1. Definujte grupu. Důležitou třídou grup jsou komutativní grupy, ty si dokonce vysloužily vlastní jméno a říkáme jim Abelovy (abelovské). Připomeňte i definici komutativity.

   Řešení: Operace je komutativní, pokud pro všechna a, b platí $a \circ b = b \circ a$.

   Grupa je dvojice $(G, \circ)$, kde G je množina a $\circ$ je binární operace na G (tedy $\circ\colon G \times G \to G$) splňující:

   (A) Operace $\circ$ je asociativní (tedy $(a \circ b) \circ c = a \circ (b \circ c)$ pro všechna $a, b, c \in G$).

   (E) Existuje prvek e takový, že pro všechna $a \in G$ platí $a \circ e = e \circ a = a$ (tento prvek nazýváme jednotkový nebo také neutrální).

   (I) Pro každé $a \in G$ existuje prvek $b \in G$ takový, že $a \circ b = b \circ a = e$, kde e je jednotkový prvek. Takovému b říkáme inverzní prvek a značíme ho a^{-1}.

2. Je daná operace binární operací na množině $\mathbb{R}$, na množině kladných přirozených čísel $\mathbb{N}^+$?

   (a) sčítání,

      i. na množině $\mathbb{N}^+$

         Řešení: Pokud sečtu dvě kladná celá čísla, dostanu kladné celé číslo. Obdobně pro reálná čísla.

         Tedy sčítání je binární operací na obou ($a + b \in \mathbb{R}$ pro všechna $a, b \in \mathbb{R}$ i pro $a, b \in \mathbb{N}^+$ máme $a + b \in \mathbb{N}^+$).

      ii. na množině $\mathbb{R}$

         Řešení:

   (b) odčítání,

      i. na množině $\mathbb{N}^+$

         Řešení: Není, například $3 - 8 = -5 \notin \mathbb{N}$.

      ii. na množině $\mathbb{R}$

         Řešení: Ano, pokud odečtu dvě reálná čísla, dostanu reálné číslo.

   (c) dělení,

      i. na množině $\mathbb{N}^+$

         Řešení: Není na kladných přirozených číslech ($5/3 \notin \mathbb{N}^+$).

      ii. na množině $\mathbb{R}$

         Řešení: Dělení není binární operací na reálných číslech, protože nemůžeme dělit nulou.

   (d) násobení

      Řešení: Násobení je na obou (obdobně jako sčítání).

3. Pro kladné celé číslo n a dvě celá čísla a, b řekneme, že a, b jsou kongruentní modulo n psáno $a \equiv b \pmod{n}$, právě když n dělí $a - b$ (tedy $a - b$ je celočíselným násobkem n). Ověřte, jestli následující jsou grupy, případně Abelovy grupy:

   (a) Regulární matice $\mathbb{R}^{12\times 12}$ s operací $\circ$ maticové násobení.

   (b) $(\mathbb{N}, \circ)$, kde $a \circ b = \max\{a, b\}$.

   (c) Binární čísla dlouhá n číslic (2^n) a operace je xor (exkluzivní or, tedy $0 \oplus 0 = 1 \oplus 1 = 0$ a $1 \oplus 0 = 0 \oplus 1 = 1$. Pro více bitová čísla počítáme po jednotlivých složkách, tedy například $1100 \oplus 0111 = 1011$.

   (d) Nosná množina jsou dvojice reálných čísel (píšeme $\mathbb{R}^2$) a binární operace je dána $(a_1, a_2) \circ (b_1, b_2) = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)$.

   (e) Otočení čtverce.

   (f) Otočení a symetrie čtverce.

   (g) Otočení pravidelného čtyřstěnu.

   (h) Oblíbené hlavolamy často tvoří grupu (Rubikova kostka, Loydova patnáctka).

   (i) Sčítání celých čísel modulo 6.

   (j) Násobení nenulových čísel modulo 6.

   (k) Násobení nenulových čísel modulo 5.

4. Dokažte, že v každé grupě pro každé a existuje právě jeden inverzní prvek.

   Řešení: Z definice grupy existuje aspoň jeden inverzní prvek. Předpokládejme, že pro dané $a \in G$ existují dva inverzní prvky b, c. Pak můžeme psát $b = b \circ a \circ c = c$ neboť $a \circ c = b \circ a = e$, kde e je jednotkový prvek a využíváme asociativitu binární operace v grupě.

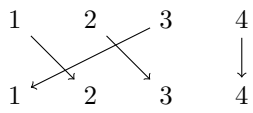
5. Dokažte, že v každé grupě existuje právě jeden jednotkový prvek.

   Řešení: Předpokládejme, že e, f jsou jednotkové prvky. Z definice jednotkového prvku máme $e = e \circ f = f$, tedy spor s předpokladem.

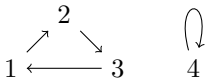
6. Dalším velice důležitým příkladem jsou grupy permutací značené S_n (kterým se říká symetrické grupy). Kde prvky jsou permutace na množině $\{1, \ldots, n\}$ a operace $\circ$ je skládání permutací. Dokažte, že toto je grupa.

   Připomeňme, že permutace je bijekce $\pi\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$. Permutaci můžeme zapsat jako tabulku hodnot, graficky znázornit pomocí šipek které ukazují který prvek se zobrazí na který. Navíc permutaci můžeme zapsat i jako permutační matici, která má v každém řádku i každém sloupci právě jednu jedničku a jinde nuly.

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



Obrázek 1: Bipartitní znázornění permutace.



Obrázek 2: Znázornění permutace pomocí orientovaného grafu.

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

Kolik je různých permutací na n prvkové množině?

Definujme množinu inverzí permutace π jako $I(\pi) = \{(i, j) \mid i < j \text{ a zároveň } \pi(i) > \pi(j)\}$. Znaménko permutace se definuje jako $\operatorname{sgn}(\pi) = (-1)^{|I(\pi)|}$. Znaménko lze definovat i jinými ekvivalentními způsoby.

Jaké je znaménko identity? Transpozice je permutace, která zamění dva prvky. Jaké je znaménko transpozice? Lze každou permutaci dostat jako složení transpozic?

Tvoří permutace znaménka 1 grupu? Co permutace znaménka -1?

Cyklus permutace je orientovaný cyklus v orientovaném grafu $(\{1, \ldots, n\}, \{(i, j) \mid j = \pi(i)\})$ (máme povolené smyčky).

Která permutace má nejvíc cyklů? Existuje permutace, která má pouze jeden cyklus?

Permutaci můžeme zapsat pomocí jejích cyklů tak, že seřadíme její cykly sestupně podle jejich minimálních prvků a zapíšeme je za sebe tak, že začneme vždy minimálním prvkem cyklu. Tedy naše ukázková permutace je zapsaná takto: 4123, což odpovídá cyklům (4)(123). To je ovšem jiná permutace, než permutace 4132, která odpovídá cyklům (4)(132).

7. Naučte se počítat v $GF(p)$ (také značeno $\mathbb{Z}_p$) pro p prvočíslo.

8. Vypište tabulku pro sčítání a tabulku pro násobení v tělese $\mathbb{Z}_5$ (tj. v tabulce sčítání budou řádky a sloupce indexované $0, 1, 2, 3, 4$ a na pozici i, j bude $i + j$, resp. $i \cdot j$).

   - Všimněte si, že pro každé číslo existuje číslo tak že když je vynásobíme, dostaneme jedničku (tj. inverzní prvek).
   - Všimněte si, že násobení nulou a jedničkou se chová, jak čekáte.
   - Všimněte si, že 4 se chová jako -1.

   Řešení:

Sčítání:

	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

Násobení:

	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

9. Praktická ukázka secret sharing. Mějme n lidí, chceme aby každých k z nich mělo možnost rekonstruovat tajemství $t \in \mathbb{Z}_p$ pro prvočíslo $p > n$. Jak tohoto docílíte pomocí polynomu vhodného stupně? Dokažte, že každých k lidí získá tajemství a že žádných $k-1$ lidí se o tajemství nic nedozví.

   Řešení: Shamirovo sdílení tajemství.