1. Počítání v tělesech

Uvažujme množinu všech racionálních čísel $\mathbf{Q}$ spolu s obvyklými operacemi $+$ a $\cdot$ a všimněme si „běžných" vlastností obou operací (tj. takových, jichž jsme bez rozmýšlení ochotni a schopni používat). Nejprve zaznamenejme takové vlastnosti sčítání:

1. $\forall a, b, c \in \mathbf{Q}$ platí rovnost $(a + b) + c = a + (b + c)$ (této vlastnosti operace se obvykle říká *asociativita*),
2. $\forall a, b \in \mathbf{Q}$ platí, že $a + b = b + a$ (této vlastnosti $+$ říkáme *komutativita*),
3. $\forall a \in \mathbf{Q}$ platí, že $a + 0 = a$ (tedy 0 je tzv. *neutrální prvek* operace $+$),
4. $\forall a \in \mathbf{Q}$ existuje racionální číslo, které označujeme $-a$, pro něž $a + (-a) = 0$ (tedy $-a$ je *opačný prvek* k a).

Velmi podobný soubor vlastností splňuje i násobení:

5. $\forall a, b, c \in \mathbf{Q}$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (*asociativita*),
6. $\forall a, b \in \mathbf{Q}$: $a \cdot b = b \cdot a$ (*komutativita*),
7. $\forall a \in \mathbf{Q}$ platí, že $a \cdot 1 = a$ (tedy 1 je *neutrální prvek* operace $\cdot$),
8. $\forall a \in \mathbf{Q} \setminus \{0\}$ existuje racionální číslo, které označujeme a^{-1}, pro něž $a \cdot a^{-1} = 1$ (a^{-1} je tzv. *inverzní prvek* k a).

Doposud jsme neuvedli žádnou vlastnost, která by uvažované operace nějak svazovala. Uvědomme si, že velmi silný požadavek na „spolupráci" $+$ a $\cdot$ na racionálních číslech vyjadřuje pravidlo *distributivity*:

9. $\forall a, b, c \in \mathbf{Q}$: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Není těžké nahlédnout, že jsme právě shrnuli důležité vlastnosti uvažovaných operací jako takových a že mnohé další samozřejmé vlastnosti lze z *axiomů* 1.-9. odvodit. Například fakt, že $-(a \cdot b) = (-a) \cdot b$, plyne z axiomů 9. a 4. a z faktu $0 \cdot b = 0$ (konkrétně $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$) a dokonce i fakt, že $0 \cdot b = 0$ můžeme, jak záhy ukážeme z axiomatiky odvodit. To samozřejmě v případě racionálních čísel, s nimiž jsme zvyklí počítat, na nic nepotřebujeme, ale může to být velmi užitečné v okamžiku, kdy se zamyslíme, zda stejný (či podobný) soubor vlastností nesplňují i jiné páry operací (a tím ani nevylučujeme ani nezaručujeme, že budou mít stejný zápis) na jiných množinách a zda právě vyjmenované vlastnosti nepostačují k tomu, abychom uměli zodpovědět otázky, které si záhy v rámci kurzu lineární algebry položíme.

Už ve chvíli, kdy jsme sestavovali soupis vlastností 1.– 9., jsme si mohli uvědomit, že jsou samozřejmě splněny pro sčítání a násobení na reálných či komplexních číslech (a že například sčítání a násobení na celých číslech splňuje všechny uvedené axiomy s výjimkou axiomu 8.). Sepišme si tedy tyto vlastnosti ještě jednou, ale uvažujme je pro nějakou obecnou množinu $\mathbf{T}$ s dvojicí binárních operací $+$ a $\cdot$:

1. $\forall a, b, c \in \mathbf{T}$: $(a + b) + c = a + (b + c)$,
2. $\forall a, b \in \mathbf{T}$: $a + b = b + a$,
3. existuje takový prvek $0 \in \mathbf{T}$, že $\forall a \in \mathbf{T}$ platí rovnost $a + 0 = a$,
4. $\forall a \in \mathbf{T}$ existuje $-a \in \mathbf{T}$, pro které $a + (-a) = 0$,
5. $\forall a, b, c \in \mathbf{T}$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
6. $\forall a, b \in \mathbf{T}$: $a \cdot b = b \cdot a$,
7. existuje takový prvek $1 \in \mathbf{T}$, že $\forall a \in \mathbf{T}$ platí rovnost $a \cdot 1 = a$,

8. $\forall a \in \mathbf{T} \setminus \{0\}$ existuje $a^{-1} \in \mathbf{T}$, pro které $a \cdot a^{-1} = 1$ (a^{-1} je tzv. *inverzní prvek* k).
9. $\forall a, b, c \in \mathbf{T}$: $a \cdot (b + c) = a \cdot b + a \cdot c$.

V novém souboru axiomů jsme do 3. a 7. axiomu přidali formulaci „existuje takový prvek", která byla v případě racionálních, reálných či komplexních čísel zbytečná (0 a 1 tam označují zcela konkrétní čísla a my jen zaznamenali jejich charakteristické vlastnosti), ale ve chvíli, kdy nemáme k dispozici nic víc než dvě operace na abstraktní množině $\mathbf{T}$, je nezbytná. Rovněž si všimněme, že jsme v nové axiomatice převzali značení obvyklé u zmiňovaných konkrétních číselných struktur (kromě symbolů pro neutrální prvky také $-$ a $^{-1}$), které v obecné situaci nemá konkrétní obsah (je okamžitě srozumitelné, jaké konkrétní racionální čísl máme na mysli, napíšemeli -5 nebo $\frac{2}{3}^{-1}$, ovšem v jiných konkrétních příkladech struktur splňujících danou axiomatiku budou symboly $-$ a $^{-1}$ teprve výzvou k následnému výpočtu).

Než shrneme naší axiomatiku pod pojem těleso, ujasněme si, co by znamenalo, kdyby oba výjimečné prvky (tj. 0 a 1) splývaly (tj. $0 = 1$). Potom by pro libovolné $a \in \mathbf{T}$ platilo $a = a \cdot 1 = a \cdot 0 = 0$, tedy množina $\mathbf{T}$ by byla pouze jednoprvková. Pro jednoprvkovou množinu a jednoznačně určené (a zjevně totožné) operace $+$ a $\cdot$ by všechny axiomy sice platily, ale počítání by v takovém případě nebylo vůbec zajímavé a při budování vektorových prostorů by připuštění jednoprvkových těles přinášelo potíže. Proto přidáme k axiomatice požadavek, aby množina $\mathbf{T}$ byla aspoň dvouprvková (nebo ekvivalentně, aby $0 \neq 1$).

1.1. Předpokládejme, že pro operace $+$ a $\cdot$ na množině T platí axiomy 1.–9. Dokažte, že pro každé $a, b \in T$ platí:

(a) $0 \cdot a = 0$,
(b) $(-1) \cdot a = -a$,
(c) jestliže $a \neq 0$ a $b \neq 0$, potom $a \cdot b \neq 0$.

(a) Nejprve uvážíme, že podle 3. axiomu máme $0 + 0 = 0$, podle 4. axiomu $0 \cdot a + (-(0 \cdot a)) = 0$, proto

$$0 = 0 \cdot a + (-(0 \cdot a)) = (0 + 0) \cdot a + (-(0 \cdot a)).$$

Nyní upravíme výraz $(0 + 0) \cdot a$ pomocí axiomu 9. a poté použijeme nejprve axiom 1 a po něm opět axiomy 4 a 3 a dostaneme

$$0 = (0 + 0) \cdot a + (-(0 \cdot a)) = 0 \cdot a + 0 \cdot a + (-(0 \cdot a)) = 0 \cdot a + 0 = 0 \cdot a.$$

(b) Stačí využít axiom 4, distribotivitu (tj. axiom 9) a právě dokázané pozorování (a), abychom dostali

$$0 = (0) \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a.$$

Protože $1 \cdot a = a$ podle 7. axiomu, vidíme, že $(-1) \cdot a$ je opravdu opačný prvek k prvku a.

(c) Budeme dokazovat obměnu tvrzení. Předpokládejme, že $a \cdot b = 0$ a $a \neq 0$. Potom existuje díky 8. axiomu inverzní prvek a^{-1}. Díky axiomu 7, 8 a 5 tedy máme

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b).$$

Nyní stačí použít předpoklad $a \cdot b = 0$ a tvrzení (a), abychom dostali

$$b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0.$$

□

Nyní ukážeme, že dobře známé struktury $\mathbf{Q}$, $\mathbf{R}$ či $\mathbf{C}$ nejsou zdaleka jediné, které splňují axiomatiku tělesa. Pomineme na tomto místě velké množství příkladů těles, která bychom mohli najít jako podtělesa reálných čísel a zaměříme se na tělesa s konečným počtem prvků.

6./7.10.

Buď v následujícím n přirozené číslo a položme $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$. Nyní definujme na $\mathbf{Z}_n$ operace $+_n$ 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.

1.2. Ověřte, že pro všechna celá a, b a libovolné přirozené n platí, že $((a)\mathrm{mod}n + (b)\mathrm{mod}n)\mathrm{mod}n = (a+b)\mathrm{mod}n$ a $((a)\mathrm{mod}n \cdot (b)\mathrm{mod}n)\mathrm{mod}n = (a \cdot b)\mathrm{mod}n$.

Zvolme libovolě celá a, b a přirozené n. Předně si rozmyslíme význam zbytku po celočíselném dělení, tedy, že existují (jednoznačně určená) celá q a r, pro něž $(a)\mathrm{mod}n + qn = a$ a $(b)\mathrm{mod}n + rn = b$. Navíc připomeňme, že $0 \leq (a)\mathrm{mod}n < n$ a $0 \leq (b)\mathrm{mod}n < n$. Nyní počítejme: $(a+b)\mathrm{mod}n = ((a)\mathrm{mod}n + qn + (b)\mathrm{mod}n + rn)\mathrm{mod}n = ((a)\mathrm{mod}n + (b)\mathrm{mod}n + (q+r)n)\mathrm{mod}n = ((a)\mathrm{mod}n + (b)\mathrm{mod}n)\mathrm{mod}n$. □

1.3. Dokažte, že $\mathbf{Z}_n$ spolu s operacemi $+_n$ a $\cdot_n$ splňuje axiomy 1.– 7. a 9.

Platnost axiomů 2.,3.,6.,7. plyne okamžitě z definice operací a odpovídající vlastnosti pro celá čísla, axiomy 1., 5. a 9. platí díky pozorování z 1.2. Konečně $-0 = 0$ a $-a = n - a$ pro všechna $a \in \mathbf{Z}_n \setminus \{0\}$, protože $(a + n - a)\mathrm{mod}n = (n)\mathrm{mod}n = 0$. □

1.4. Najděte inverzní prvky pro všechny nenulové prvky tělesa $\mathbf{Z}_5$.

V daném případě můžeme postupovat zkusmo. Snadno zjistíme, že $1^{-1} = 1$ (to platí ostatně v každém tělese), z pozorování, že $2 \cdot_5 3 = 1$, plyne, že $2^{-1} = 3$ i že $3^{-1} = 2$, a konečně $4^{-1} = 4$, protože $4 \cdot_5 4 = 1$. □

1.5. 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 axiomy 1.– 7. a 9, zřejmě tedy nemůže platit 8. axiom. Protože víme, že v každém tělese musí podle 1.1 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 $a \cdot b = (n)\mathrm{mod}n = 0$. □

Nechť $a_0 \geq a_1$ jsou dvě přirozená čísla. Připomeňme **Eukleidův algoritmus** hledání největšího společného dělitele (NSD) čísel a_0 a a_1:

Známe-li a_{i-1} a a_i spočteme $a_{i+1} = (a_{i-1})\mathrm{mod}\, a_i$. 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 $a_n = \mathrm{NSD}(a_0, a_1)$.

1.6. Najděte pomocí Euklidova algoritmu taková celá čísla x a y, aby $30x + 101y = 1$.

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:

$a_0 = 101$,

$a_1 = 30$,

$a_2 = 101 - 3 \cdot 30 = 11$,
$a_3 = 30 - 2 \cdot 11 = 8$,
$a_4 = 11 - 8 = 3$,
$a_5 = 8 - 2 \cdot 3 = 2$,
$a_6 = 3 - 2 = 1 = \mathrm{NSD}(101, 30)$.

Vidíme, že každé a_{i+1} je celočíselnou lineární kombinací prvků a_i a a_{i-1}, budeme-li postupně dosazovat předchozí vyjádření do následujících výrazů, dostaneme každé a_{i+1} jako celočíselnou lineární kombinací prvků a_0 a a_1:

$a_2 = 11 = 101 - 3 \cdot 30$,
$a_3 = 8 = 30 - 2 \cdot 11 = 30 - 2 \cdot (101 - 3 \cdot 30) = 7 \cdot 30 - 2 \cdot 101$,
$a_4 = 3 = 11 - 8 = (101 - 3 \cdot 30) - (7 \cdot 30 - 2 \cdot 101) = 3 \cdot 101 - 10 \cdot 30$,
$a_5 = 2 = 8 - 2 \cdot 3 = (7 \cdot 30 - 2 \cdot 101) - 2 \cdot (3 \cdot 101 - 10 \cdot 30) = 27 \cdot 30 - 8 \cdot 101$,
$a_6 = 1 = 3 - 2 = (3 \cdot 101 - 10 \cdot 30) - (27 \cdot 30 - 8 \cdot 101) = 11 \cdot 101 - 37 \cdot 30$.

Zjistili jsme, že $x = -37$ a $y = 11$. □

1.7. 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 $30x + 101y = 1$. Podobnou úlohu už jsme řešili v předchozím příkladu, 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 1.6.

14./20.10.

1.8. Najděte v tělese $\mathbf{Z}_{101}$ 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 $(2 \cdot \frac{p+1}{2}) \mathrm{mod} p = (p+1) \mathrm{mod} p = 1$, 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 $x = 20^{-1} \cdot_{101} 7 = 96 \cdot_{101} 7 = 66$. □

1.9. Dokažte, pomocí Euklidova algoritmu, že $\mathbf{Z}_p$ spolu s operacemi $+_p$ a $\cdot_p$ splňuje axiom 8.

Uvažujeme stejným způsobem jako v předchozích úlohách. Zvolme libovolně nenulové $a \in \mathbf{Z}_p$. Protože p je prvočíslo, jsou a a p nesoudělná, tedy pomocí Euklidova algoritmu lze najít celá x a y, pro něž $ax + py = \mathrm{NSD}(a, p) = 1$. Nyní stačí vzít $a^{-1} = (x) \mathrm{mod} p$. □

Nadále budeme sčítání a násobení v tělese $\mathbf{Z}_p$ psát bez indexu $_p$ (tj. jen $+$ a $\cdot$).

1.10. 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 $\mathbf{Z}_7$:

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

□

1.11. Spočítejte v tělese komplexních čísel $\mathbf{C}$ hodnotu výrazů $(3+i)^{-1}$ a $(1-2i)^{-1} \cdot (2+3i)$.

Obvyklým způsobem rozšíříme zlomky komplexně sdruženou hodnotou a dostaneme

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

a

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

□

1.12. Najděte (nějaká) reálná rešení soustavy rovnic:

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

Nejprve si soustavu zapíšeme do matice a poté ji pomocí přičtení vhodného násobku jedné rovnice k rovnici druhé upravíme (na střední škole se tento způsob upravování obvykle nazývá „sčítací metoda"):

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

Druhý řádek 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 $\left(\begin{array}{ccc|c} -2 & 1 & 2 & 2 \end{array}\right)$). 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 $(x, y, z) = (-\frac{3}{5}, \frac{4}{5}, 0)$. Podobně jsme jiné řešení mohli dostat po volbě $z = 1$ a jednoznačném dopočítání $y = x = 0$. □

Na tomto místě si uvědomíme 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. Nyní bychom mohli najít směr této přímky a najít tak dokonce všechna reálná řešení. Tento úkol ovšem vyřešíme až později negeometricky pro všechna tělesa.

1.13. Najděte (nějaká) racionální rešení soustavy rovnic z úlohy 1.12.

Stačí si rozmyslet, že z množiny řešení předchozí úlohy musíme vybrat ta, která jsou ve všech složkách racionální. Zřejmě mají řešení $(-\frac{3}{5}, \frac{4}{5}, 0)$ $(0, 0, 1)$ všechny složky racionální, tedy jde o hledaná racionální řešení. □

1.14. Najděte rešení soustavy rovnic z úlohy 1.12 nad tělesem $\mathbf{Z}_5$.

Budeme postupovat stejným formalizmem jako v úloze 1.12. Snadno si uvědomíme, že stačí postupovat obdobnými úpravami, kterými docílíme maticového zápisu v požadovaném („odstupňovaném" či „schodišťovém") tvaru:

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

všimněme si, že k témuž výsledku dospějeme, když finální matici z 1.12 jednoduše ve všech složkách upravíme modulo 55:

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

Nyní nejprve opět najdeme jedno řešení nehomogenní soustavy. Z druhé rovnice nutně plyne, že $z = 1$ a dosadíme-li tentokrát $y = 0$ dopočítáme z první rovnice $x = 0$. Tedy i řešení $(0, 0, 1)$ úlohy 1.12 bvyhovuje i nyní (v obecném případě bychom ho museli opět upravit modulo 5, tentokrát taková úprava ovšem řešení nezmění). Naopak racionální (a reálné) řešení $(-\frac{3}{5}, \frac{4}{5}, 0)$ nelze „přetlumočit" do tělesa $\mathbf{Z}_5$, protože zde nelze vydělit číslem $5 \mathrm{mod} 5 = 0$ (tj. přesněji řečeno najít k němu inverzní prvek). □

1.15. Najděte postupně nad tělesy racionálních čísel, $\mathbf{Z}_5$, $\mathbf{Z}_7$ a $\mathbf{Z}_{11}$ řešení soustavy rovnic:
$$\begin{array}{rcrcl} x & + & 2y & = & 3 \\ 3x & + & 2y & = & 2 \end{array}$$

Nejprve otázku pomocí maticového zápisu vyřešíme nad tělesem $\mathbf{Q}$, tentokrát si navíc uvědomíme, že maticově umíme zapsat nalezená řešení:

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

Zjistili jsme, že $(x, y) = (-\frac{1}{2}, \frac{7}{4})$ je jediné racionální řešení soustavy.

Nyní podobně jako v předchozí úloze uvážíme, že jsme při úpravách nad $\mathbf{Q}$ nikde nedělili 5,7 ani 11 a proto stačí matici $\left(\begin{array}{cc|c} 1 & 0 & -\frac{1}{2} \\ 0 & 1 & \frac{7}{4} \end{array}\right)$ jen upravit modulo příslušné prvočíslo.

Konkrétně nad tělesem $\mathbf{Z}_5$ je $2^{-1} = 3$, $4^{-1} = 4$, proto $(-\frac{1}{2})\mathrm{mod}5 = (-1 \cdot 2^{-1})\mathrm{mod}5 = (4 \cdot 3)\mathrm{mod}5 = 2$ a $(\frac{7}{4})\mathrm{mod}5 = (7 \cdot 4^{-1})\mathrm{mod}5 = (2 \cdot 4)\mathrm{mod}5 = 3$. Maticově zapsáno nad $\mathbf{Z}_5$ to znamená, že

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

$(x, y) = (2, 3)$ je jediné řešení soustavy nad tělesem $\mathbf{Z}_5$. Podobně uvážíme nad $\mathbf{Z}_7$, že $-1 \cdot 2^{-1} = 6 \cdot 4 = 3$ a $7 \cdot 4^{-1} = 0$, tedy nad tímto tělesem

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

a $(x, y) = (3, 0)$. Konečně nad tělesem $\mathbf{Z}_{11}$ stejnou úvahou dostáváme $-1 \cdot 2^{-1} = 10 \cdot 6 = 5$ a $7 \cdot 4^{-1} = 7 \cdot 3 = 10$, a proto nad tělesem $\mathbf{Z}_{11}$ dostáváme jednoznačné řešení $(x, y) = (5, 10)$, jemuž odpovídá maticový zápis

$$\left(\begin{array}{cc|c} 1 & 2 & 3 \\ 3 & 2 & 2 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 0 & 5 \\ 0 & 1 & 10 \end{array}\right).$$

□

Další úlohy

(1) Dokažte, že opačný i inverzní prvek jsou ke každému prvku v tělese určeny jednoznačně.
(2) Dokažte, že neutrální prvky obou operací v tělese jsou určeny jednoznačně.
(3) Dokažte, že pro všechny prvky a, b obecného tělesa platí $-(a \cdot b) = -a \cdot b = a \cdot (-b)$, $-(a)^{-1} = (-a)^{-1}$, $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ a $(-a)\cdot(-b) = a \cdot b$.
(4) 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 $a = -b$.
(5) Spočítejte v tělese $\mathbf{Z}_{83}$ hodnoty 15^{-1} a $(3^{-1} + 6 \cdot 53^{-1})^{-1}$.
(6) Vyřešte v tělese $\mathbf{Z}_{97}$ rovnici $7 \cdot x + 3 = 51^{-1} + 17$.
(7) Najděte nad tělesy $\mathbf{R}$, $\mathbf{Q}$, $\mathbf{C}$, $\mathbf{Z}_3$, $\mathbf{Z}_5$ a $\mathbf{Z}_7$ rešení soustavy rovnic:
$$\begin{array}{rcrcrcl} 2x & - & y & + & 2z & = & 1 \\ x & + & y & - & z & = & 1 \end{array}$$
(8) Najděte všechna komplexní řešení soustavy rovnic:
$$\begin{array}{rcrcrcl} ix & - & 2y & + & z & = & 1-i \\ x & + & (1+i)y & - & (2+3i)z & = & i \end{array}$$
(9) Najděte nad tělesy $\mathbf{Z}_5$ a $\mathbf{Z}_7$ aspoň tři řešení soustavy rovnic:
$$\begin{array}{rcrcrcrcl} x & + & y & + & z & + & u & = & 3 \\ x & + & 2y & + & 3z & + & 4u & = & 0 \\ x & + & 4y & & & & & = & 0 \end{array}$$