## 1. 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 $a_{i+1} = (a_{i-1})\mathrm{mod}\ \ a_i$. 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 $a_n = \gcd(a_0, a_1)$.

**1.1.** 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.

**1.2.** Za předpkladu, 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

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

□

**1.3.** 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 $x, y \in \mathbf{Z}$. 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.

**1.4.** 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. □

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

Hledáme celá $x$ a $y$, aby $30x + 101y = 1$. Tuto úlohu jsme ovšem řešili v Příkladu 1.3, tedy $11 \cdot 101 - 37 \cdot 30 = 1$ a $30 \cdot (-37) \equiv 1 \pmod{101}$, proto $x = -37$. □

**1.6.** 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 1.3:

$a_2 = 418 = 891 - 473$,

$a_3 = 55 = 473 - 418 = 473 - (891 - 473) = 2 \cdot 473 - 891$,

$a_4 = 33 = 418 - 7 \cdot 55 = (891 - 473) - 7 \cdot (2 \cdot 473 - 891) = 8 \cdot 891 - 15 \cdot 473$,

$a_5 = 22 = 55 - 33 = (2 \cdot 473 - 891) - (8 \cdot 891 - 15 \cdot 473) = 17 \cdot 473 - 9 \cdot 891$,

$a_6 = 11 = 33 - 22 = (8 \cdot 891 - 15 \cdot 473) - (17 \cdot 473 - 9 \cdot 891) = 17 \cdot 891 - 32 \cdot 473$.

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 $y = -1082$. □

**1.7.** Najděte $x \in \mathbf{Z}$ 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 vynássobit řešení úlohy (a) nebo (b) dvojkou, tedy například $x = -2164$. □

**1.8.** 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

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

□

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

Potřebujeme dokáat, 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. □

**1.10.** 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 a spoň jedno dělitelné dvěma, proto $6|(n - 1)n(n + 1)|(n^6 - n^2)$. Tedy

$$n^6 - n^2 \equiv n^2(n^4 - 1) \equiv (n^2 - 1)n^2(n^2 + 1) \equiv (n^2 - 1)n^2(n^2 - 4) \pmod{5}$$

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 $n^6 - n^2$. □

*16.10.*

**1.11.** 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 težké nahlédnout, že stejným postupem jako v úloze 1.2, 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 $b = -x$. □

**1.12.** Najděte polynomy $a, b \in \mathbf{R}[x]$ 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 $b = \frac{-x^2-2x+1}{5}$. □

## 2. Řešení soustav lineárních rovnic

**2.1.** Najděte reálné rešení soustavy rovnic:

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

Nejprve si soustavu zapíšeme do rozšířené matice (stejně jako v sekci 2.3.2 na přednášce) a poté ji pomocí přičtení vhodného násobku jedné rovnice k rovnici druhé upravíme (na střední škole se tento způsob upravování obvykle nazývá „sčítací metoda"), vše si budeme zapisovat pomocí maticového zápisu. Připomeňme, že soustava rovnic na levo od symbolu $\sim$ má stejnou množinu řešeni jako soustava

rovnic napravo od něj:

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

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), pokračujme v úpravách dále:

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

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

Odečtením pětinásobku druhého řádku od třetího už jsme mohli skončit a poté využít zpětné substituce, ale uvědomme si, že můžeme k výsledku dospět i v maticovém zápisu, tj. můžeme levou stranu matice upravit až na jednotkovou matici. To znamená, že ve sloupci vpravo máme postupně jednoznačně nalezené hodnoty $x = -\frac{3}{14}$, $y = \frac{2}{7}$ a $z = \frac{9}{14}$. □

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

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

Znovu si soustavu zapíšeme do matice a poté ji pomocí přičtení vhodného násobku jedné rovnice k rovnici druhé upravíme stejně jako v úloze 1.1:

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

Snadno si uvědomíme, 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 $(x, y, z)^T = (-\frac{3}{5}, \frac{4}{5}, 0)^T$. Podobně jsme jiné řešení mohli dostat po volbě $z = 1$ a jednoznačném dopočítání $y = x = 0$.

Nzní si uvědomme geometrický význam řešení dané soustavy: každou z rovnic chápeme jako rovinu v $\mathbf{R}^3$ (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 $(3, -4, 5)$ (jde právě o netriviální řešení soustav rovnic se stejnými levými a nulovými pravými stranami). Z geometrického náhledu tedy vidíme, že množin všechna řešení je přímka tvaru $\{(-\frac{3}{5} + 3t, \frac{4}{5} - 4t, 5t)^T \mid t \in \mathbf{R}\}$ □

Připomeňme, že Věta 2.14 z přednášky dokazuje negeometricou argumentací, že jsme v předchozí úloze našli všechna řešení soustavy. Zjevnou výhodou analytického důkazu je to, že se nemusíme omezovat jen na rovnice o dvou či třech neznámých.

**2.3.** Najděte všechna reálná rešení 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 $(x_1, x_2, x_3, x_4) = (2, 0, 2, 1)$. □

**2.4.** Najděte všechna racionální rešení 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 težké nahlédnout, že součin, součet i rozdíl racionálních čísel je opět racionální, proto množina $M = \{(-\frac{3}{5} + 3t, \frac{4}{5} - 4t, 5t)^T |\ t \in \mathbf{Q}\}$ 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 rešení soustavy. □

*23.10.*

## 3. Konečná tělesa

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

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

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

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

Stejnou úvahou pro násobení dostaneme

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

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 $a \in \mathbf{Z}_n$, tedy i axiomy (S2) a (N2) platí. Dále $-0 = 0$ a $-a = n - a$ pro všechna $a \in \mathbf{Z}_n \setminus \{0\}$, protože $(a + n - a) \mathrm{mod}\ n = (n) \mathrm{mod}\ n = 0$. odkud dostáváme platnost axiomu (S3). Distributivitu, tedy axiom (D), ověříme stejně jako asociativitu s využitím distributivity na celých číslech:

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

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

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

Ukázali jsme, že $\mathbf{Z}_n$ 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 $a \cdot b = (n) \mathrm{mod}\ n = 0$. □

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

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

Potřebujeme najít číslo $x \in \mathbf{Z}_{101}$, které by řešilo rovnici $(30 \cdot x) \mathrm{mod}\ 101 = 1$, což můžeme reformulovat tak, že hledáme celá $x$ a $y$, z nichž $x$ má ležet v $\mathbf{Z}_{101}$, aby $30x + 101y = 1$. Tuto úlohu už jsme ovšem vyřešili v Příkladu 1.3, 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. $30^{-1} = (-37) \mathrm{mod}\ 101 = 101 - 37 = 64$, 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 1.3.

**3.4.** Najděte nad tělesem $\mathbf{Z}_{101}$ 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 $\mathbf{Z}_p$, kde $p$ je liché prvočíslo, že $\frac{p+1}{2} \in \mathbf{Z}_p$ a že $(2 \cdot \frac{p+1}{2}) \bmod p = (p+1) \bmod p = 1$, tedy $2^{-1} = \frac{101+1}{2} = 51$ v tělese $\mathbf{Z}_{101}$.

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 $x = 20^{-1} \cdot_{101} 7 = 96 \cdot_{101} 7 = 66$. □

Nadále budeme sčítání a násobení v tělese $\mathbf{Z}_p$ pro prvočíslo $p$ psát bez indexu $_p$, tj. jen $+$ a $\cdot$.

**3.5.** Spočítejte v tělesech $\mathbf{Z}_5$ a $\mathbf{Z}_7$ hodnotu výrazu $(-2)^{-1} \cdot ((2+4) \cdot (4+4)^{-1}) + 3$.

Postupujeme podle definice operací na $\mathbf{Z}_5$ i $\mathbf{Z}_7$, nejprve počítejme nad $\mathbf{Z}_5$:

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

Podobně dostáváme nad $\mathbf{Z}_7$:

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

□

**3.6.** Najděte nad tělesem $\mathbf{Z}_2 = \{0, 1\}$ řešení soustavy rovnic:

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

Soustavu si i v tomto případě zapíšeme do matice a s počítáním v GF(2) ji budeme 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. □

**3.7.** Najděte nad tělesem $\mathbf{Z}_7$ všechna řešení soustavy rovnic $\mathbf{Ax} = \mathbf{b}$ s maticí $\mathbf{A} = \begin{pmatrix} 3 & 1 & 5 & 2 \\ 3 & 2 & 4 & 6 \\ 2 & 5 & 6 & 0 \end{pmatrix}$ a) pro $\mathbf{b} = (1,1,1)^T$, b) pro $\mathbf{b} = (1,2,5)^T$

Opět upravíme rozšířenou matici soustavy na odstupňovanou 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 snadno najdeme jedno partikulární, například $(0,1,0,0)^T$. Dále spočítáme zpětnou substitucí řešení homogenní soustavy pro volbu $(x_3, x_4) = (1,0)$ a $(x_3, x_4) = (0,1)$ a opět využijeme Větu 2.14, podle níž je množina všech řešení nehomogenní soustavy $\mathbf{Ax} = \mathbf{b}$ právě tvaru

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

□

**3.8.** Najděte nad tělesem $\mathbf{Z}_5$ všechna řešení homogenní soustavy rovnic s maticí $\mathbf{A} = \begin{pmatrix} 3 & 1 & 1 & 2 & 4 \\ 1 & 2 & 1 & 2 & 1 \\ 4 & 3 & 0 & 1 & 3 \end{pmatrix}$.

Budeme standardně upravovat matici $\mathbf{A}$ posloupností elementárních úprav na odstupňovanou matici. Nulový vektor pravých stran, který se řádkovými úpravami nebude měnit, přitom nemusí do matice zaznamenávat:

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

Vidíme, že bázické pozice jsou první, třetí a čtvrtá a volné proměnné jsou druhá a pátá. Využijeme Věty 2.14, v níž jsme si ve 2.kapitole přednášky uvědomili, že stačí zvolit hodnoty za volné proměnné $x_2$ a $x_5$ a poté ostatní proměnné jednoznačně dopočítat zpětnou substitucí. Tedy položíme nejprve $(x_2, x_5) = (1,0)$ a poté $(x_2, x_5) = (0,1)$ a postupně budeme dopočítávat řešení. Pro $x_2 = 1$ a $x_5 = 0$ snadno najdeme vektor $(3,1,0,0,0)^T$ řešící soustavu a podobně pro volbu $x_2 = 0$ a $x_5 = 1$ dostáváme řešení $(1,0,2,3,1)^T$.

Spočítali jsme, že množina všech řešení homogenní soustavy rovnic s maticí $\mathbf{A}$ je tvaru

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

□

*30.10.*

**3.9.** Existuje nějaký vektor pravých stran $\mathbf{b} \in \mathbf{Z}_5^3$, pro který neexistuje žádné řešení soustavy $\mathbf{Ax} = \mathbf{b}$, kde $\mathbf{A}$ je matice z úlohy 3.8?

Stačí si uvědomit, že pro každý vektor pravých stran bude mít odstupňovaná matice soustavy na levé straně v každém řádku nenulový koeficient, tedy podle Pozorování 2.3 z přednášky pro každý vektor pravých stran (a volbu hodnot volných proměnných) umíme dopočítat nějaké řešení. Tedy je soustava $\mathbf{Ax} = \mathbf{b}$ řešitelná pro každý vektor $\mathbf{b} \in \mathbf{Z}_5^3$. □

**3.10.** Najděte nad tělesem $\mathbf{Z}_5$ všechna řešení soustavy rovnic $\mathbf{Ax} = (1, 2, 4)^T$, kde $\mathbf{A}$ je matice z úlohy 3.8.

Protože už jsme v úloze 3.8 našli všechna řešení homogenní soustavy s maticí $\mathbf{A}$, zbývá nám podle Věty 2.14 najít už jedno partikulární řešení $\mathbf{u}$ nehomogenní soustavy $\mathbf{Ax} = (1, 2, 4)$. Každé řešení potom budou právě tvaru $\mathbf{u} + \mathbf{w}$ pro vhodné řešení $\mathbf{w}$ homogenní soustavy Postupujeme analogicky výpočtu v příkladu 3.8. Nejprve rozšířenou matici stejnými elementárními úpravami upravíme na odstupňovanou matici a poté dopočítáme řešení pro volbu $x_2 = 0$ a $x_5 = 0$:

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

Soustavu tedy řeší například vektor $(2, 0, 3, 1, 0)$. S využitím hodnot spočítaných v 3.8 dostáváme množinu všech řešení soustavy $\mathbf{Ax} = (1, 2, 4)^T$ ve tvaru

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

□

**3.11.** Najděte v závislosti na parametru $a$ nad tělesem a) $\mathbf{Q}$, b) $\mathbf{Z}_5$, c) $\mathbf{Z}_7$ d) $\mathbf{Z}_{11}$ řešení soustavy rovnic:

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

□

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 $\{(1,0,-1)^T+t(-1,1,0)^T|\ t\in\mathbf{T}\}$ pro těleso $\mathbf{T}$, jestliže je charakteristika tělesa $T$ různá od pěti. V případě b), kdy pracujeme s tělesem $\mathbf{Z}_5$ 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 $(3,0,0)^T$. Pri výpočtu řešení homogenní soustavy máme dvě volné proměnné $x_2$ a $x_3$. Obvyklým postupem nyní najdeme nad $\mathbf{Z}_5$ dvě řešení $(4,1,0)^T$ a $(2,0,1)^T$ (jednočlené) homogenní soustavy, všechna řešení jsou tedy tvaru

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

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

$$\text{a)}\{\begin{pmatrix}1\\0\\-1\end{pmatrix}+t\begin{pmatrix}-1\\1\\0\end{pmatrix}\mid t\in\mathbf{R}\},\qquad \text{b)}\{\begin{pmatrix}1\\0\\4\end{pmatrix}+t\begin{pmatrix}4\\1\\0\end{pmatrix}+s\begin{pmatrix}2\\0\\1\end{pmatrix}\mid s,t\in\mathbf{Z}_5\},$$

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

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 pro $z=1$ a dopočítáme hodnoty homogenní soustavy $y=-\frac{5}{a+2}$ a $x=-(3-\frac{5}{a+2})=-\frac{3a+1}{a+2}$ a množina všech řešení je tvaru

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

pro těleso $\mathbf{T}$, konkrétně:

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

$$\text{d)}\{\begin{pmatrix}\frac{a^2+1}{a+2}\\ \frac{2a+6}{a+2}\\ 0\end{pmatrix}+t\begin{pmatrix}3a+1\\ 5\\ 6a+5\end{pmatrix}\mid t\in\mathbf{Z}_7\},\quad \text{b)}\begin{pmatrix}\frac{a^2+1}{a+2}\\ \frac{2a-1}{a+2}\\ 0\end{pmatrix}+t\begin{pmatrix}3a+1\\ 5\\ 10a+9\end{pmatrix}\mid t\in\mathbf{Z}_{11}\}$$

Závěrem poznamenejme, že symbol $\frac{c}{d}$ je v tělese $\mathbf{Z}_p$ výraz, který je třeba dopočítat , tedy že $\frac{c}{d}=c\cdot d^{-1}$ (stejnětak by tomu bylo v případě například tělese racionálních čísel, kdyby $c$ a $d$ byly nikoli celé, nýbrže obecné racionální hodnoty). □

## 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 $\mathbf{R}$, $\mathbf{Z}_7$ a $\mathbf{Z}_{11}$.

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

Ve všech případech úlohu vyřešíme nejprve v tělese charakteristiky 0, tedy v reálných číslech a poté, obdobně jako tomu bylo v Příkladu 3.11 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 $\mathbf{R}$ a

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

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,

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

(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 $\mathbf{C}^T\cdot\mathbf{B} = \mathbf{C}^T\cdot(\mathbf{B}^T)^T = (\mathbf{B}^T\cdot\mathbf{C})^T = \begin{pmatrix}4 & 6 & 2\\ 7 & 10 & 3\\ 1 & 2 & 1\end{pmatrix}$. Našli jsme výsledky v tělese reálných čísel a nyní je upravýme 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 $\mathbf{C}^T\cdot\mathbf{B} = \begin{pmatrix}4 & 6 & 2\\ 0 & 3 & 3\\ 1 & 2 & 1\end{pmatrix}$ vše nad tělesem $\mathbf{Z}_7$ a

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

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

(c) Využijeme početních pravidel a nejprve upravíme:

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

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

Nyní snadno dopočítáme

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

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

□

**4.2.** 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 $\mathbf{Z}_5$ a definujme zobrazení $\varphi : \mathbf{Z}_5^2 \to \mathbf{Z}_5^2$ a $\psi : \mathbf{Z}_5^3 \to \mathbf{Z}_5^2$ předpisy $\varphi(\mathbf{v}) = \mathbf{A}\mathbf{v}$ a $\psi(\mathbf{v}) = \mathbf{B}\mathbf{v}$

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

(a) Připomeňme, že je zobrazení $\varphi$ prosté, jestliže $\varphi(\mathbf{u}) = \varphi(\mathbf{v}) \implies \mathbf{u} = \mathbf{v}$. Protože $\varphi(\mathbf{u}) = \varphi(\mathbf{v})$, právě když $\varphi(\mathbf{u} - \mathbf{v}) = \varphi(\mathbf{u}) - \varphi(\mathbf{v}) = 0$, lze ekvivalentně prostotu zobrazení $\varphi$ vyjádřit podmínkou $\varphi(\mathbf{u}) = 0 \implies \mathbf{u} = 0$. Tedy nám stačí zjistit, zda mají soustavy rovnic $\mathbf{A}\mathbf{x} = (0,0)^T$ a $\mathbf{B}\mathbf{x} = (0,0)^T$ nějaké nenulové řešení. V obou případech po jediné ekvivalentní úpravě vidíme, že nenulové řešení existují, v prvním případě například $\varphi((3,1)^T) = (0,0)^T = \varphi((0,0)^T)$ a v druhém příkladě například $\psi((4,1,1)^T) = (0,0)^T = \psi((0,0,0)^T)$, proto zobrazení $\varphi$ ani $\psi$ 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 $\mathbf{A}\mathbf{x} = (1,0)^T$ neexistuje. V druhém případě nám stejná úvaha jakou jsme provedli v úloze 3.9 říká, že řešení vždy existuje. Proto $\varphi$ není na, zatímco $\psi$ je zobrazení na $\mathbf{Z}_5^2$.

(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 $\psi(\mathbf{v}) = (0,0)^T$, právě když leží v množině $\{t \cdot \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix} \mid t \in \mathbf{Z}_5\}$.

(d) Tentokrát standardně řešíme soustavu rovnic tvaru $\mathbf{B}\mathbf{x} = (1,2)^T$ 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 $\psi(\mathbf{v}) = (0,0)^T$, právě když leží v množině $\{\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix} \mid t \in \mathbf{Z}_5\}$. □

*6.11.*

**4.3.** Definujme zobrazení $f_{\mathbf{A}} : \mathbf{R}^2 \to \mathbf{Z}_5^2$ předpisem $f_{\mathbf{A}}(\mathbf{v}) = \mathbf{A}\mathbf{v}$ pro reálnou matici $\mathbf{A} = \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix}$.

(a) Dokažte, že je $f_{\mathbf{A}}$ bijekce.
(b) Najděte matici $\mathbf{B}$, pro niž platí $f_{\mathbf{B}} \circ f_{\mathbf{A}} = f_{\mathbf{A}} \circ f_{\mathbf{B}} = \mathrm{Id}$, tedy $f_{\mathbf{B}} = f_{\mathbf{A}}^{-1}$.

(a) Připomeňme, že podle Věty 4.30, z přednášky máme dokázat, že je matice $\mathbf{A}$ regulární. Bod (5) zmíněné věty dokonce dává jednoduchý návod, jak zjistit, zda

je čtvercová matice regulární, stačí upravit Gaussovou eliminací a zjistit, zda je či nenív odstupňovaném tvaru dané matice nulový řádek:

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

Protože je odstupňovaný tvar matice $\mathbf{A}$ bez nulových řádků, jedná se podle Věty 4.30 o regulární matici, která indukuje bijektivní zobrazení $f_{\mathbf{A}}$.

(b) Nejprve si uvědomme, že $f_{\mathbf{A}} \circ f_{\mathbf{B}}(\mathbf{v}) = f_{\mathbf{A}}(\mathbf{B} \cdot \mathbf{v}) = \mathbf{A} \cdot \mathbf{B} \cdot \mathbf{v}$ a podobně že $f_{\mathbf{B}} \circ f_{\mathbf{A}}(\mathbf{v}) = \mathbf{B} \cdot \mathbf{A} \cdot \mathbf{v}$. Chceme-li, aby $f_{\mathbf{B}} = f_{\mathbf{A}}^{-1}$, musí $\mathbf{B} = \mathbf{A}^{-1}$, tedy potřebujeme najít inverzní matici k matici $\mathbf{A}$. K tomu využijeme postup 4.7.2-3. z přednášky: je-li $\mathbf{A}$ čtvercová matice řádu $n$, budeme elementárními úpravami upravovat matici $\mathbf{M}$ rozšířenou o jednotkovou matici, tedy matici $(\mathbf{M}|\mathbf{I}_n)$ tak, abychom dostali matici $(\mathbf{I}_n|\mathbf{N})$. Podaří-li se nám to, bude matice $\mathbf{N}$ právě inverzní maticí k matici $\mathbf{M}$, protože $(\mathbf{I}_n|\mathbf{N}) = (\mathbf{N} \cdot \mathbf{M}|\mathbf{N} \cdot \mathbf{I}_n) = \mathbf{N} \cdot (\mathbf{M}|\mathbf{I}_n)$, v opačném případě dokonce zjsitíme, že $\mathbf{M}$ nebyla regulární (to jsme ovšem už zjišťovali v bodu (a)). Upravujeme tedy řádky rozšířené matice:

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

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

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 zjsitili, že $\mathbf{B} = \mathbf{A}^{-1} = \begin{pmatrix} -4 & 3 \\ 3 & -2 \end{pmatrix}$. □

**4.4.** Existuje-li, najděte inverzní matici k maticím

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

(b) $\mathbf{C} = \begin{pmatrix} 3+4i \end{pmatrix}$ nad tělesem komplexních čísel,

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

(d) $\mathbf{F} = \begin{pmatrix} 2 & 2 \\ 3 & 1 \end{pmatrix}$ nad tělesem $\mathbf{Z}_5$,

(e) $\mathbf{F}$ nad tělesem $\mathbf{Z}_7$,

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

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

(h) $\mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ nad tělesem $\mathbf{Z}_2$.

(a) Počítáme obdobně jako v předchozí úloze:

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

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

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

(b) Snadno si z definice maticového násobení uvědomíme, že máme za úkol spočítat v tělese komplexních čísel hodnotu $(3+4i)^{-1} = \frac{1}{3+4i}$. Obvyklým způsobem tedy rozšíříme zlomky komplexně sdruženou hodnotou a dostaneme

$$\frac{1}{3+4i} = \frac{1}{3+4i} \cdot \frac{3-4i}{3-4i} = \frac{3-4i}{3^2+4^2} = \frac{3}{25} - \frac{4}{25}i$$

Spočítali jsme, že $\mathbf{C}^{-1} = \left((3+4i)^{-1}\right) = \left(\frac{3}{25} - \frac{4}{25}i\right)$.

(c) Postupujeme jako v bodech (a) a (b) s využitím aritmetiky komplexních čísel:

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

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

Tentokrát 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. 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) Upravujeme řádky rozšířené matice nad tělesem $\mathbf{Z}_5$:

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

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

Nyní vidíme, že inverzní matice k matici $\mathbf{F}$ existuje a že $\mathbf{F}^{-1} = \begin{pmatrix} 1 & 3 \\ 2 & 2 \end{pmatrix}$ nad tělesem $\mathbf{Z}_5$.

(e) Upravujeme řádky stejné rozšířené matice tentokrát ovšem nad tělesem $\mathbf{Z}_7$:

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

Nyní jsme 1) přičetli 2-násobek 1. řádku ke 2. (protože $2 \cdot 2 = -3$ v $\mathbf{Z}_7$), 2) přičetli 2. řádek k 1. (protože $5 = -2$ v $\mathbf{Z}_7$) 3) vynásobili 1. řádek číslem 4 a 2. řádek číslem 3 (protože $2^{-1} = 4$ a $5^{-1} = 3$ v $\mathbf{Z}_7$).

Spočítali jsme inverzní matici $\mathbf{F}^{-1} = \begin{pmatrix} 5 & 4 \\ 6 & 3 \end{pmatrix}$ nad tělesem $\mathbf{Z}_7$.

(f) Počítáme opět nad $\mathbf{Z}_7$:

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

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

(g) Tentokrát nemusíme nic počítat a jenom využijeme předchozí výsledek a Tvrzení 4.38(2) z přednášky, které říká

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

(h) 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 $\mathbf{H}^{-1} = \mathbf{H} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$. □

**4.5.** 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 4.22(4) a 4.38(2), 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 $\mathbf{C}\cdot\mathbf{D}^{-1} = \begin{pmatrix} 6 & -8 \\ -9 & 13 \\ -1 & 2 \end{pmatrix}$. □

Připomeňme přirozenou definici $k$-té mocniny čtvercové matice $\mathbf{A}^k = \overbrace{\mathbf{A}\mathbf{A}\ldots\mathbf{A}}^{\text{k-krát}}$.

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

(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 $\mathbf{Z}_5$ 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 $\mathbf{Z}_2$ 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 4.4(h) podmínku $\mathbf{H}^2=\mathbf{I}_4$ splňuje.

□

**4.7.** 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

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

□

**4.8.** 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 $d\in\mathbf{R}$ komutuje s $\mathbf{M}$, vezmem-li $c=6d$ snadno spočítáme, že s $\mathbf{M}$ komutují matice $\begin{pmatrix}3c&0\\-c&2c\end{pmatrix}$ pro každé $c\in\mathbf{R}$.

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. □

*13.11.*

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

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

(a) Nejprve si všimneme si, že je matice $\mathbf{A}$ zjevně invertovatelná, proto v případě, že nějaké řešení maticové rovnice $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$ existuje, potom můžeme obě strany této rovnosti vynásobit zleva maticí $\mathbf{A}^{-1}$ a dostaneme $\mathbf{A}^{-1} \cdot (\mathbf{A} \cdot \mathbf{X}) = \mathbf{A}^{-1} \cdot \mathbf{B}$ a tuto rovnost můžeme dále upravovat:

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

kde druhá rovnost platí díky asociativitě násobení matic, třetí rovnost plyne z definice inverzní matice a poslední rovnost dostáváme z vlastnosti jednotkové matice (tedy, že je $\mathbf{I}_2$ neutrální prvek vzhledem k násobení). Náhledli jsme, že existuje-li $\mathbf{X}$, nutně musí být tvaru $\mathbf{X} = \mathbf{A}^{-1} \cdot \mathbf{B}$ a zbývá ověřit, že matice $\mathbf{A}^{-1} \cdot \mathbf{B}$ splňuje danou podmínku. Tedy podobně jako výše upravujeme

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

kde první rovnost dostáváme z asociativity násobení matic, druhou z definice inverzní matice a poslední rovnost je opět dokázanou vlastností jednotkové matice.

Nyní zbývá některým ze známých způsobů dopočítat jediné řešení, použijeme například metodu úlohy 4.5: $\left(\begin{array}{cc|ccc} 5 & 5 & 1 & 2 & 5 \\ 2 & 3 & 3 & 1 & 1 \end{array}\right) \sim$

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

Zjistili jsme, že $\mathbf{X} = \mathbf{A}^{-1} \cdot \mathbf{B} = \begin{pmatrix} 6 & 3 & 2 \\ 4 & 3 & 6 \end{pmatrix}$.

(b) Uvědomme si, že máme fakticky vzřešit dvě soustavy rovnic $\mathbf{A}\mathbf{x}_1 = (0,0)^T$ a $\mathbf{A}\mathbf{x}_2 = (1,2)^T$ se stejnými levými stranami. Hledaná matice $\mathbf{X}$ potom bude tvaru $\mathbf{X} = (\mathbf{x}_1, \mathbf{x}_2)$. Podobně jako v algoritmu pro výpočet inverzní matice můžeme soustavy zapsat do jedné matice s oběma vektory pravých stran vpravo a levé strany upravíme:

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

Nyní snadno obvyklým způsobem dopočítáme, že první soustavu řeší právě vektory $c \cdot (4,1)^T$ pro všechna $c \in \mathbf{Z}_7$ druhou soustavu řeší právě vektory $(2,0)^T + d \cdot (4,1)^T$ pro všechna $d \in \mathbf{Z}_7$. Tudíž $\mathbf{X}$ řešení maticové rovnice $\mathbf{A} \cdot \mathbf{X} = \mathbf{B}$, právě když $\mathbf{X}$ leží v množině $\{(\mathbf{x}_1, \mathbf{x}_2) | \exists c, d \in \mathbf{Z}_7 : \mathbf{x}_1 = c \cdot \begin{pmatrix} 4 \\ 1 \end{pmatrix}, \mathbf{x}_2 = \begin{pmatrix} 2 \\ 0 \end{pmatrix} d \cdot \begin{pmatrix} 4 \\ 1 \end{pmatrix}\} =$

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

□

**4.10.** 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 $\mathbf{Z}_7$,

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

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

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 $a \in \mathbf{Q} \setminus \{1\}$ 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 $a \in \mathbf{Z}_5 \setminus \{0\}$:

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

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

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

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

**4.11.** 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 $\binom{k}{r} + \binom{k}{r-1} = \binom{k+1}{r}$. □

*20.11.*

**4.12.** 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 $\mathbf{R}$,

(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 $\mathbf{R}$,

(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 $\mathbf{Z}_{13}$.

(a) Použijeme vzorečku odvozeného v úloze 4.11:

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

(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 $\mathbf{Z}_p$ 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 $\lambda \in \mathbf{Z}_{13} \setminus \{0\}$), dostáváme díky 4.11

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

□

**Další úlohy**

(1) Najděte největší společný dělitel a Bezoutovy koeficienty čísel
   (a) 972 a 1122,
   (b) 42589 a 13548,
   (c) $2^{22} - 1$ a $2^{14} - 1$,
   (d) $3^{1000} - 1$ a $3^{999} - 1$,
   (e) $3^{1000} + 1$ a $3^{999} + 1$.

(2) Spočítejte aspoň jedno řešení konruence
   (a) $63x \equiv 1 \pmod{80}$,
   (b) $63x \equiv 5 \pmod{80}$,
   (c) $63x \equiv 9 \pmod{81}$,
   (d) $64x \equiv 3 \pmod{81}$.

(3) Najděte pro každé celé $n$ (všechna) řešení konruence $857x \equiv n \pmod{1021}$

(4) Najděte všechna reálná řešení soustavy rovnic:

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

(b)
$$\begin{array}{rcrcrcrcl} x & + & y & + & z & + & u & = & 3 \\ x & + & 2y & + & 3z & + & 4u & = & 0 \\ x & + & 4y & & & & & = & 0 \end{array}$$

(5) Buď $T$ těleso $\cdot$ a nechť $a, b \in T$. Jestliže $a \cdot a = b \cdot b$, dokažte z axiomatiky tělesa, že nutně $a = b$ nebo $a = -b$.

(6) Spočítejte v tělese $\mathbf{Z}_{83}$ hodnoty $15^{-1}$ a $(3^{-1} + 6 \cdot 53^{-1})^{-1}$.

(7) Vyřešte v tělese $\mathbf{Z}_{97}$ rovnici $7 \cdot x + 3 = 51^{-1} + 17$.

(8) Najděte nad tělesy $\mathbf{Z}_5$ a $\mathbf{Z}_7$ aspoň všechna soustavy rovnic:
$$\begin{array}{rcrcrcrcl} x & + & y & + & z & + & u & = & 3 \\ x & + & 2y & + & 3z & + & 4u & = & 0 \\ x & + & 4y & & & & & = & 0 \end{array}$$

(9) Existuje-li, najděte nad tělesy $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{Z}_3$, $\mathbf{Z}_5$ a $\mathbf{Z}_7$ všechna rešení soustavy rovnic:
$$\begin{array}{rcrcrcl} 2x & - & y & + & 2z & = & 1 \\ x & + & y & - & z & = & 1 \end{array}$$

(10) Vyřešte v tělese $\mathbf{Z}_7$ rovnici $5 \cdot x + 3 = 4^{-1} + 4$.

(11) Najděte nad tělesy $\mathbf{R}$, $\mathbf{Z}_5$ a $\mathbf{Z}_7$ všechna řešení homogenní soustavy rovnic s maticí $\begin{pmatrix} 2 & 0 & 1 \\ 2 & 1 & 0 \\ 3 & 3 & 1 \end{pmatrix}$.

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

(13) Uvažujme matice $\mathbf{A} = \begin{pmatrix} 1 & 2 & 2 \\ 3 & 1 & 4 \end{pmatrix}$ a $\mathbf{B} = \begin{pmatrix} 4 & 2 & 3 & 1 \\ 1 & 4 & 0 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$ nad tělesy $T$: $\mathbf{Q}$, $\mathbf{Z}_5$, $\mathbf{Z}_7$, $\mathbf{Z}_{11}$. Pro každé těleso uvažujme zobrazení $\varphi_A : T^3 \to T^2$, $\psi_A : T^2 \to T^3$, $\varphi_B : T^4 \to T^3$, $\psi_B : T^3 \to T^4$ dané předpisy $\varphi_A(\mathbf{v}) = \mathbf{A}\mathbf{v}$, $\psi_A(\mathbf{v}) = \mathbf{A}^T\mathbf{v}$, $\varphi_B(\mathbf{v}) = \mathbf{B}\mathbf{v}$, $\psi_B(\mathbf{v}) = \mathbf{B}^T\mathbf{v}$.

(a) Rozhodněte, která ze zobrazení $\varphi_A$, $\psi_A$, $\varphi_B$, $\psi_B$, $\varphi_A\varphi_B$, $\psi_B\psi_A$ jsou prostá.

(b) Rozhodněte, která ze zobrazení $\varphi_A$, $\psi_A$, $\varphi_B$, $\psi_B$, $\varphi_A\varphi_B$, $\psi_B\psi_A$ jsou na.

(c) Najděte u zobrazení $\varphi_A$, $\psi_A$, $\varphi_B$, $\psi_B$, $\varphi_A\varphi_B$, $\psi_B\psi_A$ všechny vektory, které se zobrazí na nulový vektor.

(14) Pro komplexní matice $\mathbf{A} = \begin{pmatrix} 1+i & 3-i & 1 \\ 2-i & -i & 1+i \\ 1 & 1+2i & 1-2i \end{pmatrix}$, $\mathbf{B} = \begin{pmatrix} 1-3i & 2+3i & 1 \\ 2+i & 1+2i & i \end{pmatrix}$ a $\mathbf{C} = \begin{pmatrix} 1-4i & 3 & 0 \\ -i & i & 1 \end{pmatrix}$

(a) spočítejte $\mathbf{B} + \mathbf{C}$, $\mathbf{B}^T + \mathbf{A} \cdot \mathbf{C}^T$, $\mathbf{A} \cdot \mathbf{B}^T$, $\mathbf{B} \cdot \mathbf{A}$, $\mathbf{B}^T \cdot \mathbf{C}$ a $\mathbf{B} \cdot \mathbf{C}^T$,

(b) existuje-li, najděte matici inverzní k matici $\mathbf{A}$ a k matici $\mathbf{B} \cdot \mathbf{C}^T$,

(b) dokažte, že matice $\mathbf{B}^T \cdot \mathbf{C}$ není regulární,

(d) existuje-li, najděte matici $\mathbf{X}$ splňující rovnost $\mathbf{X} \cdot \mathbf{A} = \mathbf{C}$.

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

(16) Tam, kde je to možné, najděte inverzní matice k maticím z předchozí úlohy.

(17) 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 $\mathbf{R}$, $\mathbf{Z}_5$ a $\mathbf{Z}_7$.

(18) Existují-li najděte inverzní matice k maticím $\begin{pmatrix} 11 & 12 \\ 13 & 14 \end{pmatrix}$, $\begin{pmatrix} 8 & 9 & 9 \\ 9 & 8 & 9 \\ 9 & 9 & 8 \end{pmatrix}$ a $\begin{pmatrix} 15 & 16 & 3 \\ 9 & 0 & 5 \\ 12 & 0 & 15 \end{pmatrix}$ nad tělesy $\mathbf{Z}_{17}$, $\mathbf{Z}_{19}$, $\mathbf{Z}_{53}$ a $\mathbf{Z}_{103}$.

(19) Rozhodněte, pro která $a \in \mathbf{C}$ je matice $\mathbf{A}_a$ regulární, a pro tato $a$ spočítejte matici $\mathbf{A}_a^{-1}$:

(a) $\mathbf{A}_a = \begin{pmatrix} a+1 & a+2 \\ a+3 & a+4 \end{pmatrix}$,

(b) $\mathbf{A}_a = \begin{pmatrix} a-1 & 3 \\ a+1 & 2a \end{pmatrix}$,

(c) $\mathbf{A}_a = \begin{pmatrix} a & 1 & 1 \\ a & a & 0 \\ a & 0 & 0 \end{pmatrix}$,

(d) $\mathbf{A}_a = \begin{pmatrix} a-1 & a & a+2 \\ 3a & 1 & a-1 \\ a+1 & a-1 & 0 \end{pmatrix}$,

(20) Rozhodněte, pro která $a \in \mathbf{Z}_7$ je matice $\mathbf{A}_a$ regulární, a pro tato $a$ spočítejte matici $\mathbf{A}_a^{-1}$:

(a) $\mathbf{A}_a = \begin{pmatrix} a+1 & a+2 \\ a+3 & a+4 \end{pmatrix}$, (b) $\mathbf{A}_a = \begin{pmatrix} 2a & 3a \\ 4a & a+2 \end{pmatrix}$, (c) $\mathbf{A}_a = \begin{pmatrix} a & 1 & 3 \\ a & 1 & a \\ 2a & 3a & 6 \end{pmatrix}$,

(d) $\mathbf{A}_a = \begin{pmatrix} a+1 & a & a \\ a & a+2 & a \\ a & a & a+3 \end{pmatrix}$, (e) $\mathbf{A}_a = \begin{pmatrix} a+1 & a & a & a \\ a & a+1 & a & a \\ a & a & a+1 & a \\ a & a & a & a+1 \end{pmatrix}$.

(21) Rozhodněte, pro která $a, b, c \in \mathbf{R}$ je matice $\mathbf{A}_{a,b,c}$ regulární, a pro tato $a$ spočítejte matici $\mathbf{A}_{a,b,c}^{-1}$:

(a) $\mathbf{A}_{a,b,c} = \begin{pmatrix} a & b \\ c & a \end{pmatrix}$, (b) $\mathbf{A}_{a,b,c} = \begin{pmatrix} a+b & 1 \\ c & b \end{pmatrix}$, (c) $\mathbf{A}_{a,b,c} = \begin{pmatrix} a & b & c \\ c & a & b \\ 1 & 1 & 1 \end{pmatrix}$.