Příklad 1. Pomocí Euklidova algoritmu určete 50^{-1} v tělese $\mathbb{Z}_{113}$.

Řešení. Rozšířeným Euklidovým algoritmem vyjádříme 1 ve tvaru $k \cdot 50 + l \cdot 113$.

$$\begin{aligned}\mathbf{113} &= 2 \cdot \mathbf{50} + \mathbf{13}\\ \mathbf{50} &= 3 \cdot \mathbf{13} + \mathbf{11}\\ \mathbf{13} &= 1 \cdot \mathbf{11} + \mathbf{2}\\ \mathbf{11} &= 5 \cdot \mathbf{2} + \mathbf{1}\end{aligned}$$

Z těchto vztahů postupně dostaneme:

$$\begin{aligned}\mathbf{13} &= \mathbf{113} - 2 \cdot \mathbf{50}\\ \mathbf{11} &= \mathbf{50} - 3 \cdot \mathbf{13} = \mathbf{50} - 3 \cdot (\mathbf{113} - 2 \cdot \mathbf{50}) = -3 \cdot \mathbf{113} + 7 \cdot \mathbf{50}\\ \mathbf{2} &= \mathbf{13} - 1 \cdot \mathbf{11} = (\mathbf{113} - 2 \cdot \mathbf{50}) - (-3 \cdot \mathbf{113} + 7 \cdot \mathbf{50}) = 4 \cdot \mathbf{113} - 9 \cdot \mathbf{50}\\ \mathbf{1} &= \mathbf{11} - 5 \cdot \mathbf{2} = (-3 \cdot \mathbf{113} + 7 \cdot \mathbf{50}) - 5 \cdot (4 \cdot \mathbf{113} - 9 \cdot \mathbf{50}) = -23 \cdot \mathbf{113} + 52 \cdot \mathbf{50}\end{aligned}$$

Ze vztahu $1 = 52 \cdot 50 - 23 \cdot 113$ vyplývá, že inverzní prvek k 50 v tělese $\mathbb{Z}_{113}$ je 52.

Příklad 2. Uvažujme algebru $\mathbb{M} = M(+, -, \cdot)$, kde M je množina všech čtvercových matic typu 2×2 nad celými čísly, $+$ je běžná binární operace sčítání matic, $\cdot$ je běžné násobení a $-$ je běžné (unární) minus. Dokažte, že $\mathbb{M}$ je generována množinou

$$\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}$$

Řešení. Označme $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ a $N = \langle A, B \rangle$. Zřejmě nulová matice patří do N (protože je rovná např. $A + (-A)$). Dále platí

$$\begin{aligned}A + B &= \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \in N,\\ A \cdot B &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \in N,\\ C_{22} &= (A + B) + (-(A \cdot B)) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in N,\\ C_{11} &= (A + B) + (-(B \cdot A)) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in N,\\ C_{12} &= A + (-C_{11}) + (-C_{22}) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in N,\\ C_{21} &= B + (-C_{11}) + (-C_{22}) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in N,\end{aligned}$$

Protože N je uzavřená na sčítání, indukcí snadno ukážeme, že $kC_{11}, kC_{12}, kC_{21}, kC_{22} \in N$ pro libovolné přirozené číslo k. Protože N je uzavřená na unární minus a obsahuje nulovou matici, $kC_{11}, kC_{12}, kC_{21}, kC_{22} \in N$ platí pro libovolné celé číslo k. Nyní pro libovolná celá čísla a, b, c, d máme

$$\left(\begin{array}{cc} a & b \\ c & d \end{array} \right) = aC_{11} + bC_{12} + cC_{21} + dC_{22} \in N,$$

tedy $N = M$.

Příklad 3. Najděte všechny homomorfismy $\mathbb{A} \to \mathbb{B}$, kde $\mathbb{A} = \{a, b, c, d\}(f)$ a $\mathbb{B} = \{0, 1\}(g)$ a f, g jsou unární operace dané předpisy $f(a) = f(b) = c$, $f(c) = f(d) = d$, $g(0) = g(1) = 1$.

Řešení. Zobrazeni $h : \mathbb{A} \to \mathbb{B}$ je podle definice homorfismem právě tehdy, když pro libovolné $x \in \{a, b, c, d\}$ platí

$$h(f(x)) = g(h(x)).$$

Vzhledem k tomu, jak je definována operace g, pravá strana je pro libovolné x rovná 1. Takže aby h byl homomorfismus, je nutné a stačí, aby

$$h(f(a)) = 1, \quad h(f(b)) = 1, \quad h(f(c)) = 1, \quad h(f(d)) = 1$$

neboli

$$h(c) = 1, \quad h(c) = 1, \quad h(d) = 1, \quad h(d) = 1$$

Homomorfimy $h : \mathbb{A} \to \mathbb{B}$ jsou právě všechna čtyři zobrazení, pro něž $h(c) = h(d) = 1$.

Příklad 4. Najděte všechny kongruence algebry $\{a, b, c, d\}(*)$, kde

*	a	b	c	d
a	b	a	b	c
b	b	d	b	d
c	b	c	b	a
d	d	d	d	d

Řešení. Ekvivalence $\sim$ je kongruencí dané algebry právě tehdy, když pro libovolné $x \in \{a, b, c, d\}$ platí $a * x \sim b * x$ a $x * a \sim x * b$ (**musí platit obojí!!!**). Běžným způsobem zjistíme (viz řešení domácí úlohy), že jediná kongruence $\sim$, pro kterou $a \sim b$, je triviální kongruence $\sim = \{a, b, c, d\}^2$. Dále zjistíme, že $a \sim d$, $b \sim c$ a $c \sim d$ platí pouze pro triviální kongruenci a že z $b \sim d$ plyne $a \sim c$. Jedinými kandidáty na kongruence jsou, kromě triviálních kongruencí, ekvivalence $|ac|b|d|, |ac|bd|$ (zápis používaný na cvičení). Zkontrolováním podmínky formulované výše zjistíme, že tyto ekvivalence jsou skutečně kongruece.

Algebra má právě čtyři kongruence: $|a|b|c|d|, |ac|b|d|, |ac|bd|, |abcd|$.

Příklad 5. Uvažujme permutaci $\pi = (1\ 3\ 10\ 2)(4\ 5\ 9)(6\ 7) \in S_{11}$.

- (1 bod) Jaký je řád π v grupě S_{11}?
- (2 body) Spočítejte π^{2009}.

Řešení.

- Snadno lze vidět, že řád permutace v grupě S_n je nejmenší společný násobek délek cyklů. V našem případě 12.
- Pokud α, β jsou nezávislé cykly, pak zřejmě $(\alpha\beta)^n = \alpha^n\beta^n$ pro libovolné celé číslo n. Pokud α je cyklus délky k, pak $\alpha^k = id$ z čehož snadno plyne, že $\alpha^n = \alpha^{n \bmod k}$.

$$\pi^{2009} = [(1\ 3\ 10\ 2)(4\ 5\ 9)(6\ 7)]^{2009} = (1\ 3\ 10\ 2)^{2009}(4\ 5\ 9)^{2009}(6\ 7)^{2009} =$$

$$= (1\ 3\ 10\ 2)^{2009 \bmod 4}(4\ 5\ 9)^{2009 \bmod 3}(6\ 7)^{2009 \bmod 2} =$$

$$= (1\ 3\ 10\ 2)^1(4\ 5\ 9)^2(6\ 7)^1 = (1\ 3\ 10\ 2)(4\ 9\ 5)(6\ 7).$$

Chybná odpověď na některou z následujících otázek znamená nepochopení nějaké zásadní definice nebo trvrzení. Proto vám doporučuji si odpovědi důkladně promyslet.

Příklad 6. Pro libovolný homomorfismus $f : \mathbb{A} \to \mathbb{B}$ platí
- **ANO NE** Jádro f je kongruencí algebry $\mathbb{A}$.
- **ANO NE** Obraz f je kongruencí algebry $\mathbb{B}$.
- **ANO NE** Jádro f je podalgebrou algebry $\mathbb{A}$.
- **ANO NE** Jádro f je kongruencí algebry $\mathbb{B}$.
- **ANO NE** Obraz f je podalgebrou algebry $\mathbb{B}$.

Řešení. Jádro zobrazení je ekvivalence na A, obraz zobrazení je podmožina B, takže druhé až čtvrté tvrzení nedávají smysl. První a páté tvrzení platí.

- ANO.
- NE.
- NE.
- NE.
- ANO.

Příklad 7.
$\mathbb{Z}_n$ značí grupu s prvky $0, 1, \dots, n-1$ a binární grupová operace je sčítání modulo n. $\mathbb{Z}_n^*$ značí grupu s těmi prvky $\mathbb{Z}_n$, které jsou nesoudělné s n, a binární grupová operace je násobení modulo n.
- **ANO NE** Řád prvku 4 v grupě $\mathbb{Z}_{11}$ je 3.
- **ANO NE** Řád prvku 4 v grupě $\mathbb{Z}_{12}$ je 3.

- **ANO NE** Libovolný prvek $a \in \mathbb{Z}_{11}^*$, $a \neq 1$ má řád 10.

Řešení.

- NE.
- ANO. Řád prvku grupě $\mathbb{G}$ je nejmenší přirozené číslo n takové, že $a^n = 1$, kde a^n značí $a \cdot a \dots a$ (n-krát), kde $\cdot$ je **binární grupová operace** $\mathbb{G}$ a 1 je **jednotkový prvek v grupě** $\mathbb{G}$.

  Binární grupovou operací v $\mathbb{Z}_{12}$ je sčítání modulo 12 a jednotkovým prvkem je 0! Řád prvku a v grupě $\mathbb{Z}_{12}$ je tedy nejmenší přirozené číslo n takové, že $n \times a = 0$, kde $n \times a$ značí $a + a + \ldots + a$, neboli $n \times a = na \bmod 12$.
- NE. Např. prvek 10 má řád 2. (Ale víme, že řád libovolného prvku dělí 10).

Příklad 8.
Poznámka: cyklická grupa = grupa generovaná jedním prvkem. Značení je jako u předchozího příkladu.
- **ANO NE** Grupa $\mathbb{Z}_4$ je cyklická.
- **ANO NE** Grupa $\mathbb{Z}_4 \times \mathbb{Z}_2$ je cyklická.
- **ANO NE** Grupa $\mathbb{Z}_5 \times \mathbb{Z}_3$ je cyklická.

Řešení.

- ANO. Grupa je generovaná prvkem 1 (nebo také prvkem 3.)
- NE. Každý prvek má řád nejvíce 4.
- ANO. Podle čínské věty o zbytcích je tato grupa izomorfní $\mathbb{Z}_{15}$. Generátorem je např. $(1, 1)$.

Příklad 9.
- **ANO NE** Každá podmnožina komutativní (=abelovské) grupy $\mathbb{G}$ je podgrupou $\mathbb{G}$.
- **ANO NE** Každá podgrupa komutativní grupy $\mathbb{G}$ je normální podgrupou $\mathbb{G}$.
- **ANO NE** Nechť N je normální podgrupou grupy $\mathbb{G}$. Pak pro libovolné $n_1, n_2 \in N, g \in G$ platí $g^{-1}n_1^{-1}n_2g \in N$.

- NE. Např. žádná podmožina neobsahující jednotkový prvek není podgrupou.
- ANO. Pro libovolnou podgrupu N a prvky $n \in N, g \in G$ platí $gng^{-1} = gg^{-1}n = n \in N$, tedy N je normální.

- ANO. Protože N je podgrupa, platí $n_1^{-1}n_2 \in N$. Protože N je normální, platí $g^{-1}n_1^{-1}n_2(g^{-1})^{-1} = g^{-1}n_1^{-1}n_2g \in N$.

Příklad 10.

• **ANO NE** Pro libovolnou permutaci $\pi \in S_{10}$ platí: Pokud $\pi^2 = id$, pak π je transpozice.

• **ANO NE** Pro libovolné permutace $\pi, \rho \in S_{10}$ existuje právě jedno $\nu \in S_{10}$, pro které $\pi \circ \nu = \rho$.

• **ANO NE** Pro libovolnou permutaci $\pi \in S_{10}$ platí: Pokud $\pi^3 = id$, pak π je sudá.

Řešení.

- NE. Např. $\pi = (1\ 2)(3\ 4)$
- ANO. Vynásobením rovnice permutací π^{-1} zleva dostaneme $\nu = \pi^{-1}\rho$ a toto ν zřejmě rovnost splňuje.
- ANO. $1 = \mathrm{sgn}(id) = \mathrm{sgn}(\pi^3) = (\mathrm{sgn}(\pi))^3$, čili nutně $\mathrm{sgn}(\pi) = 1$.