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} + b \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} + c \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, tedy budeme počítat řešení nehomogenní soustavy rovnic:

(a) Pro $\mathbf{v} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ zřejmě $[\mathbf{v}]_M = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$.

(b) Tentokrát je vektor $\mathbf{v}$ jedním z bázových vektorů báze $M$, proto bez počítání vidíme, že $[\mathbf{v}]_M = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$.

(c) Nyní obvyklým způsobem spočítáme jednoznačné řešení nehomogenní soustavy s maticí $\left(\begin{array}{ccc|c} 1 & 2 & 1 & 4 \\ 0 & 1 & 1 & 1 \\ 2 & 1 & 1 & 3 \end{array}\right)$. Zjistili jsme, že $[\mathbf{v}]_M = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$. □

**5.15.** Najděte nějakou bázi podprostoru $\mathbf{U} = \langle (3,1,4,2)^T, (2,3,5,1)^T, (1,5,6,1)^T \rangle$ aritmetického vektorového prostoru $\mathbb{Z}_7^4$ a doplňte ji bázi celého prostoru $\mathbb{Z}_7^4$.

I tentokrát můžeme využít Důsledku 5.23 o řádkovém vektorovém prostoru matice $\mathbf{M} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 2 & 3 & 5 & 1 \\ 1 & 5 & 6 & 1 \end{pmatrix}$, pro níž platí, že $\mathbf{U} = \mathrm{Im}\mathbf{M}^T$. Nejprve standardní cestou upravíme matici $\mathbf{M}$ na matici odstupňovanou:

$$\begin{pmatrix} 3 & 1 & 4 & 2 \\ 2 & 3 & 5 & 1 \\ 1 & 5 & 6 & 1 \end{pmatrix} \sim \begin{pmatrix} 3 & 1 & 4 & 2 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 3 & 1 & 4 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \mathbf{N}.$$

Vidíme, že báze $\mathrm{Im}\mathbf{M}^T = \mathrm{Im}\mathbf{N}^T = \mathbf{U}$ je tvořena například nenulovými řádkovými vektory odstupňované matice $\mathbf{N}$. Tedy $\{(3,1,4,2)^T, (0,0,0,1)^T\}$ je báze $\mathbf{U}$. Nyní už postupujeme stejně jako v předchozí úloze, doplníme nenulové řádky matice $\mathbf{N}$ pomocí vektorů standardní báze, abychom dostali odstupňovanou regulární matici

$\begin{pmatrix} 3 & 1 & 4 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Tudíž posloupnost $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ doplňuje posloupnost $\begin{pmatrix} 3 \\ 1 \\ 4 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ na bázi celého $\mathbb{Z}_7^4$. □

**5.16.** Uvažujme dvě posloupnosti vektorů $M = (\begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix})$ a $N = (\begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 3 \end{pmatrix})$ v lineárním prostoru $\mathbb{Z}_5^3$ nad tělesem $\mathbb{Z}_5$.

(a) Ověřte, že je posloupnost $M$ lineárně nezávislá,
(b) dokažte, že $N \subset \langle M \rangle$,
(c) spočítejte souřadnice vektorů posloupnosti $N$ vzhledem k bázi $M$,
(d) ověřte, že $N$ tvoří bázi podprostoru $\langle M \rangle$.

(a) Stačí si všimnout, že jeden z vektorů není násobkem druhého, tedy, že má matice $\begin{pmatrix} 1 & 3 \\ 2 & 2 \\ 4 & 1 \end{pmatrix}$ má hodnost 2.

(b) Ptáme se, zda jsou vektory z posloupnosti $N$ lineární kombinací vektorů z posloupnosti $M$, to znamená, že se ptáme, zda existuje řešení soustav rovnic s maticemi $\left(\begin{array}{cc|c} 1 & 3 & 3 \\ 2 & 2 & 0 \\ 4 & 1 & 3 \end{array}\right)$ a $\left(\begin{array}{cc|c} 1 & 3 & 1 \\ 2 & 2 & 3 \\ 4 & 1 & 3 \end{array}\right)$. Tuto úlohu můžeme pomocí Frobeniovy věty přeformulovat na otázku, zda jsou hodnosti matic $\left(\begin{array}{cc|cc} 1 & 3 & 3 & 1 \\ 2 & 2 & 0 & 3 \\ 4 & 1 & 3 & 3 \end{array}\right)$ a $\begin{pmatrix} 1 & 3 \\ 2 & 2 \\ 4 & 1 \end{pmatrix}$ stejné, tedy podle (a) rovná dvěma. To zjistíme ovšem standardně Gaussovou eliminací:

$$\left(\begin{array}{cc|cc} 1 & 3 & 3 & 1 \\ 2 & 2 & 0 & 3 \\ 4 & 1 & 3 & 3 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 3 & 3 & 1 \\ 0 & 1 & 4 & 1 \\ 0 & 4 & 1 & 4 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 3 & 3 & 1 \\ 0 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right),$$

protože je hodnost matice 2, platí, že že $N \subset \langle M \rangle$.

(c) Nyní máme najít řešení soustav s maticemi uvedenými v bodě (b). Obě přitom upravujeme stejně, proto počítáme obvyklým způsobem s využitím úprav v (b):

$$\left(\begin{array}{cc|cc} 1 & 3 & 3 & 1 \\ 2 & 2 & 0 & 3 \\ 4 & 1 & 3 & 3 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 3 & 3 & 1 \\ 0 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 1 & 3 \\ 0 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right).$$

Stejně jako v 5.14 jsme zjistili, že $[\begin{pmatrix} 3 \\ 0 \\ 3 \end{pmatrix}]_M = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$ a $[\begin{pmatrix} 1 \\ 3 \\ 3 \end{pmatrix}]_M = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$.

(d) Stejnou úvahou jako v bodu (a) nahlédneme, že je posloupnost $N$ lineárně nezávislá, proto jde podle (c) o bázi podprostoru $\langle M \rangle$. □

**5.17.** Ověřte, že $(3 - 5i, 1 - 2i)$ tvoří bázi lineárního prostoru komplexních čísel $\mathbb{C}$ nad tělesem reálných čísel $\mathbb{R}$.

Protože $K = (1, i)$ je zřejmě báze $\mathbb{C}$ nad $\mathbb{R}$, stačí přejít k souřadnicovým vektorům $[3-5i]_K = \begin{pmatrix} 3 \\ -5 \end{pmatrix}$ a $[1-2i]_K = \begin{pmatrix} 1 \\ -2 \end{pmatrix}$ a u nich obvyklým způsobem nahlédnout, že jde o bázi aritmetického vektorového prostoru $\mathbb{R}^2$, tj. všimnout si, že je matice $\begin{pmatrix} 3 & 1 \\ -5 & -2 \end{pmatrix}$ regulární. □

**5.18.** Najděte matice přechodu:

(a) $[\mathrm{Id}]^B_{K_2}$ a $[\mathrm{Id}]^{K_2}_B$, kde $B = (\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix})$ a $K_2$ je kanonická báze v lineárním prostoru $\mathbb{R}^2$ nad tělesem $\mathbb{R}$

(b) $[\mathrm{Id}]^N_M$ a $[\mathrm{Id}]^M_N$, kde $N$ a $M$ jsou báze z úlohy 5.16,

(c) $[\mathrm{Id}]^M_N$, kde $N = (\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ k bázi $M = (\begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix})$ jsou báze $\mathbb{Z}_3^2$ nad tělesem $\mathbb{Z}_3$.

(d) $[\mathrm{Id}]^L_K$ a $[\mathrm{Id}]^K_L$, kde $K = (1, i)$ a $L = (3-5i, 1-2i)$ jsou báze $\mathbb{C}$ nad tělesem $\mathbb{R}$.

(a) Postupujeme-li podle definice, vidíme, že souřadnice vektorů vzhledem ke kanonické bázi jsou tytéž vektory a protože matice $[\mathrm{Id}]^B_{K_2}$ obsahuje ve sloupcích právě souřadnice vektorů báze $B$ vzhledem ke kanonické bázi, stačí do sloupců přepsat bázi $B$. Tudíž $[\mathrm{Id}]^B_{K_2} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$.

Provedeme-li stejnou úvahu jako v Příkladu 5.74 z přednášky, potřebujeme najednou vyřešit dvě soustavy rovnic s maticí levých stran $[\mathrm{Id}]^B_{K_2} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$ a s vektory pravých stran z báze $K_2$. Tedy postupujeme stejně jako při hledání inverzní matice.

$$\left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 2 & 3 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 3 & -1 \\ 0 & 1 & -2 & 1 \end{array}\right)$$

Spočítali jsme, že $[\mathrm{Id}]^{K_2}_B = ([\mathrm{Id}]^B_{K_2})^{-1} = \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix}$

(b) Protože jsme v 5.16(c) našli souřadnice vektorů báze $N$ vzhledem k bázi $M$, stačí je sepsat do sloupců, abychom dostali $[\mathrm{Id}]^N_M = \begin{pmatrix} 1 & 3 \\ 4 & 1 \end{pmatrix}$.

Obdobnou úvahou jako v úloze (a) tentokrát ovšem v souřadnicích zjistíme a obvyklým způsobem spočítáme, že $[\mathrm{Id}]^M_N = ([\mathrm{Id}]^N_M)^{-1} = \begin{pmatrix} 1 & 3 \\ 4 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 3 \\ 4 & 4 \end{pmatrix}$.

(c) Postupujeme-li podle definice , potřebujeme vyřešit maticovou rovnici $[\mathrm{Id}]^M_{K_2} \cdot \mathbf{X} = [\mathrm{Id}]^N_{K_2}$, kde $\mathbf{X}$ je právě hledaná matice přechodu $[\mathrm{Id}]^M_N$ Stačí nám tedy známým způsobem spočítat

$$[\mathrm{Id}]^M_N = ([\mathrm{Id}]^M_{K_2})^{-1} \cdot [\mathrm{Id}]_{NK_2} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}.$$

(d) V úloze 5.17 jsme určili souřadnice vektorů báze $L$ vzhledem ke $K$, proto $[\mathrm{Id}]_K^L = \begin{pmatrix} 3 & 1 \\ -5 & -2 \end{pmatrix}$. Nyní zbývá podobně jako v (a) a (b) nahlédnout a dopočítat, že $[\mathrm{Id}]_L^K = ([\mathrm{Id}]_K^L)^{-1} = \begin{pmatrix} 2 & 1 \\ -5 & -3 \end{pmatrix}$ □

**5.19.** Určete nad tělesy $\mathbb{R}$ a $\mathbb{Z}_5$ hodnost matice $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 1 & 4 & 3 \end{pmatrix}$ a matice $\mathbf{A}^T$ a dimenze prostorů $\mathrm{Im}\mathbf{A}$, $\mathrm{Im}\mathbf{A}^T$, $\mathrm{Ker}\,\mathbf{A}$, $\mathrm{Ker}\,\mathbf{A}^T$.

Podle Vět 5.82, 5.94 a definice hodnosti stačí spočítat hodnost matice. Upravujme tedy matici posloupností elementárních úprav nejprve nad tělesem $\mathbb{R}$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 1 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -5 \\ 0 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & -5 \end{pmatrix}.$$

Zjistili jsme, že nad tělesem $\mathbb{R}$ platí, že $\mathrm{rank}(\mathbf{A}) = 3$, a proto

$$\mathrm{rank}(\mathbf{A}) = \mathrm{rank}(\mathbf{A}^T) = \dim \mathrm{Im}\mathbf{A} = \dim \mathrm{Im}\mathbf{A}^T = 3.$$

Díky 5.94 je potom

$$\mathrm{Ker}\,\mathbf{A} = 3 - \mathrm{rank}(\mathbf{A}) = 3 - 3 = 0, \mathrm{Ker}\,\mathbf{A}^T = 3 - \mathrm{rank}(\mathbf{A}^T) = 3 - 3 = 0.$$

Podobně určíme hodnost $\mathbf{A}$ nad tělesem $\mathbb{Z}_5$:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 1 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Tedy nad tělesem $\mathbb{Z}_5$ je $\mathrm{rank}(\mathbf{A}) = \mathrm{rank}(\mathbf{A}^T) = \dim \mathrm{Im}\mathbf{A} = \dim \mathrm{Im}\mathbf{A}^T = 2$ a $\mathrm{Ker}\,\mathbf{A} = \mathrm{Ker}\,\mathbf{A}^T = 3 - \mathrm{rank}(\mathbf{A}) = 3 - 2 = 1$. □

**5.20.** Najděte nad tělesem $\mathbb{Z}_5$ báze prostorů $\mathrm{Im}\mathbf{A}$, $\mathrm{Im}\mathbf{A}^T$, $\mathrm{Ker}\,\mathbf{A}$, $\mathrm{Ker}\,\mathbf{A}^T$ pro matici $\mathbf{A}$ z předchozí úlohy.

Z odstupňovaného tvaru matice

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 1 & 4 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Okamžitě vidíme, že $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ je báze $\mathrm{Im}\mathbf{A}^T$ a snadno spočítáme bazické řešení $\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$ homogenní soustavy s maticí $\mathbf{A}$, tj. bázi $\mathrm{Ker}\,\mathbf{A}$. Pro nalezení báze $\mathrm{Ker}\,\mathbf{A}^T$ řádkově upravíme $\mathbf{A}^T$:

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 4 \\ 3 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

Zpětnou substitucí najdeme bázi $\begin{pmatrix}1\\4\\1\end{pmatrix}$ prostoru $\operatorname{Ker}\mathbf{A}^T$. Zároveň vidíme, že báze $\operatorname{Im}\mathbf{A}$ je například $\begin{pmatrix}1\\2\\1\end{pmatrix}$, $\begin{pmatrix}0\\2\\2\end{pmatrix}$ (nebo kterákoli jiná dvojice lineárně nezávislých vektorů tohoto prostoru). □

**5.21.** Určete dimenzi průniku podprostorů **U** a **V** racionálního vektorového prostoru $\mathbf{Q}^3$, je-li $\mathbf{U} = \langle \begin{pmatrix}1\\2\\1\end{pmatrix}, \begin{pmatrix}1\\0\\2\end{pmatrix} \rangle$ a $\mathbf{V} = \langle \begin{pmatrix}1\\1\\0\end{pmatrix}, (\begin{pmatrix}-1\\-1\\1\end{pmatrix} \rangle$.

Snadno zjistíme, že $\dim \mathbf{U} = \operatorname{rank}(\begin{pmatrix}1&1\\2&0\\1&2\end{pmatrix}) = 2$, $\dim \mathbf{V} = \operatorname{rank}(\begin{pmatrix}1&1\\1&-1\\0&1\end{pmatrix}) = 2$ a $\dim(\mathbf{U}+\mathbf{V}) = \operatorname{rank}(\begin{pmatrix}1&1&1&1\\2&0&1&-1\\1&2&0&1\end{pmatrix}) = 3$, proto je díky Větě o dimenzi součtu a průniku podprostorů (5.98) $\dim(\mathbf{U}\cap\mathbf{V}) = \dim\mathbf{U} + \dim\mathbf{V} - \dim(\mathbf{U}+\mathbf{V}) = 1$. □

**5.22.** Jestliže $\mathbf{U} = \langle \begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}0\\2\\1\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\2\end{pmatrix} \rangle$ a $\mathbf{V} = \langle \begin{pmatrix}1\\2\\2\\1\end{pmatrix}, \begin{pmatrix}0\\1\\2\\1\end{pmatrix}, \begin{pmatrix}0\\0\\2\\2\end{pmatrix} \rangle$ podprostory lineárního prostoru $\mathbb{Z}_3^4$ nad tělesem $\mathbb{Z}_3$, spočítejte dimenze a najděte báze podprostorů **U**, **V** , $\mathbf{U}+\mathbf{V}$, $\mathbf{U}\cap\mathbf{V}$.

Nejprve snadno zjistíme, že posloupnost $B = (\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}0\\2\\1\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\2\end{pmatrix})$ je lineárně nezávislá, tudíž báze **U** a podobně je posloupnost $C = (\begin{pmatrix}1\\2\\2\\1\end{pmatrix}, \begin{pmatrix}0\\1\\2\\1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\2\end{pmatrix})$ lineárně nezávislá, a proto báze **V**. Protože $3 \leq \dim \mathbf{U} + \mathbf{V} \leq 4$, stačí si všimnout, že vektor $\mathbf{e}_4 = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\\2\end{pmatrix} + \begin{pmatrix}0\\0\\2\\2\end{pmatrix}$ leží v $\mathbf{U}+\mathbf{V}$. To znamená, že $\mathbf{U}+\mathbf{V}$ obsahuje čtyřprvkovou lineárně nezávislou posloupnost $B \cup (\mathbf{e}_4)$, a proto $\dim \mathbf{U} + \mathbf{V} = 4$. Nyní zbývá použít Větu 5.98, abychom zjistili, že

$$\dim(\mathbf{U}\cap\mathbf{V}) = \dim\mathbf{U} + \dim\mathbf{V} - \dim(\mathbf{U}+\mathbf{V}) = 3 + 3 - 4 = 2.$$

Při počítání dimenzí jsme zjistili, že je $B$ báze **U**, dále $C$ je báze **V** a například kanonická báze je bází $\mathbf{U}+\mathbf{V} = \mathbb{Z}_3^4$.

Zbývá nejít bázi $\mathbf{U} \cap \mathbf{V}$. Hledáme tedy všechny vektory, které leží zároveň v $\mathbf{U}$ i ve $\mathbf{V}$, což si opět vyjádříme rovnicí:

$$x_1 \begin{pmatrix}1\\1\\1\\1\end{pmatrix} + x_2 \begin{pmatrix}0\\2\\1\\1\end{pmatrix} + x_3 \begin{pmatrix}0\\0\\1\\2\end{pmatrix} = y_1 \begin{pmatrix}1\\2\\2\\1\end{pmatrix} + y_2 \begin{pmatrix}0\\1\\2\\1\end{pmatrix} + y_3 \begin{pmatrix}0\\0\\2\\2\end{pmatrix},$$

kterou opět upravíme na

$$x_1 \begin{pmatrix}1\\1\\1\\1\end{pmatrix} + x_2 \begin{pmatrix}0\\2\\1\\1\end{pmatrix} + x_3 \begin{pmatrix}0\\0\\1\\2\end{pmatrix} + y_1 \begin{pmatrix}2\\1\\1\\2\end{pmatrix} + y_2 \begin{pmatrix}0\\2\\1\\2\end{pmatrix} + y_3 \begin{pmatrix}0\\0\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}.$$

Znovu počítáme všechna řešení homogenní soustavy s maticí:

$$\mathbf{D} = \begin{pmatrix}1&0&0&2&0&0\\1&2&0&1&2&0\\1&1&1&1&1&1\\1&1&2&2&2&1\end{pmatrix} \sim \begin{pmatrix}1&0&0&2&0&0\\0&2&0&2&2&0\\0&1&1&2&1&1\\0&1&2&0&2&1\end{pmatrix} \sim$$

$$\sim \begin{pmatrix}1&0&0&2&0&0\\0&2&0&2&2&0\\0&0&1&1&0&1\\0&0&2&2&1&1\end{pmatrix} \sim \begin{pmatrix}1&0&0&2&0&0\\0&2&0&2&2&0\\0&0&1&1&0&1\\0&0&0&0&1&2\end{pmatrix}.$$

Nyní obvyklým způsobem spočítáme najít bázi podprostoru $\operatorname{Ker} \mathbf{D}$, například bázi $(1,2,2,1,0,0)^T$, $(0,2,2,0,1,1)^T$. Zjistili jsme, že:

$$\begin{pmatrix}1\\2\\2\\1\end{pmatrix} = 1 \cdot \begin{pmatrix}1\\1\\1\\1\end{pmatrix} + 2 \cdot \begin{pmatrix}0\\2\\1\\1\end{pmatrix} + 2 \cdot \begin{pmatrix}0\\0\\1\\2\end{pmatrix} = 1 \cdot \begin{pmatrix}1\\2\\2\\1\end{pmatrix} + 0 \cdot \begin{pmatrix}0\\1\\2\\1\end{pmatrix} + 0 \cdot \begin{pmatrix}0\\0\\2\\2\end{pmatrix},$$

a

$$\begin{pmatrix}0\\1\\1\\0\end{pmatrix} = 0 \cdot \begin{pmatrix}1\\1\\1\\1\end{pmatrix} + 2 \cdot \begin{pmatrix}0\\2\\1\\1\end{pmatrix} + 2 \cdot \begin{pmatrix}0\\0\\1\\2\end{pmatrix} = 0 \cdot \begin{pmatrix}1\\2\\2\\1\end{pmatrix} + 1 \cdot \begin{pmatrix}0\\1\\2\\1\end{pmatrix} + 1 \cdot \begin{pmatrix}0\\0\\2\\2\end{pmatrix},$$

Tudíž vektory $(1,2,2,1)^T$ a $(0,1,1,0)^T$ leží v podprostoru $\mathbf{U} \cap \mathbf{V}$. Konečně si uvědomíme, že libovolné řešení soustavy lze napsat ve tvaru

$$a_1 \cdot (1,2,2,1,0,0)^T + a_2 \cdot (0,2,2,0,1,1)^T = (a_1, 2a_1 + 2a_2, 2a_1 + 2a_2, a_1, a_2, a_2)^T,$$

kde $a_1, a_2 \in \mathbb{Z}_3$, proto lze každý vektor z průniku vyjádřit:

$$a_1 \cdot (1,1,1,1)^T + (2a_1 + 2a_2) \cdot (0,2,1,1)^T + (2a_1 + 2a_2) \cdot (0,0,1,2)^T =$$

$$= a_1 \cdot (1,2,2,1)^T + a_2 \cdot (0,1,1,0)^T.$$

Tím jsme zjistili, že každý vektor z podprostoru $\mathbf{U}\cap\mathbf{V}$ lze napsat ve tvaru $a_1 \cdot \begin{pmatrix}1\\2\\2\\1\end{pmatrix} +$ $a_2 \cdot \begin{pmatrix}0\\1\\1\\0\end{pmatrix}$, tedy posloupnost $\left(\begin{pmatrix}1\\2\\2\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}\right)$ podprostor $\mathbf{U}\cap\mathbf{V}$ generuje. Zjevně se jedná o posloupnost lineárně nezávislou, tedy jde o bázi průniku. Není přitom těžké si uvědomit, že výsledné vektory budou jistě lineárně nezávislé, jestliže jsme hledali jejich souřadnice vzhledem k bázím prostorů $\mathbf{U}$ a $\mathbf{V}$.

Závěrem si ještě všimněme, že jsme soustavu nemuseli dopočítávat, neboť nám stačilo najít souřadnice báze řešení odpovídající proměnným $y_i$ (tj. poslední 3 souřadnice) nebo $x_i$ (tj. první 3 souřadnice). □

**5.23.** Najděte nenulový reálný polynom stupně (nejvýše) 2, jehož kořenem je komplexní číslo $3-i$.

Stačí když uvážíme, že jsou vektory $(3-i)^0 = 1$, $(3-i)^1 = 3-i$ a $(3-i)^2 = 8-6i$ nad tělesem $\mathbf{R}$ nutně lineárně závislé, tedy existuje trojice $(a_0, a_1, a_2) \in \mathbf{R}^3 \setminus \{(0,0,0)\}$, pro níž $a_0 + a_1(3-i) + a_2(8-6i) = 0$. Obdobnou úvahou jako v předchozím příkladu zjistíme, že potřebujeme vyřešit homogenní soustavu s maticí $\begin{pmatrix}1 & 3 & 8\\0 & -1 & -6\end{pmatrix}$. Snadno zjistíme, že řešením je například trojice $(a_0, a_1, a_2) = (10, -6, 1)$, proto je komplexní číslo $3-i$ kořenem polynomu $x^2 - 6x + 10$. □

**5.24.** Najděte všechny reálné polynom stupně nejvýše 2, jejichž kořenem je komplexní číslo $3-i$.

V předchozí úloze jsme si uvědomili, že každý takový polynom odpovídá řešení homogenní soustavy lineárních rovnic s maticí typu (2,3) hodnosti 2. Protože je množina všech řešení podprostor dimenze 1, jsou hledané reálné polynomy tvaru $rx^2 - 6rx + 10r$ pro libovolné reálné $r \in \mathbf{R}$. □

**5.25.** Dokažte, že je množina $\mathbf{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} |\ a, b, c \in \mathbf{Q}\}$ podprostor racionálního vektorového prostoru $\mathbf{R}$ a navíc, že $\alpha \cdot \beta \in \mathbf{Q}[\sqrt[3]{2}]$ pro každé $\alpha, \beta \in \mathbf{Q}[\sqrt[3]{2}]$.

Stačí pro libovolné $d, a_1, a_2, b_1, b_2, c_1, c_3 \in \mathbf{Q}$ nahlédnout, že

$$(a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4})+(a_2+b_2\sqrt[3]{2}+c_2\sqrt[3]{4}) = (a_1+a_2)+(b_1+b_2)\sqrt[3]{2}+(c_1+c_2)\sqrt[3]{4} \in \mathbf{Q}[\sqrt[3]{2}]$$

a dále, že

$$d(a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}) = da_1 + db_1\sqrt[3]{2} + dc_1\sqrt[3]{4} \in \mathbf{Q}[\sqrt[3]{2}]$$

a konečně, že $(a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}) \cdot (a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4}) =$

$$= (a_1a_2+2b_1c_2+2c_1b_2)+(a_1b_2+b_1a_2+2c_1c_2)\sqrt[3]{2}+(a_1c_2+c_1a_2+b_1b_2)\sqrt[3]{4} \in \mathbf{Q}[\sqrt[3]{2}].$$

□

**5.26.** Najděte nenulový racionální polynom stupně (nejvýše) 3, jehož kořenem je reálné číslo $1 - \sqrt[3]{2}$.

Uvažujeme stejně jako v úloze 5.23. Opět si všimneme, že $\dim_{\mathbf{Q}}(\mathbf{Q}[\sqrt[3]{2}]) \leq 3$, proto jsou vektory $(1-\sqrt[3]{2})^0 = 1$, $(1-\sqrt[3]{2})^1 = 1-\sqrt[3]{2}$, $(1-\sqrt[3]{2})^2 = 1-2\sqrt[3]{2}+\sqrt[3]{4}$ a $(1-\sqrt[3]{2})^3 = -1-3\sqrt[3]{2}+3\sqrt[3]{4}$ nad tělesem $\mathbf{Q}$ lineárně závislé. Najdeme tedy opět netriviální řešení vektorové rovnice

$$a_0 + a_1(1-\sqrt[3]{2}) + a_2(1-2\sqrt[3]{2}+\sqrt[3]{4}) + a_3(-1-3\sqrt[3]{2}+3\sqrt[3]{4}) = 0,$$

která vede na homogenní soustavy lineárních rovnic s maticí

$$\begin{pmatrix} 1 & 1 & 1 & -1 \\ 0 & -1 & -2 & -3 \\ 0 & 0 & 1 & 3 \end{pmatrix}.$$

Vidíme, že řešením je čtveřice $(a_0, a_1, a_2, a_3) = (1, 3, -3, 1)$, tudíž je číslo $1-\sqrt[3]{2}$ kořenem polynomu $x^3 - 3x^2 + 3x + 1$. □

## 6. Lineární zobrazení

**6.1.** Nechť $f : \mathbb{Z}_5^3 \to \mathbb{Z}_5^2$ je zobrazení dané předpisem $f(\mathbf{v}) = \begin{pmatrix} 4 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \cdot \mathbf{v}$. Rozhodněte, zda jde o lineární zobrazení.

Na přednášce jsme si uvědomili, že díky Tvrzením 4.18 a 4.20 zobrazení dané násobením sloupcového vektoru (tedy matice typu $(n,1)$) maticí splňuje axiomy lineárního zobrazení, tedy

$$\mathbf{A}(\mathbf{u}+\mathbf{v}) = \mathbf{A}\mathbf{u} + \mathbf{A}\mathbf{v} \quad \text{a} \quad \mathbf{A}(r \cdot \mathbf{u}) = r \cdot \mathbf{A}(\mathbf{u})$$

pro každé $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_5^3$ a $r \in \mathbb{Z}_5$. □

Označujme $K_n$ kanonickou bázi libovolného aritmetického vektorového prostoru $T^n$ nad tělesem $T$ a její $i$-tý vektor $\mathbf{e}_i$.

**6.2.** Najděte matici lineárního zobrazení $f$ z předchozí úlohy vzhledem

(a) ke kanonickým bázím $K_3$ a $K_2$,

(b) k bázi $B = (\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix})$ a $K_2$,

(c) k bázi $B$ a $C = (\begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 0 \end{pmatrix})$,

(a) Podle definice nejprve potřebujeme zjistit souřadnice vektorů $f(\mathbf{e}_i)$ vzhledem ke kanonické bázi prostoru $\mathbb{Z}_5^2$:

$$[f(\mathbf{e}_1)]_{K_2} = [\begin{pmatrix} 4 \\ 1 \end{pmatrix}]_{K_2} = \begin{pmatrix} 4 \\ 1 \end{pmatrix},$$

$$[f(\mathbf{e}_2)]_{K_2} = [\begin{pmatrix} 1 \\ 2 \end{pmatrix}]_{K_2} = \begin{pmatrix} 1 \\ 2 \end{pmatrix},$$

$$[f(\mathbf{e}_3)]_{K_2} = [\begin{pmatrix} 2 \\ 3 \end{pmatrix}]_{K_2} = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

Nyní zbývá souřadnicové vektory uspořádat do sloupců matice lineárního zobrazení vzhledem ke kanonickým bázím $[f]_{K_2}^{K_3} = \begin{pmatrix} 4 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \mathbf{A}$.

(b) Opět postupujeme podle definice a dostáváme souřadnice

$$[f(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix})]_{K_2} = \begin{pmatrix} 4 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix},$$

$$[f(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix})]_{K_2} = \begin{pmatrix} 4 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \end{pmatrix},$$

$$[f(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix})]_{K_2} = \begin{pmatrix} 4 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ 1 \end{pmatrix}.$$

Zjistili jsme, že $[f]_{K_2}^{B} = \begin{pmatrix} 2 & 0 & 4 \\ 1 & 3 & 1 \end{pmatrix}$.

(c) Tentokrát využijeme Tvrzení 6.15 můžeme vyjádřit hledanou matici $[f]_C^B$ jakou součin matic: $[f]_C^B = [\mathrm{Id}]_C^{K_3} \cdot [f]_{K_3}^B = ([\mathrm{Id}]_{K_3}^C)^{-1} \cdot [f]_{K_3}^B$. Přímo z definice určíme matici přechodu $[\mathrm{Id}]_{K_3}^C = \begin{pmatrix} 2 & 3 \\ 3 & 0 \end{pmatrix}$. Obvyklým způsobem nyní počítáme součin $[f]_C^B = \begin{pmatrix} 2 & 3 \\ 3 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 2 & 0 & 4 \\ 1 & 3 & 1 \end{pmatrix}$:

$$\left(\begin{array}{cc|ccc} 2 & 3 & 2 & 0 & 4 \\ 3 & 0 & 1 & 3 & 1 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 3 & 0 & 1 & 3 & 1 \\ 0 & 3 & 3 & 3 & 0 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 1 & 0 & 2 & 1 & 2 \\ 0 & 1 & 1 & 1 & 0 \end{array}\right).$$

Spočítali jsme, že $[f]_C^B = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 1 & 0 \end{pmatrix}$. □

**6.3.** Pro lineární zobrazení $f$ z předchozích dvou příkladů najděte bázi podprostorů $\mathrm{Ker}\, f$ a $\mathrm{Im} f$ a souřadnice báze $\mathrm{Ker}\, f$ vzhledem k bázi $B$ z předchozí úlohy.

Připomeňme, že $\mathrm{Ker}\, f = \{\mathbf{v} |\ f(\mathbf{v}) = \mathbf{0}\} = \{\mathbf{v} |\ \mathbf{A}\mathbf{v} = \mathbf{0}\}$. Tedy $\mathrm{Ker}\, f$ je právě množina všech řešení homogenní soustavy s maticí $\mathbf{A}$, tj. $\mathrm{Ker}\, f = \mathrm{Ker}\, \mathbf{A}$. Snadno spočítáme, že $\mathrm{Ker}\, f = \langle \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \rangle$, tudíž $\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$ je báze $\mathrm{Ker}\, f$.

Vezmeme-li libovolnou generující množinu $G$ vektorového prostoru $\mathbb{Z}_5^3$ (například kanonickou bázi), potom $f(G)$ tvoří generující množinu podprostoru $\mathrm{Im} f = f(\mathbb{Z}_5^3)$. Vidíme, že $f((1,0,0)^T) = (4,1)^T$, $f((0,1,0)^T) = (1,2)^T$ a $f((0,0,1)^T) = (2,3)^T$, tj. obrazy vektorů kanonické báze tvoří právě sloupce matice $\mathbf{A}$. To znamená, že $\mathrm{Im} f = \mathrm{Im}\mathbf{A} = \langle \begin{pmatrix} 4 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix} \rangle = \mathbb{Z}_5^2$. Dimenze $\mathrm{Im} f$ je jak víme také podle Věty o dimenzi jádra a obrazu 5.94 rovna $3 - \dim \mathrm{Ker}\, \mathbf{A} = 2$ a bází $\mathrm{Im} f$ je tudíž libovolná báze $\mathbb{Z}_5^2$, například kanonická báze.

Pro nalezení souřadnic báze Ker $f$ vzhledem k $B$ můžeme buď obvyklým způsobem spočítat souřadnice nalezeného vektoru $\begin{pmatrix}2\\0\\1\end{pmatrix}$, což znamená vyřešit nehomogenní soustavu rovnic, nebo můžeme využít Tvrzení 6.25, podle nějž stačí najít bázi homogenní soustavy rovnic s již nalezenou maticí $[f]^B_{K_2} = \begin{pmatrix}2 & 0 & 4\\1 & 3 & 1\end{pmatrix}$. To je zjevně velmi snadné a vidíme, že souřadnicovým vektorem báze Ker $f$ vzhledem k $B$ je například vektor $\begin{pmatrix}3\\2\\1\end{pmatrix}$. $\square$

**6.4.** Nechť $g : \mathbf{R}^2 \to \mathbf{R}^3$ je zobrazení určené předpisem

$$g((x_1, x_2)) = (x_1 + 2x_2, 4x_1 - x_2, 2x_2).$$

Dokažte, že se jedná o lineární zobrazení.

Snadno zjistíme, že lze předpis definující zobrazení $g$ vyjádřit jako součin matice a aritmetického vektoru: $g(\begin{pmatrix}x_1\\x_2\end{pmatrix}) = \begin{pmatrix}1 & 2\\4 & -1\\0 & 2\end{pmatrix}\begin{pmatrix}x_1\\x_2\end{pmatrix}$. Proto jde o lineární zobrazení.

$\square$

**6.5.** Najděte matici vzhledem ke kanonickým bázím lineárního zobrazení $g$ z předchozího příkladu.

Postupujeme stejně jako v Příkladu 6.2. Stačí tedy dosadit vektory kanonické báze do $g$ a seřadíme je do sloupců matice $[g]^{K_2}_{K_3} = \begin{pmatrix}1 & 2\\4 & -1\\0 & 2\end{pmatrix}$. $\square$

**6.6.** Mějme $A = (\begin{pmatrix}1\\4\end{pmatrix}, \begin{pmatrix}3\\1\end{pmatrix})$ bázi prostoru $\mathbb{Z}_7^2$ a $B = (\begin{pmatrix}1\\1\\2\end{pmatrix}, \begin{pmatrix}1\\0\\3\end{pmatrix}, \begin{pmatrix}6\\0\\5\end{pmatrix})$ bázi prostoru $\mathbb{Z}_7^3$. Najděte matici lineárního zobrazení $h : \mathbb{Z}_7^2 \to \mathbb{Z}_7^3$ vzhledem k bázím $A$ a $B$, známe-li matici $h$ vzhledem ke kanonickým bázím $[h]^{K_2}_{K_3} = \begin{pmatrix}1 & 3\\4 & 0\\2 & 6\end{pmatrix}$.

Dvojí aplikací Tvrzení 6.15 můžeme vyjádřit hledanou matici $[h]^A_B$ jakou součin matic:

$$[h]^A_B = [\mathrm{Id}]^{K_3}_B \cdot [h]^A_{K_3} = [\mathrm{Id}]^{K_3}_B \cdot [h]^{K_2}_{K_3} \cdot [\mathrm{Id}]^A_{K_2} = ([\mathrm{Id}]^B_{K_3})^{-1} \cdot [h]^{K_2}_{K_3} \cdot [\mathrm{Id}]^A_{K_2}.$$

Snadno určíme přímo podle definice matice přechodu od kanonické báze k bázi $A$ resp. $B$, tj. do sloupečků sepíšeme bázi $A$ resp. $B$:

$$[\mathrm{Id}]^A_{K_2} = \begin{pmatrix}1 & 3\\4 & 1\end{pmatrix}, \quad [\mathrm{Id}]^B_{K_3} = \begin{pmatrix}1 & 1 & 6\\1 & 0 & 0\\2 & 3 & 5\end{pmatrix}.$$

Dokončení úlohy je už jen rutinním počítáním s maticemi:

$$[h]_B^A = \begin{pmatrix} 1 & 1 & 6 \\ 1 & 0 & 0 \\ 2 & 3 & 5 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 3 \\ 4 & 0 \\ 2 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 6 \\ 1 & 0 & 0 \\ 2 & 3 & 5 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 6 & 6 \\ 4 & 5 \\ 5 & 5 \end{pmatrix}.$$

Nyní součin matic dopočítáme standardním postupem:

$$\left(\begin{array}{ccc|cc} 1 & 1 & 6 & 6 & 6 \\ 1 & 0 & 0 & 4 & 5 \\ 2 & 3 & 5 & 5 & 5 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 4 & 5 \\ 0 & 1 & 6 & 2 & 1 \\ 0 & 3 & 5 & 4 & 2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 4 & 5 \\ 0 & 1 & 6 & 2 & 1 \\ 0 & 0 & 1 & 5 & 6 \end{array}\right) \sim \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 4 & 5 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 5 & 6 \end{array}\right).$$

Zjistili jsme, že $[h]_B^A = \begin{pmatrix} 4 & 5 \\ 0 & 0 \\ 5 & 6 \end{pmatrix}$. □

**6.7.** Buď $A = ((1,1,1)^T, (1,0,1)^T(1,1,0)^T)$ báze vektorového prostoru $\mathbb{Z}_3^3$ a $B = ((1,2)^T, (1,1^T))$ báze vektorového prostoru $\mathbb{Z}_3^2$. Najděte maticí lineárního zobrazení $\psi : \mathbb{Z}_3^3 \to \mathbb{Z}_3^2$ vzhledem ke kanonickým bázím, má-li matici $[\psi]_B^A = \begin{pmatrix} 1 & 1 & 0 \\ 2 & 1 & 1 \end{pmatrix}$ vzhledem k bázím $A$ a $B$.

Postupujeme stejně jako v předchozí úloze s využitím Tvrzení 6.15:

$$[\psi]_{K_2}^{K_3} = [\mathrm{Id}]_{K_2}^B \cdot [\psi]_B^A \cdot [\mathrm{Id}]_A^{K_3} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 2 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}^{-1}.$$

a některým ze známých způsobů dopočítáme $[\psi]_{K_2}^{K_3} = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 0 \end{pmatrix}$. □

**6.8.** Uvažujme první derivaci $()'$ na lineárním prostoru reálných polynomů $\mathbb{R}[x]_4 = \{\sum_{i=0}^3 a_i x^i |\ a_i \in \mathbb{R}\}$ stupně menšího než 4 a označme $K = (x^0, x^1, x^2, x^3)$ bázi $\mathbb{R}[x]_4$. Z matematické analýzy víme, že je $()'$ lineární zobrazení.

(a) Najděte matici $[()']_K^K$,
(b) určete jádro $\mathrm{Ker}()'$ a $\mathrm{Im}()'$,
(c) je-li nějaká $B$ báze $\mathbb{R}[x]_4$, najděte nejmenší $n$ pro které $([()']_B^B)^n = \mathbf{0}$.

(a) Stačí derivovat jednotlivé polynomy báze $K$ a určit souřadnice derivací vzhledem k této bázi:

$[(x^0)']_K = [0]_K = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $[(x^1)']_K = [x^0]_K = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $[(x^2)']_K = [2x^1]_K = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}$,

$[(x^3)']_K = [3x^2]_K = \begin{pmatrix} 0 \\ 0 \\ 3 \\ 0 \end{pmatrix}$, tedy $[()']_K^K = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

(b) Odpověď dostaneme buď elementární úvahou na půdě matematické analýzy, která říká, že nulovou derivaci mají právě konstantní funkce, tedy $\mathrm{Ker}()' = \langle x^0 \rangle$, a obrazem polynomů stupně menšího než 4 jsou právě polynomy stupně menšího než 3, tedy $\mathrm{Im}()' = \langle x^0, x^1, x^2 \rangle$, nebo týž výsledek můžeme vyčíst v souřadnicích vzhledem ke $K$ z matice $[()']_K^K$ pomocí Tvrzení 6.25.

(c) Uvědomíme-li si, že složením n derivací dostaneme derivaci n-tého stupně, tj. $(()')^n = ()^{(n)}$ a připomeneme-li si, že $(\mathbb{R}[x]_4)^{(n)} = 0$, právě když $n \geq 4$, pak stačí jen opakovaně využít Tvrzení 6.15, abychom zjistili, že

$$([()']_B^B)^n = ([(()')^n]_B^B) = ([()^{(n)}]_B^B) = \mathbf{0} \Leftrightarrow n \geq 4.$$

To ovšem znamená, že nejmenší $n$ pro které $([()']_B^B)^n = \mathbf{0}$ je $n = 4$. □

**6.9.** Najděte matici lineárního zobrazení $\varphi$ vektorového prostoru $\mathbb{R}^2$ vzhledem ke kanonickým bázím, víte-li, že $\varphi((1,2)^T) = (3,0)^T$ a $\varphi((2,1)^T) = (3,3)^T$.

Protože $B = ((1,2)^T, (2,1)^T)$ tvoří bázi $\mathbb{R}^2$, zaručuje nám Tvrzení 7.4, že daná podmínka určuje lineární zobrazení $f$ jednoznačně, a bezprostředně z definice dostaneme matici $[\varphi]_{K_2}^B = \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix}$. Dále postupujeme obvyklým způsobem:

$$[\varphi]_{K_2}^{K_2} = [\varphi]_{K_2}^B \cdot [\mathrm{Id}]_B^{K_2} = [\varphi]_{BK_2} \cdot ([\mathrm{Id}]_{K_2}^B)^{-1} =$$

$$= \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 3 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} -\frac{1}{3} & \frac{2}{3} \\ \frac{2}{3} & -\frac{1}{3} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}.$$

□

**6.10.** Je-li $\begin{pmatrix} 2 & 3 & 1 & 4 \\ 1 & 1 & 2 & 5 \\ 1 & 2 & 6 & 6 \end{pmatrix}$ matice lineárního zobrazení $f : \mathbb{Z}_7^4 \to \mathbb{Z}_7^3$ vzhledem k bázím $M = ((1,1,0,0)^T, (0,1,1,0)^T, (0,0,1,1)^T, (1,0,0,0)^T)$ prostoru $\mathbb{Z}_7^4$ a $N = ((3,1,4)^T, (3,3,0)^T, (2,1,6)^T)$ prostoru $\mathbb{Z}_7^3$. Určete dimenze jádra $\mathrm{Ker}\, f$ a obrazu $\mathrm{Im} f$.

Nejprve standardní cestou určíme hodnost matice $[f]_N^M = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 1 & 1 & 2 & 5 \\ 1 & 2 & 6 & 6 \end{pmatrix}$ a zjistíme, že $h([f]_{MN}) = 2$. Nyní využijeme Tvrzení 5.94, které říká, že $\dim(\mathrm{Im} f) = h([f]_{MN}) = 2$ a že $\dim(\mathrm{Im} f) + \dim(\mathrm{Ker}\, f) = \dim(\mathbb{Z}_7^4) = 4$. Proto $\dim(\mathrm{Ker}\, f) = 4 - \dim(\mathrm{Im} f) = 2$. □

## 7. Determinanty

**7.1.** Spočítejte nad tělesy $\mathbf{Q}$, $\mathbf{R}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ determinant matice $\mathbf{A} = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$.

Postupujeme přímo podle definice. Rozmyslíme si, že $S_2 = \{\mathrm{Id}, (12)\}$. a proto $\det(\mathbf{A}) = 3 \cdot 2 - 1 \cdot 1 = 5$ nad tělesy $\mathbf{Q}$, $\mathbf{R}$. Obvyklá úvaha o počítání v tělesech $\mathbb{Z}_p$ nám umožní využít výsledku spočítaného v tělese reálných (či racionálních) čísel, který nakonec stačí upravit modulo $p$. To znamená, že $\det(\mathbf{A}) = (5) \bmod 5 = 0$ nad tělesem $\mathbb{Z}_5$ a $\det(\mathbf{A}) = (5) \bmod 7 = 5$ nad tělesem $\mathbb{Z}_7$. □

**7.2.** Spočítejte nad tělesy $\mathbf{Q}$, $\mathbf{R}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ determinant matice $\mathbf{B} = \begin{pmatrix} 1 & 2 & 1 \\ 4 & 0 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

I tentokrát budeme fakticky postupovat podle definice. Sudým permutacím Id, (123) a (132) z $S_3$ odpovídají po řadě součiny $1 \cdot 0 \cdot 1$, $2 \cdot 3 \cdot 2$ a $1 \cdot 4 \cdot 3$ (vždy bereme nejprve hodnotu z prvního řádku, poté z druhého a nakonec z třetího) a lichým permutacím (12), (13) a (23) odpovídají součiny $2 \cdot 4 \cdot 1$, $1 \cdot 0 \cdot 2$ a $1 \cdot 3 \cdot 3$, proto

$$\det(\mathbf{B}) = \det\left(\begin{pmatrix} 1 & 2 & 1 \\ 4 & 0 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right) = 1 \cdot 0 \cdot 1 + 2 \cdot 3 \cdot 2 + 1 \cdot 4 \cdot 3 - (2 \cdot 4 \cdot 1 + 1 \cdot 0 \cdot 2 + 1 \cdot 3 \cdot 3).$$

Tedy $\det(\mathbf{B}) = 7$ nad tělesy $\mathbf{Q}$, $\mathbf{R}$, $\det(\mathbf{B}) = 2$ nad tělesem $\mathbb{Z}_5$ a $\det(\mathbf{B}) = 0$ nad tělesem $\mathbb{Z}_7$. □

**7.3.** Rozhodněte, zda je nad tělesy $\mathbf{Q}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ regulární matice:

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 4 & 4 \end{pmatrix}, \ \mathbf{B} = \begin{pmatrix} 2 & 2 & 3 \\ 1 & 3 & 2 \\ 1 & 1 & 3 \end{pmatrix}, \ \mathbf{A} \cdot \mathbf{B} \text{ a } \mathbf{A}^{555}.$$

Díky Tvrzení 7.22 stačí zjistit, zda jsou determinanty jednotlivých matic nenulové. Spočítejme nejprve determinanty matic $\mathbf{A}$ a $\mathbf{B}$:

$$\det \mathbf{A} = \det \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 4 & 4 \end{pmatrix} = \det \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \\ -3 & -4 & 0 \end{pmatrix} = \det \begin{pmatrix} 2 & 1 \\ -3 & -4 \end{pmatrix} = -5$$

nad $\mathbf{Q}$, $\det \mathbf{A} = 0$ nad $\mathbb{Z}_5$ a $\det \mathbf{A} = 2$ nad $\mathbb{Z}_7$, což znamená, že je $\mathbf{A}$ regulární nad $\mathbf{Q}$ a $\mathbb{Z}_7$ a $\mathbf{A}$ je singulární nad $\mathbb{Z}_5$. Podobně

$$\det \mathbf{B} = \det \begin{pmatrix} 2 & 2 & 3 \\ 1 & 3 & 2 \\ 1 & 1 & 3 \end{pmatrix} = \det \begin{pmatrix} 2 & 0 & 3 \\ 1 & 2 & 2 \\ 1 & 0 & 3 \end{pmatrix} = 2 \cdot \det \begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix} = 6$$

nad $\mathbf{Q}$, $\det \mathbf{B} = 1$ nad $\mathbb{Z}_5$ a $\det \mathbf{B} = 6$ nad $\mathbb{Z}_7$, tedy $\mathbf{B}$ jr regulární nad všemi tělesy $\mathbf{Q}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$. Použijeme-li Větu 7.26, která říká, že $\det(\mathbf{A} \cdot \mathbf{B}) = \det(\mathbf{A}) \cdot \det(\mathbf{B})$, pak vidíme, že $\det(\mathbf{A} \cdot \mathbf{B}) \neq 0$ právě když $\det \mathbf{A} \neq 0$ a $\det \mathbf{B} \neq 0$. Tudíž matice $\mathbf{A} \cdot \mathbf{B}$ je regulární nad $\mathbf{Q}$ a $\mathbb{Z}_7$ a není regulární nad $\mathbb{Z}_5$. Konečně indukčním rozšířením Věty 7.26 dostaneme, že $\det(\mathbf{A}^{555}) = \det(\mathbf{A})^{555}$, a proto je matice $\mathbf{A}^{555}$ regulární právě nad tělesy $\mathbf{Q}$ a $\mathbb{Z}_7$. □

**7.4.** Určete nad tělesy $\mathbf{Q}$, $\mathbf{R}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ determinanty matic

$$\mathbf{C}_1 = \begin{pmatrix} 3 & 4 & 4 & 2 & 1 \\ 0 & 2 & 4 & 0 & 3 \\ 0 & 0 & 4 & 3 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix} \quad \text{a} \quad \mathbf{C}_2 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 2 & 4 & 0 & 3 \\ 0 & 0 & 4 & 3 & 2 \\ 3 & 4 & 4 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

Determinant matice $\mathbf{C}_1 = (c_{ij})$ můžeme opět spočítat podle definice, uvědomíme-li si, že pro každou neidentickou permutaci $\sigma \in S_5$ bude existovat aspoň jedno $j$, pro něž $j > \sigma(j)$, a proto $c_{j\sigma(j)} = 0$ a $c_{1\sigma(1)} \cdot \dots \cdot c_{5\sigma(5)} = 0$. Tedy determinant Gaussovy čtvercové matice $\mathbf{C}_1$ je právě součin hodnot na hlavní diagonále, tj.

$\det(\mathbf{C}_1) = 3 \cdot 2 \cdot 4 \cdot 1 \cdot 2 = 48$ nad tělesy $\mathbf{Q}$ a $\mathbf{R}$, $\det(\mathbf{C}_1) = (48) \bmod 5 = 3$ nad tělesem $\mathbb{Z}_5$ a $\det(\mathbf{C}_1) = (48) \bmod 7 = 6$ nad tělesem $\mathbb{Z}_7$.

Nyní si všimněme, že matici $\mathbf{C}_2$ dostaneme z matice $\mathbf{C}_1$ výměnou 1. a 4. řádku. Proto podle Tvrzení 7.18 a 7.19 je $\det(\mathbf{C}_2) = -\det(\mathbf{C}_1)$, tudíž $\det(\mathbf{C}_2) = -48$ nad tělesy $\mathbf{Q}$, $\mathbf{R}$, $\det(\mathbf{C}_2) = (-48) \bmod 5 = 2$ nad tělesem $\mathbb{Z}_5$ a $\det(\mathbf{C}_2) = (-48) \bmod 7 = 1$ nad tělesem $\mathbb{Z}_7$. $\square$

**7.5.** Spočítejte nad tělesy $\mathbf{Q}$, $\mathbf{R}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ determinant matice $\mathbf{D} = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 1 & 1 & 0 & 3 \\ 0 & 2 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

Připomeňme, že Tvrzení 7.18 a 7.19 nám říkají, jak se změní determinant matice, provedeme-li některou z řádkových úprav. V předchozí úloze jsme si navíc uvědomili, že je velmi snadné určit determinant Gaussovy matice jako součin hodnot na hlavní diagonále. Budeme-li tedy standardními prostředky pomocí elementárních úprav řádků převádět matici $\mathbf{D}$ na její Gaussovu matici, budeme v každém kroku znát, jak jsme původní determinant změnili. Tedy upravujme a počítejme:

$$\det(\mathbf{D}) = \det(\begin{pmatrix} 1 & 0 & 2 & 1 \\ 1 & 1 & 0 & 3 \\ 0 & 2 & 1 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix}) = \det(\begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & -2 & 2 \\ 0 & 2 & 1 & 2 \\ 0 & 2 & 1 & 3 \end{pmatrix}) =$$

$$= \det(\begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 5 & -2 \\ 0 & 0 & 5 & -1 \end{pmatrix}) = \det(\begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 5 & -2 \\ 0 & 0 & 0 & 1 \end{pmatrix}) = 1 \cdot 1 \cdot 5 \cdot 1 = 5.$$

Tedy zjistili jsme, že $\det(\mathbf{D}) = 5$ nad tělesy $\mathbf{Q}$, $\mathbf{R}$, $\det(\mathbf{D}) = 0$ nad tělesem $\mathbb{Z}_5$ a $\det(\mathbf{D}) = 5$ nad tělesem $\mathbb{Z}_7$. $\square$

**7.6.** Spočítejte nad tělesy $\mathbf{Q}$, $\mathbf{R}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ determinant matice $\mathbf{G} = \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 0 & 3 & 0 \\ 1 & 4 & 1 & 2 \\ 2 & 2 & 4 & 0 \end{pmatrix}$.

Tentokrát k výpočtu použijeme Tvrzení 7.18 Větu 7.32 a budeme determinant rozvíjet podle 2. řádku:

$$\det(\mathbf{G}) = (-1)^{2+1} \cdot 0 \cdot \det(\begin{pmatrix} 0 & 2 & 1 \\ 4 & 1 & 2 \\ 2 & 4 & 0 \end{pmatrix}) + (-1)^{2+2} \cdot 0 \cdot \det(\begin{pmatrix} 1 & 2 & 1 \\ 1 & 1 & 2 \\ 2 & 4 & 0 \end{pmatrix}) +$$

$$+ (-1)^{2+3} \cdot 3 \cdot \det(\begin{pmatrix} 1 & 0 & 1 \\ 1 & 4 & 2 \\ 2 & 2 & 0 \end{pmatrix}) + (-1)^{2+4} \cdot 0 \cdot \det(\begin{pmatrix} 1 & 0 & 2 \\ 1 & 4 & 1 \\ 2 & 2 & 4 \end{pmatrix}) =$$

$$= -3 \cdot \det(\begin{pmatrix} 1 & 0 & 1 \\ 1 & 4 & 2 \\ 2 & 2 & 0 \end{pmatrix}) = -3 \cdot (1 \cdot 1 \cdot 2 - 1 \cdot 4 \cdot 2 - 1 \cdot 2 \cdot 2) = 30.$$

Tedy jako obvykle $\det(\mathbf{G}) = 18$ nad $\mathbf{Q}$ a $\mathbf{R}$, $\det(\mathbf{G}) = 3$ nad $\mathbb{Z}_5$ a $\det(\mathbf{G}) = 4$ nad $\mathbb{Z}_7$. $\square$

Poznamenejme, že jsme determinanty ani další členy rozvoje, které přísluší nulovému prvku z řádku, podle nějž determinant rozvíjíme, vůbec nemuseli psát. Navíc si uvědomme, že tato metoda je vhodná právě v případě, kdy některý z řádků nebo sloupců, využijeme-li pozorování obsahuje ,,hodně”nul.

**7.7.** Spočítejte determinant matice $\mathbf{H} = \begin{pmatrix} 1 & 3 & -3 & 1 & 1 \\ 3 & 2 & 7 & 5 & -9 \\ 2 & 1 & -1 & 2 & 0 \\ 1 & 2 & 2 & 1 & -1 \\ 2 & -1 & 3 & 2 & 7 \end{pmatrix}$ nad tělesem racionálních čísel.

V matici $\mathbf{H}$ sice žádný řádek ani sloupec neobsahuje větší počet nul, ovšem první a čtvrtý sloupec se liší jen na jedné pozici. Víme, že odečteme-li od jednoho z těchto sloupců druhý, nezmění se podle Tvrzení 7.19 hodnota determinantu. Po této úpravě už ovšem můžeme použít metodu rozvoje podle sloupce (tedy Větu 7.32):

$$\det(\mathbf{H}) = \det(\begin{pmatrix} 1 & 3 & -3 & 1 & 1 \\ 3 & 2 & 7 & 5 & -9 \\ 2 & 1 & -1 & 2 & 0 \\ 1 & 2 & 2 & 1 & -1 \\ 2 & -1 & 3 & 2 & 7 \end{pmatrix}) = \det(\begin{pmatrix} 0 & 3 & -3 & 1 & 1 \\ -2 & 2 & 7 & 5 & -9 \\ 0 & 1 & -1 & 2 & 0 \\ 0 & 2 & 2 & 1 & -1 \\ 0 & -1 & 3 & 2 & 7 \end{pmatrix}) =$$

$$= (-1)\cdot(-2)\cdot\det(\begin{pmatrix} 3 & -3 & 1 & 1 \\ 1 & -1 & 2 & 0 \\ 2 & 2 & 1 & -1 \\ -1 & 3 & 2 & 7 \end{pmatrix}).$$

Nyní odečteme od prvního řádku upravené matice trojnásobek druhého řádku. Na prvním řádku zůstanou dva nenulové prvky, podle nichž determinant rozvedeme a snadno dopočítáme:

$$\det(\mathbf{H}) = 2\cdot\det(\begin{pmatrix} 3 & -3 & 1 & 1 \\ 1 & -1 & 2 & 0 \\ 2 & 2 & 1 & -1 \\ -1 & 3 & 2 & 7 \end{pmatrix}) = 2\cdot\det(\begin{pmatrix} 0 & 0 & -5 & 1 \\ 1 & -1 & 2 & 0 \\ 2 & 2 & 1 & -1 \\ -1 & 3 & 2 & 7 \end{pmatrix}) =$$

$$= 2\cdot(-5)\cdot\det(\begin{pmatrix} 1 & -1 & 0 \\ 2 & 2 & -1 \\ -1 & 3 & 7 \end{pmatrix}) - 2\cdot 1\cdot\det(\begin{pmatrix} 1 & -1 & 2 \\ 2 & 2 & 1 \\ -1 & 3 & 2 \end{pmatrix}) =$$

$$= -10\cdot(14-1+3+14) - 2\cdot(4+1+12+4+4-3) = -344.$$

□

**7.8.** Rozhodněte pro která reálná $a$ jsou reálné matice $\mathbf{P}(a) = \begin{pmatrix} 1 & 1 & 0 \\ a & 1 & a \\ 1 & a & 0 \end{pmatrix}$, $\mathbf{Q}(a) = \begin{pmatrix} a & -1 & -1 \\ a-1 & 1 & 1 \\ a+1 & 1 & 0 \end{pmatrix}$, $\mathbf{P}(a)\cdot\mathbf{Q}(a)$ a $\mathbf{P}(a)^{257}\cdot\mathbf{Q}(a)^{374}$ regulární.

Nejprve spočítáme determinanty $\det(\mathbf{P}(a)) = \det \begin{pmatrix} 1 & 1 & 0 \\ a & 1 & a \\ 1 & a & 0 \end{pmatrix} = a - a^2$, a

$$\det(\mathbf{Q}(a)) = \det \begin{pmatrix} a & -1 & -1 \\ a-1 & 1 & 1 \\ a+1 & 1 & 0 \end{pmatrix} = \det \begin{pmatrix} 2a-1 & 0 & 0 \\ a-1 & 1 & 1 \\ a+1 & 1 & 0 \end{pmatrix} = 1 - 2a.$$

Věta 7.22 z přednášky říká, že je matice regulární, právě když je její determinant nenulový. Determinanty matic $\mathbf{P}(a)$ a $\mathbf{Q}(a)$ už jsme spočítali, zbývá nám s využitím Věty 7.26 spočítat $\det(\mathbf{P}(a) \cdot \mathbf{Q}(a)) = \det(\mathbf{P}(a)) \cdot \det(\mathbf{Q}(a)) = a(1-a)(1-2a)$. Vidíme, že je matice $\mathbf{P}(a)$ regulární, právě když $a \in \mathbf{R} \setminus \{0, 1\}$, matice $\mathbf{Q}(a)$ je regulární, právě když $a \in \mathbf{R} \setminus \{\frac{1}{2}\}$ a součin $\mathbf{P}(a) \cdot \mathbf{Q}(a)$ je regulární, právě když $a \in \mathbf{R} \setminus \{0, \frac{1}{2}, 1\}$.

Konečně indukční aplikací Věty 7.26 dostáváme, že

$$\det(\mathbf{P}(a)^{257} \cdot \mathbf{Q}(a)^{374}) = \det(\mathbf{P}(a))^{257} \cdot \det(\mathbf{Q}(a))^{374} = a^{257}(1-a)^{257}(1-2a)^{374}.$$

Protože polynom $a^{257}(1-a)^{257}(1-2a)^{374}$ v proměnné $a$ nemá jiné kořeny než $0$, $\frac{1}{2}$, $1$, vidíme, že je matice $\mathbf{P}(a)^{257} \cdot \mathbf{Q}(a)^{374}$ regulární opět právě tehdy, když $a \in \mathbf{R} \setminus \{0, \frac{1}{2}, 1\}$. □

**7.9.** Rozhodněte pro která $x \in \mathbb{Z}_5$ je matice $\begin{pmatrix} 2x & x+3 & 2x+1 \\ x+4 & 3x+2 & 3 \\ x+1 & x & 4x \end{pmatrix}$ nad tělesem $\mathbb{Z}_5$ singulární.

Opět spočítáme determinant matice $\mathbf{A}(x) = \begin{pmatrix} 2x & x+3 & 2x+1 \\ x+4 & 3x+2 & 3 \\ x+1 & x & 4x \end{pmatrix}$, nejprve přičteme třetí sloupec k druhému a pak rozvedeme podle třetího řádku:

$$\det \begin{pmatrix} 2x & x+3 & 2x+1 \\ x+4 & 3x+2 & 3 \\ x+1 & x & 4x \end{pmatrix} = \det \begin{pmatrix} 2x & 3x+4 & 2x+1 \\ x+4 & 3x & 3 \\ x+1 & 0 & 4x \end{pmatrix} =$$

$$= (x+1) \cdot (4x^2 + x + 2) + 4x \cdot (3x^2 + 4x + 4) = x^3 + x^2 + 4x + 2.$$

Stejně jako v předchozí úloze potřebujeme najít $x \in \mathbb{Z}_5$, pro něž je hodnota $\det(\mathbf{A}(x)) = x^3 + x^2 + 4x + 2 = 0$, což snadno zjistíme dosazováním jednotlivých prvků tělesa $\mathbb{Z}_5$:

$$\det(\mathbf{A}(0)) = 2,\ \det(\mathbf{A}(1)) = 1^3 + 1^2 + 4 \cdot 1 + 2 = 3,\ \det(\mathbf{A}(2)) = 2^3 + 2^2 + 4 \cdot 2 + 2 = 2,$$

$$\det(\mathbf{A}(3)) = 3^3 + 3^2 + 4 \cdot 3 + 2 = 0, \qquad \det(\mathbf{A}(4)) = 4^3 + 4^2 + 4 \cdot 4 + 2 = 3.$$

Zjistili jsme, že je matice $\mathbf{A}(x)$ singulární, právě když je $x = 3$. □

**7.10.** Vyřešte nad reálnými čísly soustavu rovnic $\mathbf{A}\mathbf{x}^T = (1, 0, 0)^T$ s reálným parametrem $a$, kde $\mathbf{A} = \begin{pmatrix} 2a+1 & a & 2a \\ a & 1 & a+1 \\ 2a & 0 & 2a \end{pmatrix}$.

Pro počítání použijeme Cramerovo pravidlo, tedy Věty 7.28 z přednášky. Nejdříve určíme $\det \mathbf{A} = 2a \cdot (a+1)$. To znamená, že Cramerovo pravidlo můžeme využít pro parametr $a \in \mathbf{R} \setminus \{0, -1\}$, t.j. je-li matice A regulární. Dále určíme determinant matic $\mathbf{A}_i$, které vzniknou z matice $\mathbf{A}$ nahrazením $i$-tého sloupce sloupcem pravých stran vektorem, tedy $(1,0,0)^T$:

$$\det \mathbf{A}_1 = \det \begin{pmatrix} 1 & a & 2a \\ 0 & 1 & a+1 \\ 0 & 0 & 2a \end{pmatrix} = 2a, \ \det \mathbf{A}_2 = \det \begin{pmatrix} 2a+1 & 1 & 2a \\ a & 0 & a+1 \\ 2a & 0 & 2a \end{pmatrix} = 2a \text{ a}$$

$$\det \mathbf{A}_3 = \det \begin{pmatrix} 2a+1 & a & 1 \\ a & 1 & 0 \\ 2a & 0 & 0 \end{pmatrix} = -2a.$$

Nyní pomocí Věty 7.28 spočítáme hodnotu $i$-té neznámé jako $x_i = (\det \mathbf{A})^{-1} \cdot \det \mathbf{A}_i$. Tedy $x_1 = x_2 = \frac{2a}{2a(a+1)} = \frac{1}{a+1}$ a $x_3 = \frac{-2a}{2a(a+1)} = -\frac{1}{a+1}$. Konečně standardním postupem zjistíme, že soustava pro $a = -1$ nemá řešení a pro $a = 0$ leží všechna řešení v množině $(1,0,0)^T + \langle((0,1,-1))\rangle$. □

## 8. Kongruence celých čísel a Euklidův algoritmus

Nechť $a$, $b$ jsou dvě přirozená čísla. Připomeňme **Euklidův algoritmus** hledání největšího společného dělitele čísel $a$ a $b$:

```
gcd(a,b)
if b = 0 return a
else return gcd(b, a mod b)
```

Postupně tedy počítáme hodnoty $a_i$, kdy $a_0 = a$ a $a_1 = b$, pro něž platí $a_{i+1} = (a_{i-1}) \bmod a_i$. Tedy víme, že existuje takové $q_i \in \mathbf{N}$ že $a_{i-1} = q_i a_i + a_{i+1}$ a $a_{i+1} < a_i$. Algoritmus skončí, když $a_{n+1} = 0$, potom $a_n = \gcd(a_0, a_1)$.

**8.1.** Najděte pomocí Euklidova algoritmu
(a) $\gcd(4116, 2849)$,
(b) $\gcd(7^{1000} - 1, 7^{999} - 1)$.

(a) Mezivýsledky v běhu Euklidova algoritmu budeme stejně jako výše označovat $a_i$:
$a_0 = 4116$,
$a_1 = 2849$,
$a_2 = 4116 - 2849 = 1267$,
$a_3 = 2849 - 2 \cdot 1267 = 315$,
$a_4 = 1267 - 4 \cdot 315 = 7 = \gcd(4116,2849)$,
$a_5 = 315 - 45 \cdot 7 = 0$.
Spočítali jsme, že největší společný dělitel čísel 4116 a 2849 je 7.
(b) Všimněme si, že $7 \cdot (7^{999} - 1) - (7^{1000} - 1) = 6$ a označíme $c = \gcd(7^{1000} - 1, 7^{999} - 1)$ a $d = \gcd(6, 7^{999} - 1)$. Protože jistě $c | 7^{999} - 1$ a $c | 7^{1000} - 1$ platí, že $c | 6 = 7 \cdot (7^{999} - 1) - (7^{1000} - 1)$. Tedy $c$ je společný dělitel čísel 6 i $7^{999} - 1$, proto $c | d$.

Naopak číslo $d$ dělí hodnotu 6 i $7^{999} - 1$, proto dělí i číslo $(7^{1000} - 1) = 7 \cdot (7^{999} - 1) - 6$, tudíž $d | c$. Vidíme, že místo $\gcd(7^{1000} - 1, 7^{999} - 1)$ stačí spočítat $\gcd(6, 7^{999} - 1)$. Protože ovšem obecně $a^{n+1} - 1 = (a-1)\sum_{i=0}^{n} a^i$ a v našem případě $7^{999} - 1 = (7-1)\sum_{i=0}^{998} 7^i$, vidíme, $6 / 7^{999} - 1$, a proto $\gcd(7^{1000} - 1, 7^{999} - 1) = \gcd(6, 7^{999} - 1) = 6$. □

Na bodu (b) předchozího příkladu si lze snadno uvědomit, že obdobně funguje indukční krok důkaz Euklidova algoritmu.

**8.2.** Za předpokladu, že pro všechna $a, b, c \in \mathbf{N}$ platí podmínka $c/a$ a $c/b \rightarrow c/NSD(a,b)$, dokažte, že Euklidův algoritmus pro nalezení největšího společného dělitele dvou přirozených čísel pracuje správně.

Budeme používat značení mezivýsledků Euklidova algoritmu zavedené výše.
Nejprve si všimněme, že $a_n = \gcd(a_{n-1}, a_n)$, neboť $a_n/a_{n-1}$ a poté dokážeme, že $\gcd(a_i, a_{i+1}) = \gcd(a_{i-1}, a_i)$.
Položme $c = NSD(a_{i-1}, a_i)$ a $d = NSD(a_i, a_{i+1})$. Protože $d/a_i$ a $d/a_{i+1}$, platí, že $d/q \cdot ai + a_{i+1} = a_{i-1}$, tudíž $d/c$. Podobně nahlédneme, že $c/a_{i+1} = a_{i-1} - q \cdot ai$, tedy $c = d$. Tím jsme ověřili, že

$$a_n = \gcd(a_n, a_{n-1}) = \cdots = \gcd(a_2, a_1) = \gcd(a_1, a_0).$$

$\square$

**8.3.** Najděte pomocí Euklidova algoritmu celá čísla $x$ a $y$, aby $x$ bylo kladné a
(a) $30x + 101y = 1$,
(b) $18x + 25y = 1$.

(a) Nejprve si všimněme, že číslo 101 je prvočíslo, tedy největší společný dělitel čísel 30 a 101 je zcela jistě roven jedné. Euklidův algoritmus na nalezení největšího společného dělitele čísel 30 a 101 nám tedy samozřejmě musí dát výsledek 1. Přesto ho použijeme a budeme věnovat pozornost vztahu předchozích a následujících prvků:
$a_0 = 101$,
$a_1 = 30$,
$a_2 = 101 - 3 \cdot 30 = 11$,
$a_3 = 30 - 2 \cdot 11 = 8$,
$a_4 = 11 - 8 = 3$,
$a_5 = 8 - 2 \cdot 3 = 2$,
$a_6 = 3 - 2 = 1 = \gcd(101, 30)$.
Vidíme, že každé $a_{i+1}$ je celočíselnou kombinací prvků $a_i$ a $a_{i-1}$, budeme-li postupně dosazovat předchozí vyjádření do následujících výrazů, dostaneme každé $a_{i+1}$ jako celočíselnou kombinací prvků $a_0$ a $a_1$:
$a_2 = 11 = 101 - 3 \cdot 30$, (to je vyjádření využívající přímo hodnot 30 a 101)
$a_3 = 8 = 30 - 2 \cdot 11 = 30 - 2 \cdot (101 - 3 \cdot 30) = 7 \cdot 30 - 2 \cdot 101$, (dosadíme jen za 11)
$a_4 = 3 = 11 - 8 = (101 - 3 \cdot 30) - (7 \cdot 30 - 2 \cdot 101) = 3 \cdot 101 - 10 \cdot 30$,
$a_5 = 2 = 8 - 2 \cdot 3 = (7 \cdot 30 - 2 \cdot 101) - 2 \cdot (3 \cdot 101 - 10 \cdot 30) = 27 \cdot 30 - 8 \cdot 101$,
$a_6 = 1 = 3 - 2 = (3 \cdot 101 - 10 \cdot 30) - (27 \cdot 30 - 8 \cdot 101) = 11 \cdot 101 - 37 \cdot 30$.
Našli jsme řešení $x = -37$ a $y = 11$, které ovšem nevyhovuje požadavku na kladnost $x$. Upravíme-li rovnost

$$1 = 11 \cdot 101 - 37 \cdot 30 + c \cdot 101 \cdot 30 - cc \cdot 101 \cdot 30 = (11 + 30c) \cdot 101 - (37 + 101c) \cdot 30$$

vidíme, že řešením úlohy jsou hodnoty $x = -37 - 101c$ a $y = 11 + 30c$ pro každé celé $c$. Zvolíme-li $c = -1$ dostáváme vyhovující řešení $x = 64$ a $y = -19$.
(b) Protože $\gcd(18, 25) = 1$, zaručuje nám Euklidův algoritmus existenci požadovaných čísel $x, y \in \mathbb{Z}$. Euklidův algoritmus použijeme (podobně jako v předchozí úloze) i k jejich nalezení:
$a_0 = 25$,
$a_1 = 18$,
$a_2 = 7 = 25 - 18$,
$a_3 = 4 = 18 - 2 \cdot 7 = 18 - 2 \cdot (25 - 18) = 3 \cdot 18 - 2 \cdot 25$,

$a_4 = 3 = 7 - 4 = 25 - 18 - (3 \cdot 18 - 2 \cdot 25) = 3 \cdot 25 - 4 \cdot 18,$
$a_5 = \gcd(25, 18) = 1 = 4 - 3 = 3 \cdot 18 - 2 \cdot 25 - (3 \cdot 25 - 4 \cdot 18) = 7 \cdot 18 - 5 \cdot 25.$
Vidíme, že $x = 7$ a $y = -5$. □

Hodnotám $x$ a $y$,které jsme našli pomocí Euklidova algoritmu se obvykle říká *Bezoutovy koeficienty.* V následující úloze ukážeme, že lze nalezení Bezoutových koeficientů snadno formalizovat rekurentním vzorcem.

**8.4.** Uvažujme hodnoty $a_0 > a_1 > \cdots > a_{i+1} > a_i > \ldots a_n = \gcd(a_0, a_1)$ získané během Euklidova algoritmu, tj. $a_{i-1} = q_i a_i + a_{i+1}$ a $a_n | a_{n-1}$. Definujme posloupnosti $x_i$ a $y_i$ tak, že $x_0 = y_1 = 1$, $x_1 = y_0 = 0$, a pro $i \geq 1$ položme $x_{i+1} = x_{i-1} - x_i \cdot q_i$ a $y_{i+1} = y_{i-1} - y_i \cdot q_i$. Dokažte, že $a_i = x_i \cdot a_0 + y_i \cdot a_1$ pro každé $i = 0, \ldots, n$, a speciálně, že $\gcd(a_0, a_1) = x_n \cdot a_0 + y_n \cdot a_1$.

Platnost formule $a_i = x_i \cdot a_0 + y_i \cdot a_1$ dokážeme indukcí podle $i$.

Pro $i = 0, 1$ dostáváme $x_0 \cdot a_0 + y_0 \cdot a_1 = 1 \cdot a_0 + 0 \cdot a_1 = a_0$ a $x_1 \cdot a_0 + y_1 \cdot a_1 = 0 \cdot a_0 + 1 \cdot a_1 = a_1$.

Předpokládejme, že tvrzení platí pro $i - 1$ a $i$, tedy, že platí

$$a_{i-1} = x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1 \quad \text{a} \quad a_i = x_i \cdot a_0 + y_i \cdot a_1$$

a dokážeme, že tvrzení platí i pro $i + 1$. Dosadíme-li do (obecně platného) výrazu $a_{i+1} = a_i \cdot q_i - a_{i-1}$ hodnoty $a_i$ a $a_{i-1}$ z indukčního předpokladu, dostaneme

$$a_{i+1} = (x_i \cdot a_0 + y_i \cdot a_1) \cdot q_i - x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1 =$$
$$= (x_{i-1} - x_i \cdot q_i) \cdot a_0 + (y_{i-1} - y_i \cdot q_i) \cdot a_1 = x_{i+1} \cdot a_0 + y_{i+1} \cdot a_1.$$

Tedy $a_{i+1} = x_{i+1} \cdot a_0 + y_{i+1} \cdot a_1$, což jsme měli ověřit. □

**8.5.** Najděte řešení rovnice $30x \equiv 1 \pmod{101}$.

Hledáme celá $x$ a $y$, aby $30x + 101y = 1$. Tuto úlohu jsme ovšem řešili v Příkladu 8.3, tedy $11 \cdot 101 - 37 \cdot 30 = 1$ a $30 \cdot (-37) \equiv 1 \pmod{101}$, proto $x = -37$. □

**8.6.** Najděte celá čísla $x$ a $y$, aby

(a) $\gcd(891, 473) = 891x + 473y$,

(b) $\gcd(4321, 1234) = 4321x + 1234y$.

(a) Položíme $a_0 = 891$ a $a_1 = 495$ a počítáme stejně jako v úloze 8.3:
$a_2 = 418 = 891 - 473,$
$a_3 = 55 = 473 - 418 = 473 - (891 - 473) = 2 \cdot 473 - 891,$
$a_4 = 33 = 418 - 7 \cdot 55 = (891 - 473) - 7 \cdot (2 \cdot 473 - 891) = 8 \cdot 891 - 15 \cdot 473,$
$a_5 = 22 = 55 - 33 = (2 \cdot 473 - 891) - (8 \cdot 891 - 15 \cdot 473) = 17 \cdot 473 - 9 \cdot 891,$
$a_6 = 11 = 33 - 22 = (8 \cdot 891 - 15 \cdot 473) - (17 \cdot 473 - 9 \cdot 891) = 17 \cdot 891 - 32 \cdot 473.$
Spočítali jsme, že $11 = \gcd(891, 473) = 17 \cdot 891 - 32 \cdot 473$, proto tedy $x = 17$ a $y = -32$.

(b) Tentokrát použijeme rekurentní vzorec. Nejprve ovšem opět musíme spočítat celočíselné zbytky i podíly v průběhu Euklidova algoritmu pro $a_0 = 4321$ a $a_1 = 1234$:
$a_2 = 619 = 4321 - 3 \cdot 1234$, tedy $q_1 = 3$,
$a_3 = 615 = 1234 - 619$, tedy $q_2 = 1$,
$a_4 = 4 = 619 - 615$, tedy $q_3 = 1$,

$a_5 = 3 = 615 - 153 \cdot 4$, tedy $q_4 = 153$,
$a_6 = 1 = 4 - 3$, tedy $q_5 = 1$,
Nyní položíme $(x_0, y_0) = (1, 0)$ a $(x_1, y_1) = (0, 1)$ a počítáme:

$$x_2 = x_0 - q_1 x_1 = 1 - 3 \cdot 0 = 1 \quad \text{a} \quad y_2 = y_0 - q_1 y_1 = 0 - 3 \cdot 1 = -3,$$

$$x_3 = x_1 - q_2 x_2 = 0 - 1 \cdot 1 = -1 \quad \text{a} \quad y_3 = y_1 - q_2 y_2 = 1 - 1 \cdot (-3) = 4,$$

$$x_4 = x_2 - q_3 x_3 = 1 - 1 \cdot (-1) = 2 \quad \text{a} \quad y_4 = y_2 - q_3 y_3 = -3 - 1 \cdot 4 = -7,$$

$$x_5 = x_3 - q_4 x_4 = -1 - 153 \cdot 2 = -307 \quad \text{a} \quad y_5 = y_3 - q_4 y_4 = 4 - 153 \cdot (-7) = 1075,$$

$$x_6 = x_4 - q_5 x_5 = 2 - 1 \cdot (-307) = 309 \quad \text{a} \quad y_6 = y_4 - q_5 y_5 = -7 - 1 \cdot 1075 = -1082,$$

Spočítali jsem, že $\gcd(4321, 1234) = 1 = 4321 \cdot 309 - 1234 \cdot 1082$, tedy $x = 309$ a $y = -1082$. □

**8.7.** Najděte $x \in \mathbb{Z}$ splňující
(a) $1234x \equiv 1 \pmod{4321}$,
(b) $1234x \equiv 1 \pmod{4321}$ a $x > 0$
(c) $1234x \equiv 2 \pmod{4321}$,

(a) Úlohu už jsme vyřešili v předchozím příkladu, kde jsme spočítali, že

$$1234 \cdot (-1082) \equiv 1 \pmod{4321},$$

proto řešením je například $x = -1082$.
(b) Snadno nahlédneme, že naší kongruenci řeší všechny hodnoty

$$x = 4321 \cdot a - 1082$$

pro libovolné celé $a$, tedy zadané podmínce vyhovuje například řešení $x = 4321 - 1082 = 3239$.
(c) Tentokrát stačí vynásobit řešení úlohy (a) nebo (b) dvojkou, tedy například $x = -2164$. □

**8.8.** Najděte poslední cifru čísla celá čísla $x$ a $y$, aby
(a) $7^{777}$,
(b) $153^{831}$.

(a) Zajímá nás hodnota $(7^{777}) \bmod 10$. Počítejme:

$$(7^1) \bmod 10 = 7, \quad (7^2) \bmod 10 = 9, \quad (7^3) \bmod 10 = (9 \cdot 7) \bmod 10 = 3,$$

$$(7^4) \bmod 10 = (3 \cdot 7) \bmod 10 = 1.$$

To znamená, že

$$(7^{777}) \bmod 10 = (7^{776} \cdot 7) \bmod 10 = ((7^4)^{194} \cdot 7) \bmod 10 = (1^{194} \cdot 7) \bmod 10 = 7.$$

(b) Stejně jako v případě (a) nahlédneme, že $(3^4) \bmod 10 = 1$, proto

$$(153^{831}) \bmod 10 = (3^{831}) \bmod 10 = (3^{828} \cdot 3^3) \bmod 10 = ((3^4)^{207} \cdot 7) \bmod 10 = 7.$$

□

**8.9.** Dokažte, že je číslo $16^{15} + 29^{14} + 42^{13}$ dělitelné číslem 13.

Potřebujeme dokázat, že $(16^{15} + 29^{14} + 42^{13}) \equiv 0 \pmod{13}$. Proto upravujme:
$$(16^{15} + 29^{14} + 42^{13}) \equiv 3^{15} + 3^{14} + 3^{13} \equiv 3^{13} \cdot (9 + 3 + 1) \equiv 3^{13} \cdot 0 \equiv 0 \pmod{13},$$
čímž jsme hotovi. □

**8.10.** Dokažte, že $n^6 - n^2$ je dělitelné číslem 60 pro každé přirozené $n$.

Nejprve upravíme $(n^6 - n^2) = (n^2 - 1)n^2(n^2 + 1) = (n - 1)n(n + 1)n(n^2 + 1)$. Protože $(n - 1)$, $n$, $(n + 1)$ jsou tři po sobě jdoucí čísla, je právě jedno z nich je dělitelné třemi aspoň jedno dělitelné dvěma, proto $6|(n-1)n(n+1)|(n^6-n^2)$. Tedy
$$n^6 - n^2 \equiv n^2(n^4 - 1) \equiv (n^2 - 1)n^2(n^2 + 1) \equiv (n^2 - 1)n^2(n^2 - 4) \pmod 5$$
$$\text{a dále } (n^2 - 1)n^2(n^2 - 4) \equiv n(n - 2)(n - 1)n(n + 1)(n + 2) \equiv 0 \pmod 5.$$
Protože $(n-2)$, $(n-1)$, $n$, $(n+1)$, $(n+2)$ je pět po sobě jdoucích čísel, tudíž právě jedno z nich je dělitelné pěti. Tím jsme dokázali, že nejmenší společný násobek čísel 3, 4 a 5, jímž je číslo 60, dělí $n^6 - n^2$. □

**8.11.** Najděte největšího společného dělitele reálných polynomů
$$p = x^4 + x^3 + 2x^2 + x + 1 \quad \text{a} \quad q = x^3 + x^2 + x + 1.$$
Dále najděte reálné polynomy $a$ a $b$ tak, aby $\gcd(p, q) = a.p + b.q$.

I tentokrát můžeme podobně jako v případě počítání v celých číslech k hledání největšího společného dělitele dvou polynomů (tj. monického polynomu, který oba polynomy dělí a je největšího možného stupně) použít Euklidův algoritmus. Místo celočíselného dělení se zbytkem budeme ovšem používat dělení polynomů se zbytkem (připomeňme, že zbytek po takovém dělení musí být buď nulový nebo musí mít stupeň menší než dělitel). Není těžké nahlédnout, že stejným postupem jako v úloze 8.2, lze obecně ověřit korektnost algoritmu. Počítejme:

$a_0 = x^4 + x^3 + 2x^2 + x + 1,$
$a_1 = x^3 + x^2 + x + 1,$
$a_2 = x^2 + 1 = x^4 + x^3 + 2x^2 + x + 1 - x.(x^3 + x^2 + x + 1),$
$a_3 = 0 = x^3 + x^2 + x + 1 - (x + 1)(x^2 + 1).$

Největším společným dělitelem polynomů $x^4 + x^3 + 2x^2 + x + 1$ a $x^3 + x^2 + x + 1$ je polynom $x^2 + 1$. Rozšířený Euklidův algoritmus má tentokrát jediný krok, tedy hledané polynomy jsou $a = 1$ a $b = -x$. □

**8.12.** Najděte polynomy $a, b \in \mathbb{R}[x]$ tak, aby $1 = a \cdot (x^3 + 2) + b \cdot (x^2 + 1)$.

Opět využijme rozšířeného Euklidova algoritmu na polynomy $a_0 = x^3 + 2$ a $a_1 = x^2 + 1$:

$a_2 = -x + 2 = x^3 + 2 - x \cdot (x^2 + 1),$
$a_3 = 5 = x^2 + 1 + (x + 2) \cdot (-x + 2) = (x + 2) \cdot (x^3 + 2) + (-x^2 - 2x + 1) \cdot (x^2 + 1),$

Vydělením číslem 5 dostáváme $1 = \frac{1}{5}(x+2) \cdot (x^3+2) + \frac{1}{5}(-x^2 - 2x + 1) \cdot (x^2+1)$. Spočítali jsme, že $a = \frac{x+2}{5}$ a $b = \frac{-x^2-2x+1}{5}$. □

Připomeňme, na množině $\mathbb{Z}_n$ definice operací $+_n$ a $\cdot_n$ předpisem $a +_n b = (a + b) \bmod n$ a $a \cdot_n b = (a \cdot b) \bmod n$, kde mod $n$ znamená zbytek po celočíselném dělení hodnotou $n$.

**8.13.** Je-li $n > 1$ celé číslo, dokažte, že $\mathbb{Z}_n$ spolu s operacemi $+_n$ a $\cdot_n$ splňuje axiomy (S1)–(S4), (N1), (N2), (N4), (D) a ($\neg$T) z definice tělesa.

Z vlastností kongruencí, jednoznačnosti zbytku po celočíselném dělení a asociativity sčítání na celých číslech spočítáme, že

$$(a +_n b) +_n c = ((a + b)\text{mod } n + c)\text{mod } n {=} ((a + b) + c)\text{mod } n =$$

$$(a + (b + c))\text{mod } n {=} ((a + b)\text{mod } n + c)\text{mod } n = a +_n (b +_n c).$$

Stejnou úvahou pro násobení dostaneme

$$(a \cdot_n b) +_n c {=} ((a \cdot b) \cdot c)\text{mod } n = (a \cdot (b \cdot c))\text{mod } n {=} a \cdot_n (b \cdot_n c).$$

Ukázali jsme, že jsou axiomy (S1) a (N1) splněny. Platnost komutativních zákonů, tedy axiomů (S4) a (N4) plyne okamžitě z definice operací a komutativity příslušných operací na celých číslech, podobně snadno z definice operací nahlédneme, že $0 +_n a = a$ a $1 \cdot_n a = a$ pro každé $a \in \mathbb{Z}_n$, tedy i axiomy (S2) a (N2) platí. Dále $-0 = 0$ a $-a = n - a$ pro všechna $a \in \mathbb{Z}_n \setminus \{0\}$, protože $(a + n - a)\text{mod } n = (n)\text{mod } n = 0$. odkud dostáváme platnost axiomu (S3). Distributivitu, tedy axiom (D), ověříme stejně jako asociativitu s využitím distributivity na celých číslech:

$$(a +_n b) \cdot_n c {=} ((a + b) \cdot c)\text{mod } n = (a \cdot c + b \cdot c)\text{mod } n {=} a \cdot_n c +_n b \cdot_n c.$$

Konečně axiom netriviality je zřejmý z předpokladu, že $n > 1$. $\square$

**8.14.** Jsou-li $r, s \in \mathbf{N}$, $r > 1, s > 1$ a položme $n = rs$. Dokažte, že $\mathbb{Z}_n$ spolu s operacemi $+_n$ a $\cdot_n$ není těleso.

Ukázali jsme, že $\mathbb{Z}_n$ splňuje všechny axiomy tělesa s výjimkou axiomu (N3). Protože víme, že v každém tělese musí podle Tvrzení 3.3(6) z přednášky platit pro $a \neq 0$ a $b \neq 0$, že $a \cdot b \neq 0$, stačí, abychom tuto podmínku vyvrátili. Položíme-li $a = r$ a $b = s$, pak vidíme, že $a \neq 0$ a $b \neq 0$, ovšem $a \cdot b = (n)\text{mod } n = 0$. $\square$

Jak bylo na přednášce ukázáno ve Větě 3.4 tvoří $\mathbb{Z}_p$ pro $p$ prvočíslo těleso (v dalším budeme u operací index $_p$ obvykle vynechávat). Připomeňme, že nalezení inverzního prvky je dokázáno konstruktivně pomocí Euklidova algoritmu:

**8.15.** Najděte inverzní prvek k prvku 30 v tělese $\mathbb{Z}_{101}$.

Potřebujeme najít číslo $x \in \mathbb{Z}_{101}$, které by řešilo rovnici $(30 \cdot x)\text{mod } 101 = 1$, což můžeme reformulovat tak, že hledáme celá $x$ a $y$, z nichž $x$ má ležet v $\mathbb{Z}_{101}$, aby $30x + 101y = 1$. Tuto úlohu už jsme ovšem vyřešili v Příkladu 8.3, nyní si stačí uvědomit, že nalezené $x$, které neleží v požadovaném intervalu můžeme posunout pomocí vhodného násobku čísla 101. Dostaneme tedy zbytek po celočíselném dělení číslem 101, tj. $30^{-1} = (-37)\text{mod } 101 = 101 - 37 = 64$, protože

$$1 = 11 \cdot 101 - 37 \cdot 30 = 11 \cdot 101 - 30 \cdot 101 + 101 \cdot 30 - 37 \cdot 30 = (11 - 30) \cdot 101 + (101 - 37) \cdot 30.$$

Tedy jsme našli další a pro nás zajímavější řešení řešení $1 = 64 \cdot 30 - 19 \cdot 101$ rovnice z 8.3.

**8.16.** Najděte nad tělesem $\mathbb{Z}_{101}$ prvky $63^{-1}$, $20^{-1}$, $2^{-1}$, $(20 \cdot 63)^{-1}$ a vyřešte nad ním rovnici $20 \cdot_{101} x = 7$.

U prvních dvou hodnot postupujme stejně jako v předchozích úvahách, tedy využijeme Euklidův algoritmus:
$38 = 101 - 63$,
$25 = 63 - 38 = 2 \cdot 63 - 101$,
$13 = 38 - 25 = 2 \cdot 101 - 3 \cdot 63$,
$12 = 25 - 13 = 5 \cdot 63 - 3 \cdot 101$,
$1 = 13 - 12 = 5 \cdot 101 - 8 \cdot 63$.
Zjistili jsme, že $63^{-1} = (-8) \mathrm{mod}\ 101 = 93$.
Podobně už v prvním kroku Euklidova algoritmu zjistíme, že $1 = 101 - 5 \cdot 20$, tedy $20^{-1} = (-5) \mathrm{mod}\ 101 = 96$
Při určování hodnoty $2^{-1}$ můžeme udělat jednoduchou obecnou úvahu pro $\mathbb{Z}_p$, kde $p$ je liché prvočíslo, že $\frac{p+1}{2} \in \mathbb{Z}_p$ a že $(2 \cdot \frac{p+1}{2}) \mathrm{mod}\ p = (p+1) \mathrm{mod}\ p = 1$, tedy $2^{-1} = \frac{101+1}{2} = 51$ v tělese $\mathbb{Z}_{101}$.
Uvážíme-li, že z axiomatiky tělesa plyne $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ a $(-a)^{\cdot}(-b) = a \cdot b$ pro všechny jeho prvky $a$ a $b$ (zkuste podrobně dokázat!), a využijeme-li vypočítaných hodnot, pak

$$(20 \cdot_{101} 63)^{-1} = 20^{-1} \cdot_{101} 63^{-1} = (-5) \cdot_{101} (-8) = 40.$$

Protože obvyklý způsob upravovaní rovnic je ekvivalentní (tj. vratný) i pro rovnice nad obecným tělesem, zjišťujeme, že hledané $x$ je tvaru $x = 20^{-1} \cdot_{101} 7 = 96 \cdot_{101} 7 = 66$. □

**Další úlohy**

(1) Rozhodněte, zda je posloupnost vektorů $(1,3,2,1)^T$, $(3,0,1,1)^T$, $(1,4,2,4)^T$ lineárně závislá ve vektorovém prostorech $\mathbf{R}^4$, $\mathbf{C}^4$, $\mathbb{Z}_5^4$ a $\mathbb{Z}_7^4$.
(2) Určete bázi a dimenzi podprostoru $\langle (1,3,2,1)^T,\ (3,0,1,1)^T,\ (1,4,2,4)^T \rangle$ vektorových prostorů $\mathbf{R}^4$, $\mathbf{C}^4$, $\mathbb{Z}_5^4$ a $\mathbb{Z}_7^4$.
(3) Najděte všechny podmnožiny množiny $X = \{(1,2,1,1,1)^T, (3,1,3,3,3)^T, (2,4,2,2,2)^T, (1,0,1,3,2)^T\}$, které tvoří bázi podprostoru $U = \langle X \rangle$ vektorových prostorů $\mathbf{Q}^5$, $\mathbb{Z}_5^5$, $\mathbb{Z}_7^5$.
(4) Kolik existuje bází podprostoru $\langle (1,1,2,0)^T,\ (4,1,3,1)^T,\ (1,3,2,1)^T \rangle$ vektorových prostorů $\mathbb{Z}_5^4$ a $\mathbb{Z}_7^4$?
(5) Určete dimenze podprostorů $\mathbf{U}$, $\mathbf{V}$, $\mathbf{U}+\mathbf{V}$ a $\mathbf{U} \cap \mathbf{V}$ vektorových prostorů $\mathbb{Z}_5^4$ nad tělesem $\mathbb{Z}_5$ a $\mathbb{Z}_7^4$ nad tělesem $\mathbb{Z}_7$, jestliže $\mathbf{U} = \langle (1,2,1,3)^T, (1,2,4,1)^T, (3,4,1,0)^T \langle$ a $\mathbf{V} = \langle (4,1,2,3)^T,\ (0,3,3,1)^T,\ (1,2,1,3)^T \rangle$.
(6) Uvažujme v lineárním prostoru $\mathbb{Z}_5^3$ nad tělesem $\mathbb{Z}_5$ posloupnosti vektorů

$$B_1 = (\begin{pmatrix}1\\2\\4\end{pmatrix}, \begin{pmatrix}3\\2\\1\end{pmatrix}, \begin{pmatrix}1\\1\\2\end{pmatrix}), B_2 = (\begin{pmatrix}3\\2\\1\end{pmatrix}, \begin{pmatrix}1\\1\\2\end{pmatrix}, \begin{pmatrix}1\\2\\4\end{pmatrix}),$$

$$B_3 = (\begin{pmatrix}2\\3\\4\end{pmatrix}, \begin{pmatrix}3\\1\\2\end{pmatrix}, \begin{pmatrix}1\\2\\1\end{pmatrix}), B_4 = (\begin{pmatrix}2\\0\\3\end{pmatrix}, \begin{pmatrix}4\\1\\3\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix})$$

a označme $B_0$ kanonickou bázi lineárního prostoru $\mathbb{Z}_5^3$ nad tělesem $\mathbb{Z}_5$.
(a) Ověřte, že je $B_i$ pro každé $i = 1,2,3,4$ báze $\mathbb{Z}_5^3$,
(b) najděte matice přechodu $[\mathrm{Id}]_{B_j}^{B_i}$ pro všechna $i, j \in \{0,1,2,3,4\}$,

(c) najděte pro každé $i \in \{0,1,2,3,4\}$ báze $C$ a $D$, aby

$$[\mathrm{Id}]_C^{B_i} = [\mathrm{Id}]_{B_i}^D = \begin{pmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix}.$$

(7) Určete nad tělesy $\mathbf{R}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ hodnost matice $\mathbf{A} = \begin{pmatrix} 2 & 0 & 1 \\ 2 & 1 & 0 \\ 3 & 3 & 1 \end{pmatrix}$, matice $\mathbf{A}+\mathbf{A}$ a $\mathbf{A}\cdot\mathbf{A}$.

(8) Najděte nad tělesy $\mathbf{R}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ všechna řešení homogenní soustavy rovnic s maticí $\mathbf{A}$ z předchozí úlohy.

(9) Najděte nad tělesy $\mathbf{Q}$, $\mathbb{Z}_3$ a $\mathbb{Z}_7$ všechna řešení nehomogenní soustavy rovnic s maticí $\left(\begin{array}{ccccc|c} 1 & 0 & 1 & 2 & 2 & 2 \\ 2 & 0 & 2 & 1 & 1 & 0 \end{array}\right)$.

(10) Je-li podprostor $\mathbf{U} = \langle (2,4,0,1,4)^T, (1,2,1,0,3)^T \rangle$ vektorového prostoru $\mathbb{Z}_5^5$ nad tělesem $\mathbb{Z}_5$, najděte bázi nějakého takového podprostoru $\mathbf{V}$, aby $\mathbf{U}+\mathbf{V} = \mathbb{Z}_5^5$ a $\mathbf{U}\cap\mathbf{V} = \{\mathbf{0}\}$.

(11) Uvažujme podprostor $\mathbf{W} = \langle (1,6,2,4,5)^T \rangle$ vektorového prostoru $\mathbb{Z}_7^5$ nad tělesem $\mathbb{Z}_7$. Najděte báze nějakých takových podprostorů $\mathbf{U}$ a $\mathbf{V}$, aby $\dim(\mathbf{U})^T = \dim(\mathbf{V})^T = 3$, $\mathbf{U}+\mathbf{V} = \mathbb{Z}_7^5$ a $\mathbf{U}\cap\mathbf{V} = \mathbf{W}$.

(12) Kolika způsoby lze lineárně nezávislou posloupnost $((1,2,2,1)^T, (2,1,1,0)^T)$ doplnit na bázi (chápanou jako posloupnost, tj. záleží na pořadí prvků) vektorového prostoru $\mathbb{Z}_3^4$?

(13) Buď $k \leq n$ přirozená čísla, $p$ prvočíslo a $\mathbf{U}$ podprostor dimenze $k$ vektorového prostoru $\mathbb{Z}_p^n$ nad tělesem $\mathbb{Z}_p$. Určete kolik existuje podprostorů $\mathbf{V}$ prostoru $\mathbb{Z}_p^n$, pro něž platí, že $\mathbf{U}+\mathbf{V} = \mathbb{Z}_5^5$ a $\mathbf{U}+\mathbf{V} = \{\mathbf{0}\}$.

(14) Dokažte, že lze nad tělesem $\mathbb{Q}$ převést posloupností elementárních řádkových úprav matici $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix}$ na matici $\mathbf{B} = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 3 & 5 \end{pmatrix}$.

(15) Uvažujme matice $\mathbf{A}$ a $\mathbf{B}$ z předchozího příkladu. Najděte nějakou posloupností elementárních řádkových úprav, pomocí nichž lze převést matici $\mathbf{A}$ na matici $\mathbf{B}$.

(16) Nechť $f : \mathbb{Z}_7^4 \to \mathbb{Z}_7^3$ je zobrazení určené předpisem $g((x_1,x_2,x_3,x_4)) = (2x_1+3x_2+6x_3+x_4, 6x_1+5x_2+2x_3+3x_4, 3x_1+3x_2+3x_3+5x_4)$. Spočítejte dimenze a báze jádra $\mathrm{Ker}\, f$ a obrazu $\mathrm{Im} f$, rozhodněte, zda $\begin{pmatrix} 2 \\ 3 \\ 6 \end{pmatrix} \in \mathrm{Im} f$ a najděte matice $[f]_{K_3}^{K_4}$, $[f]_{K_3}^{B}$, $[f]_C^{K_4}$ a $[f]_C^B$, jestliže $K_3$ a $K_4$ jsou kanonické báze a $B = (\begin{pmatrix} 4 \\ 3 \\ 5 \\ 6 \end{pmatrix}, \begin{pmatrix} 3 \\ 6 \\ 4 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 0 \\ 0 \end{pmatrix})$, $C = (\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 0 \end{pmatrix})$

(17) Spočítejte determinant matic $\mathbf{A} = \begin{pmatrix} 2 & 1 & 2 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 2 & 1 & 2 \\ 2 & 1 & 1 & 0 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 1 & 1 & 0 & 2 \\ 2 & 1 & 1 & 2 \\ 1 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 \end{pmatrix}$, $\mathbf{A}^{-1}$, $\mathbf{A}\cdot\mathbf{B}$ a $\mathbf{A}\cdot\mathbf{B}^{-1}$ nad tělesy $\mathbf{R}$, $\mathbf{C}$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$.

(18) Najděte pro libovolná $a \in \mathbf{Q}$ nad $\mathbf{Q}$ rekurentní vzorec pro výpočet determinant čtvercové matice $\mathbf{G}_n = (g_{ij})$ stupně $n$, kde $g_{ii} = 1$, $g_{ii+1} = a$ a $g_{i+1i} = b$ a jinde je $g_{ij} = 0$.

(19) Rozhodněte, zda jsou nad tělesy $\mathbf{Q}$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ regulární matice $\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 0 \\ 2 & 1 & 2 \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ a $\mathbf{B}^3$.

(20) Najděte nad tělesy $\mathbf{Q}$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$ adjungované matice k maticím z předchozí úlohy.

(21) Rozhodněte, pro která $a \in \mathbb{Z}_7$ je nad $\mathbb{Z}_7$ matice $\begin{pmatrix} a & 2+a & 1 \\ 3a+2 & 1 & a \\ 2a^2 & a+6 & 2+a \end{pmatrix}$ regulární.

(22) Najděte pro všechna $a \in \mathbb{Z}_7$, pro něž je to možné, inverzní matici k matici z předchozí úlohy.

(23) Spočítejte $(\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 3 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ 3 & 4 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 4 \\ 1 & 3 \end{pmatrix})^{-1}$ nad tělesy $\mathbf{R}$, $\mathbb{Z}_5$ a $\mathbb{Z}_7$.