**5 Pratybos.** *Keitiniai.*

**Apibrėžimas 1**. *Keitinio* $\pi \in S_n$ ***eile*** *vadinamas toks mažiausias sveikas skaičius* $k \geq 1$, *kad* $\pi^k = id_{S_n}$.
*Žymime* $\text{ord}(\pi) = k$.

**Apibrėžimas 2**. *Skaičius* $d(\pi)$, *apibrėžiamas formule* $d(\pi) = s - k$ , *čia* $s$ - *keičiami keitinyje* $\pi$ *skaičiai,* $k$ - *nepriklausomų ciklų skaičius, vadinamas keitinio* $\pi$ **dekrementu**.

**Teorema.**

*1. Ciklo* $(i_1, i_2, ..., c_k)$ *eilė lygi* $k$.

*2. Jei keitinio* $\pi$ *reiškimas nepriklausomais ciklais yra*

$$\pi = \pi_1 \pi_2 \cdots \pi_r$$

*tai*

$$\text{ord}(\pi) = MBK\left(\text{ord}\left(\pi_1\right), \text{ord}\left(\pi_2\right), ..., \text{ord}\left(\pi_r\right)\right)$$

1. Keitinį $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 6 & 9 & 2 & 4 & 8 & 1 & 3 \end{pmatrix}$ parašykite nesikertančiais ciklais. Kokia keitinio $\sigma$ eilė ? Lyginis ar nelyginis šis keitinys ? Raskite $\sigma^{-1}$ .

2. Tegu $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 5 & 1 & 8 & 3 & 6 & 4 & 7 & 9 \end{pmatrix}$,
$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 4 & 7 & 2 & 6 & 8 & 9 & 3 \end{pmatrix}$ . Pararašykite keitinius $\sigma, \tau, \sigma \circ \tau, \sigma \circ \tau \circ \sigma^{-1}, \sigma^{-1}, \tau^{-1}, \tau \circ \sigma, \tau \circ \sigma \circ \tau^{-1}$ nesikertančiais ciklais. Kokios šių keitinių eilės? Lyginiai ar nelyginiai šie keitiniai ?

3. Tegu $\alpha = (1, 3, 5, 7, 9), \beta = (1, 2, 6), \gamma = (1, 2, 5, 3) \in S_{10}$ . Parašykite keitinį $\sigma = \alpha\beta\gamma$ nesikertančių ciklų sandauga. Raskite $\sigma$ ir $\sigma^{-1}$ eiles. Lyginiai ar nelyginiai šie keitiniai ?

4. Tegu $\sigma = (2, 4, 9, 7)(6, 4, 2, 5, 9)(1, 6)(3, 7, 6) \in S_9$ . Parašykite keitinį $\sigma$ nesikertančių ciklų sandauga. Raskite $\sigma$ ir $\sigma^{-1}$ eiles. Lyginiai ar nelyginiai šie

keitiniai ?

5. Tegu $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 7 & 2 & 11 & 4 & 6 & 8 & 9 & 10 & 1 & 3 & 5 \end{pmatrix}$, o $\sigma = (3, 8, 7) \in S_{11}$ . Pararašykite keitinius $\sigma, \tau, \sigma \circ \tau, \sigma \circ \tau \circ \sigma^{-1}, \sigma^{-1}, \tau^{-1}, \tau \circ \sigma, \tau \circ \sigma \circ \tau^{-1}$ nesikertančiais ciklais. Kokios šių keitinių eilės? Lyginiai ar nelyginiai šie keitiniai ?

6. Įrodykite, kad grupėje $S_{10}$ yra 10, 12, 14 eilės keitiniai , bet nėra 11 ir 13 eilių keitinių .

7. Įrodykite: Jei keitinio $\pi$ dekrementas $d(\pi) = d$ , tai sign$\pi = (-1)^d$ .

**Geometrinių figūrų simetrijų aibės**

Tegu $\triangle ABC-$ lygiakraštis trikampis. Jo simetrijų aibė yra reiškiama $S_3$ keitiniais:

$\varepsilon = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$ tapati simetrija

$a = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$ posūkis 120° kampu

$b = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$ posūkis 240° kampu

$c = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$ simetrija A atžvilgiu

$d = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$ simetrija B atžvilgiu

$e = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$ simetrija C atžvilgiu

**Uždaviniai**

1. Sudarykite trikampio simetrijų daugybos lemtelę.

2. Raskite ir apibrėžkite keitiniais visas kvadrato simetrijas ir sudarykite visų kvadrato simetrijų daugybos lentelę.

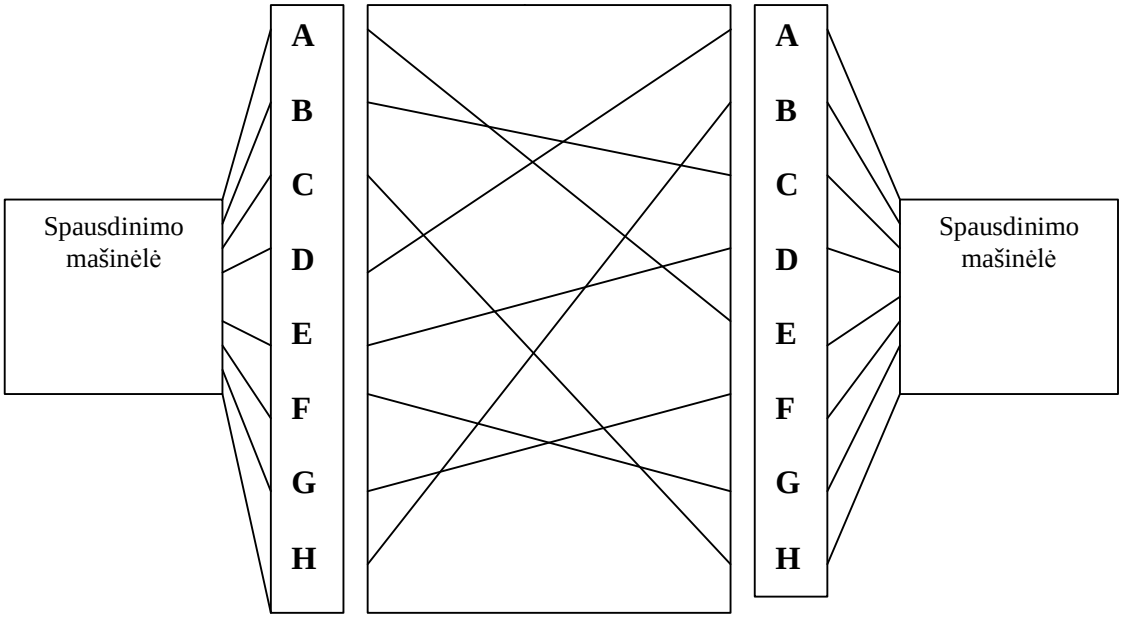
3. Raskite ir apibrėžkite keitiniais visas rombo( ne kvadrato) simetrijas ir sudarykite visų rombo simetrijų daugybos lentelę.

4. Raskite ir apibrėžkite keitiniais visas stačiakampio( ne kvadrato) simetrijas ir sudarykite visų stačiakampio simetrijų daugybos lentelę.

5. Raskite ir apibrėžkite keitiniais visas taisyklingojo tetraedro simetrijas ir sudarykite visų taisyklingojo tetraedro simetrijų daugybos lentelę.

6. Raskite ir apibrėžkite keitiniais visas kubo simetrijas ir sudarykite visų kubo simetrijų daugybos lentelę

**ENIGMA kodas su vienu rotoriumi**




Enigma tipo šifravimo įrenginio su vienu rotoriumi veikimo principas

Nagrinėjamoje abėcėlėje $\mathcal{A}_8$ yra 8 raidės: $\mathcal{A}_8 = \{\text{A,B,C,D,E,F,G,H}\}$. Kiekvienai šios abėcėlės raidę koduojame jos eilės numeriu:

raidę A koduojame 1, raidę B - 2, C - 3, D - 4, E - 5, F - 6, G - 7 ir H - 8.

Rotoriaus keitinį pažymėkime

$$\lambda = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ i_1 & i_2 & i_3 & i_4 & i_5 & i_6 & i_7 & i_8 \end{pmatrix}.$$

Pateiktame pavyzdyje rotoriaus keitinys yra

$$\lambda = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 2 & 5 & 1 & 7 & 6 & 3 \end{pmatrix}$$

Pirmos šifruojamo teksto raidės keitinys bus

$$\sigma_0 = \lambda = \varepsilon\lambda\varepsilon$$

Rotoriaus vieno žingsnio posūkio keitinys( posūkis viena pozicija pagal laikrodžio rodyklę) yra

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix}.$$

Antros šifruojamo teksto raidės keitinys bus

$$\sigma_1 = \rho^{-1}\lambda\rho.$$

Vadinasi pasukę rotorių per m pozicijų, gausime $(m+1)$-ojo šifruojamo teksto raidės keitinį :

$$\sigma_m = \rho^{-m}\lambda\rho^m.$$

Skaičiuojant reiktų atsižvelgti, kad $\mathrm{ord}(\rho) = 8$, t.y. $\rho^8 = \varepsilon$.

Jeigu yra šifruojamas tekstas koduotas skaičių seka $r_1\ r_2\ \cdots\ r_n$, tai teksto šifras bus

$\sigma_0(r_1)\ \sigma_1(r_2)\ \cdots\ \sigma_{n-1}(r_n)$.

Pavyzdžiui, jei rotoriaus keitinys $\lambda$ kaip pavyzdyje, o yra šifruojamas tekstas yra HFEECDAD, tai ketvirtoji teksto raidė E, kurios kodas yra 5, yra šifruojama taip:

$$\sigma_3(5) =$$
$$\rho^{-3}\lambda\rho^3(5) =$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix}^{-3} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 2 & 5 & 1 & 7 & 6 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix}^{3} (5) =$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 6 & 7 & 8 & 1 & 2 & 3 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 2 & 5 & 1 & 7 & 6 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 6 & 7 & 8 & 1 & 2 & 3 \end{pmatrix} (5) =$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 8 & 1 & 2 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 2 & 5 & 1 & 7 & 6 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 6 & 7 & 8 & 1 & 2 & 3 \end{pmatrix} (5) =$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 4 & 3 & 8 & 1 & 5 & 7 \end{pmatrix} (5) = 8$$

Gavome, kad ketvirtoji teksto raidė E šifruojama raide H (aštuntoji abėcėlės raidė).

**Uždaviniai**

1. Įodykite, kad šifro$(m+1)$-ojo simbolio dešifravimo keitinys yra

$$\sigma_m^{-1} = \rho^{-m}\lambda^{-1}\rho^m.$$

2. Užšifruokite pranešimą:

DAEGGCGFFHEACFAHDGAEDGAFEE

ENIGMA mašina, kurios rotoriaus keitinys $\lambda = (138)\,(27)\,(54)$

3. Dešifruokite šifrą

CGEDFFGAECDDCADGHEACDEEABD

ENIGMA mašina, kurios rotoriaus keitinys $\lambda = (278)\,(16543)\,.$