6. Konečná tělesa $\mathbb{Z}_p$

Cv. 6.1 Vyjádřete jako prvky daného tělesa výrazy:

(a) $((2^{-1}+1)4)^{-1}$ a $4/3$ v tělese $\mathbb{Z}_5$,

(b) $6+7$, -7, $6\cdot 7$, 7^{-1} a $6/7$ v tělese $\mathbb{Z}_{11}$.

Řešení:

(a) Těleso $\mathbb{Z}_5$ je definováno jako množina všech zbytků v $\mathbb{Z}$ po dělení 5 spolu s operacemi součtu a součinu modulo 5. Pro názornost uvádíme tabulky pro obě operace.

$\mathbb{Z}_5,+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

,

$\mathbb{Z}_5,\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Podle definice tělesa má množina $\mathbb{Z}_5 \setminus \{0\} = \{1,2,3,4\}$ se součinem modulo 5 tvořit Abelovu grupu; zde je to takzvaná multiplikativní grupa modulo 5. V tabulce můžeme některé vlastnosti grupy snadno nahlédnout, například komutativitu nebo existenci neutrálního a inverzního prvku.

Nyní můžeme vyhodnotit zadané výrazy v $\mathbb{Z}_5$, kde při výpočtu nalezneme multiplikativní inverzi k libovolnému $a \in \mathbb{Z}_5 \setminus \{0\}$ v tabulce tak, že v řádku s a najdeme hodnotu 1 a index b odpovídajícího sloupce musí být hledaná multiplikativní inverze a^{-1}, protože $a \cdot b = 1$ v $\mathbb{Z}_5$. Dostáváme:

$$((2^{-1}+1)4)^{-1} = ((3+1)4)^{-1} = (4\cdot 4)^{-1} = (1)^{-1} = 1 \text{ v } \mathbb{Z}_5$$

a

$$4/3 = 4\cdot 3^{-1} = 4\cdot 2 = 3 \text{ v } \mathbb{Z}_5.$$

(b) Postupujeme podobně jako pro $\mathbb{Z}_5$, ale nebudeme konstruovat celou tabulku pro součin v $\mathbb{Z}_{11}$. Dostáváme:

$$\begin{aligned} 6+7 &= 6+7 \pmod{11} = 13 \pmod{11} = 2 \text{ v } \mathbb{Z}_{11},\\ -7 &= 11-7 \pmod{11} = 4 \text{ v } \mathbb{Z}_{11}.\\ 6\cdot 7 &= 6\cdot 7 \pmod{11} = 42 \pmod{11} = 9 \text{ v } \mathbb{Z}_{11}. \end{aligned}$$

Při hledání multiplikativní inverze k prvku 7 můžeme postupovat jako při výpočtu řádku odpovídajícího 7 v tabulce pro součin v $\mathbb{Z}_{11}$. Výpočet zasta-

víme v momentě, kdy uvidíme na pravé straně číslo 1:

$$\begin{aligned} 7 \cdot 1 &= 7, \\ 7 \cdot 2 &= 3, \\ 7 \cdot 3 &= 10, \\ 7 \cdot 4 &= 6, \\ 7 \cdot 5 &= 2, \\ 7 \cdot 6 &= 9, \\ 7 \cdot 7 &= 5, \\ 7 \cdot 8 &= 1. \end{aligned}$$

Vidíme, že

$$7^{-1} = 8 \text{ v } \mathbb{Z}_{11}.$$

Tuto hodnotu využijeme i při posledním výpočtu:

$$6/7 = 6 \cdot 7^{-1} = 6 \cdot 8 = 48 \,(\mathrm{mod}\ 11) = 4 \text{ v } \mathbb{Z}_{11}.$$

Cv. 6.2 Nad $\mathbb{Z}_5$ najděte množinu všech řešení soustavy rovnic

$$\begin{aligned} 3x + 2y + z &= 1, \\ 4x + y + 3z &= 3 \end{aligned}$$

a spočítejte její mohutnost.

Řešení:
Postupujeme podobně jako pro soustavy rovnic nad $\mathbb{R}$. Využijeme toho, že eliminovat prvky pod pivotem můžeme přičtením vhodného násobku řádku s pivotem. Přičtením 2-násobku prvního řádku k druhému dostáváme

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

Za volné proměnné zvolíme parametry $y, z \in \mathbb{Z}_5$ a vyjádříme

$$x = 3^{-1}(1 - 2y - z) = 2(1 + 3y + 4z) = 2 + y + 3z.$$

Množina všech řešení dané soustavy je tedy

$$\{(2,0,0)^T + y(1,1,0)^T + z(3,0,1)^T \mid y, z \in \mathbb{Z}_5\}.$$

Máme $25 = 5 \cdot 5$ různých voleb parametrů y a z a mohutnost množiny řešení je tedy 25.

Cv. 6.3 V $\mathbb{Z}_7$ spočítejte mocninu matice A^{100} pro matici $A = \left(\begin{smallmatrix} 3 & 2 \\ 1 & 4 \end{smallmatrix}\right)$.

Řešení:

Nad konečným tělesem musí být posloupnost matic A^i pro $i = 1, \ldots, \infty$ cyklická. Spočtěme několik prvních členů této posloupnosti:

$$\begin{aligned}
A = A^1 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix}, \\
A^2 &= \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \\
A^3 &= \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix}, \\
A^4 &= \begin{pmatrix} 5 & 1 \\ 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \\
A^5 &= \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix}, \\
A^6 &= \begin{pmatrix} 6 & 4 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \\
A^7 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 4 \end{pmatrix} = A.
\end{aligned}$$

Vidíme, že perioda této posloupnost je 6. Hledanou mocninu matice tedy spočítáme jako

$$A^{100} = A^{100 \,(\mathrm{mod}\, 6)} = A^4 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Poznámka. Trochu práce si můžeme ušetřit tím, že si uvědomíme, že druhá mocnina má tvar $A^2 = 4I_2$. Tudíž

$$A^{100} = (A^2)^{50} = (4I_2)^{50} = 4^{50} I_n.$$

Tím jsme maticový problém zredukovali na skalární problém. Z Malé Fermatovy věty víme, že $4^6 = 1$ v $\mathbb{Z}_7$, čili

$$4^{50} I_n = 4^{50 \,(\mathrm{mod}\, 6)} I_n = 4^2 I_n = 2I_n.$$

Cv. 6.4 Spočítejte 20^{3332} v tělese $\mathbb{Z}_{31}$.

Řešení:
Z Malé Fermatovy věty víme, že v tělese $\mathbb{Z}_{31}$ je $20^{30} = 1$. Proto

$$20^{3332} = 20^{3332 \,(\mathrm{mod}\, 30)} = 20^2 = 28.$$