2. KEITINIAI

(2021–2023)

Teorinę medžiagą parengė bei antrąją užduotį sudarė Vilniaus universiteto docentas Aivaras Novikas

Keitinio apibrėžimas. Keitiniai yra tam tikros funkcijos. Funkcija yra taisyklė, pagal kurią kiekvienam vienos aibės X elementui x priskiriamas lygiai vienas kitos aibės Y elementas y. Aibė X vadinama atitinkamos funkcijos apibrėžimo sritimi, ir sakoma, kad ta funkcija apibrėžta aibėje X. Pavyzdžiui, funkcija $f(x) = x^2$, apibrėžta visų realiųjų skaičių aibėje $\mathbb{R}$, reiškia taisyklę, kad skaičiui $x = 5$ priskiriamas skaičius $y = f(5) = 5^2 = 25$, skaičiui $x = -\sqrt[4]{3}$ – skaičius $y = \sqrt{3}$, skaičiui $x = 2\pi \approx 6{,}28$ – skaičius $y = 4\pi^2 \approx 39{,}48$, ir t. t. Visų x reikšmių neišvardysime, nes jų yra be galo daug, tačiau bet kuriai iš jų galime pritaikyti taisyklę ir apskaičiuoti funkcijos reikšmę $y = f(x)$. Mokykloje nagrinėjamos funkcijos, apibrėžtos begalinėse aibėse: aibėje $\mathbb{R}$, šios aibės intervaluose ir intervalų sąjungose. Pavyzdžiui, funkcija $f(x) = \frac{1}{x^2+4}$ gali būti apibrėžta visoje aibėje $\mathbb{R}$, funkcija $f(x) = \frac{1}{\sqrt{x+4}}$ – intervale $(-4;\ +\infty)$, o funkcija $f(x) = \frac{1}{\sqrt{x^2-4}}$ – intervalų $(-\infty;\ -2)$ ir $(2;\ +\infty)$ sąjungoje. Čia nagrinėsime kitokias – baigtines – aibes. Keitiniai yra tokios funkcijos, kurioms $X = Y = \{1, 2, 3, \dots, n\}$. Čia n yra duotas natūralusis skaičius, o aibę $\{1, 2, 3, \dots, n\}$ sudaro visi natūralieji skaičiai nuo 1 iki n. Taigi keitinys yra funkcija, kiekvienam natūraliajam skaičiui nuo 1 iki n priskirianti po kokį nors natūralųjį skaičių nuo 1 iki n. Yra dar viena sąlyga: jokios dvi keitinio reikšmės negali sutapti, t. y. jei funkcija f yra keitinys, tai visos jos reikšmės $f(1), f(2), \dots, f(n)$ turi būti tarpusavyje skirtingos. Funkcija, kurios jokios dvi reikšmės nesutampa, vadinama *injektyvia*.

Dabar galime suformuluoti keitinio **apibrėžimą**: keitiniu vadinama injektyvi funkcija, apibrėžta ir įgyjanti reikšmes aibėje $\{1, 2, 3, \dots, n\}$, kur n yra duotas natūralusis skaičius.

Kadangi keitinio apibrėžimo sritis yra baigtinė aibė, tai konkretų keitinį galima apibrėžti tiesiog išvardijant visas n jo reikšmių. Pavyzdžiui, kai $n = 4$, keitinį f galima apibrėžti keturiomis lygybėmis $f(1) = 3$, $f(2) = 4$, $f(3) = 2$, $f(4) = 1$. Tuo tarpu funkcija g su apibrėžimo sritimi $\{1, 2, 3, 4\}$, apibrėžta lygybėmis $g(1) = 3$, $g(2) = 4$, $g(3) = 2$, $g(4) = 3$, nėra keitinys, nes reikšmę $3 = g(1) = g(4)$ įgyja du kartus. Kiekvienas keitinys f žymimas tokia lentele:

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$$

(pirmoje eilutėje iš eilės užrašyti natūralieji skaičiai nuo 1 iki n, o po jais išvardytos atitinkamos keitinio reikšmės). Mūsų pavyzdyje vietoj keturių lygybių būtų galima užrašyti $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$. Šis užrašas nurodo taisyklę, kaip priskiriamos funkcijos reikšmės, tik kitu būdu nei, pavyzdžiui, užrašas $f(x) = x^2$. Jis reiškia, kad funkcija f skaičiui $x = 1$ priskiria po juo antroje eilutėje esantį skaičių $y = f(1) = 3$, ir t. t. Kad lentelė $\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$ žymėtų kokį nors keitinį, antros eilutės skaičiai $f(1)$, $f(2)$, ..., $f(n)$ turi priklausyti aibei $\{1, 2, 3, \dots, n\}$ ir būti tarpusavyje skirtingi. Pavyzdžiui, lentelė $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 3 \end{pmatrix}$ galėtų žymėti nagrinėtąją funkciją g, bet nežymi keitinio, nes jos antroje eilutėje yra du trejetai.

Keitiniai ir kėliniai. Mokykloje nagrinėjami baigtinės aibės kėliniai – tos aibės visų elementų surašymai kokia nors tvarka. Pavyzdžiui,

$$1, 2, 3, 4; \qquad 1, 2, 4, 3; \qquad 4, 3, 2, 1; \qquad 2, 4, 1, 3$$

yra keturi skirtingi aibės $\{1, 2, 3, 4\}$ kėliniai. Kad gautume šios aibės kėlinį, pirmąjį jo skaičių galime parinkti keturiais būdais, tada antrąjį – trimis, tada trečiąjį – dviem, o tada ketvirtąjį – tik vienu. Vadinasi, aibės $\{1, 2, 3, 4\}$ kėlinių yra $4 \cdot 3 \cdot 2 \cdot 1 = 4! = 24$. Panašiai įrodoma, kad aibė $\{1, 2, 3, \dots, n\}$ turi lygiai $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n!$ kėlinių.

Keitinio lentelės $\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$ antroje eilutėje yra n skirtingų skaičių iš aibės $\{1, 2, 3, \dots, n\}$. Šioje aibėje tėra n skaičių, todėl lentelės antroje eilutėje turi būti jie visi (kiekvienas po vieną kartą). Vadinasi, keitinį gausime, lentelės $\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$ antroje eilutėje užrašę aibės $\{1, 2, 3, \dots, n\}$ kėlinį. Su kiekvienu kėliniu gausime vis kitokį keitinį. Todėl duotam skaičiui n keitinių yra $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n = n!$ – tiek pat, kiek kėlinių. Duotam skaičiui n visų keitinių

$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}$ aibę žymėsime S_n. Vėliau apibrėšime keitinių daugybą. Aibė S_n su joje apibrėžta daugyba yra vadinama **simetrine grupe**. Pavyzdžiui, simetrinėje grupėje S_3 yra $3! = 6$ keitiniai: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Kiekvienoje grupėje S_n yra keitinys e_n, kurio lentelėje abi eilutės vienodos. Jis pasižymi savybe $e_n(x) = x$ (kiekvienam x). Šis keitinys vadinamas **vienetiniu**. Pavyzdžiui, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e_5 \in S_5$.

Keitinių daugyba. Dviejų tos pačios aibės S_n keitinių f ir g sandauga apibrėžiama taip:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ g\big(f(1)\big) & g\big(f(2)\big) & \dots & g\big(f(n)\big) \end{pmatrix}.$$

Taigi vietoj įprastos funkcijų sandaugos $f(x) \cdot g(x)$, kai tiesiog dauginame jų atitinkamas reikšmes, iš tikrųjų turime funkcijų kompoziciją $g\big(f(x)\big)$, kai viena funkcija įrašoma į kitą. Kad nustatytume funkcijos $g\big(f(x)\big)$ konkrečią reikšmę $z_0 = g\big(f(x_0)\big)$, turime pirmiausiai nustatyti reikšmę $y_0 = f(x_0)$, o po to reikšmę $z_0 = g(y_0)$. Keitiniams tokią kompoziciją įprasta žymėti daugybos ženklu.

1 pavyzdys. Sandaugą $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 6 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 3 & 6 & 1 \end{pmatrix}$ galime gauti (t. y. užpildyti geltonus langelius) taip: kai $x_0 = 1$, tai $y_0 = 4$ (pirmasis keitinys); kai $y_0 = 4$, tai $z_0 = 2$ (antrasis keitinys); todėl sandaugos lentelėje po $x_0 = 1$ rašome $z_0 = 2$. Trumpiau: skaičiui 1 priskiriamas skaičius 4, o tada skaičiui 4 – skaičius 2, taigi sandauga skaičiui 1 priskiria skaičių 2. Dar trumpiau: $1 \to 4 \to 2$. Analogiškai baigiame pildyti antrąją sandaugos lentelės eilutę (veiksmus galima atlikti mintinai): $2 \to 5 \to 4$; $3 \to 3 \to 5$; $4 \to 6 \to 3$; $5 \to 1 \to 6$; $6 \to 2 \to 1$.

Daugybos savybės. Toliau keitinius žymėsime ne f, g, ..., bet a, b, c, ...

1) Keitinių a ir b iš S_n sandauga $a \cdot b$ taip pat yra keitinys iš S_n.

Iš tiesų, a yra keitinys, todėl visi skaičiai $a(1)$, $a(2)$, ..., $a(n) \in \{1, 2, \dots, n\}$ yra tarpusavyje skirtingi. Kadangi b yra keitinys, o skaičiai $a(1)$, $a(2)$, ..., $a(n)$ yra tarpusavyje skirtingi, tai skaičiai $b\big(a(1)\big)$, $b\big(a(2)\big)$, ..., $b\big(a(n)\big) \in \{1, 2, \dots, n\}$ taip pat yra tarpusavyje skirtingi, o lentelė $\begin{pmatrix} 1 & 2 & \dots & n \\ b\big(a(1)\big) & b\big(a(2)\big) & \dots & b\big(a(n)\big) \end{pmatrix}$ žymi keitinį.

2) $a \cdot b$ nebūtinai lygu $b \cdot a$. Įsitikinkime tuo, sukeitę 1 pavyzdžio keitinius vietomis:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 2 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 6 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 5 & 6 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 3 & 6 & 1 \end{pmatrix}.$$

3) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Iš tiesų, jei $a(x_0) = y_0$, $b(y_0) = z_0$, $c(z_0) = t_0$, tai nesvarbu ar gausime, kad keitiniui $a \cdot b$ turime $x_0 \to y_0 \to z_0$, o keitiniui c turime $z_0 \to t_0$, ar kad keitiniui $b \cdot c$ turime $y_0 \to z_0 \to t_0$, o keitiniui a turime $x_0 \to y_0$. Abiem atvejais gausime situaciją $x_0 \to y_0 \to z_0 \to t_0$ ir tą patį galutinį daugybos rezultatą $c\Big(b\big(a(x_0)\big)\Big) = t_0$.

4) Prisiminus e_n apibrėžimą, nesunku suvokti, kad jei $a \in S_n$, tai $a \cdot e_n = e_n \cdot a = a$. Pastebėkime, kad keitinių daugybos atžvilgiu keitinys e_n aibėje S_n atlieka panašų vaidmenį, kokį realiųjų skaičių aibėje atlieka skaičius 1, taip pat pasižymintis savybe $a \cdot 1 = 1 \cdot a = a$. Todėl keitinys e_n ir vadinamas vienetiniu.

5) Jei $a \in S_n$, tai egzistuoja toks $a^{-1} \in S_n$, kad $a \cdot a^{-1} = a^{-1} \cdot a = e_n$. Keitinys a^{-1} vadinamas keitinio a **atvirkštiniu** keitiniu.

Iš tiesų, kad turėtume reikiamą keitinį a^{-1}, jis turi pasižymėti savybe: jei keitiniui a turime $x_0 \to y_0$, tai keitiniui a^{-1} turime $y_0 \to x_0$. Tokį keitinį a^{-1} gausime, su keitiniu a atlikę veiksmus: jo lentelėje kiekvieną stulpelį $\begin{matrix} x_0 \\ y_0 \end{matrix}$ pakeitę stulpeliu $\begin{matrix} y_0 \\ x_0 \end{matrix}$ (t. y. sukeitę eilutes vietomis), o tada stulpelių tvarką pakeitę taip, kad pirmoje eilutėje skaičiai eitų didėjimo tvarka.

Jei vienetinis keitinys atitinka skaičių 1, tai atvirkštiniai keitiniai turėtų priminti atvirkštinius skaičius. Pavyzdžiui, skaičiai 2 ir $2^{-1} = 0{,}5$ yra vienas kitam atvirkštiniai, nes $2 \cdot 0{,}5 = 0{,}5 \cdot 2 = 1$.

2 pavyzdys. Nustatykime šią trijų keitinių sandaugą ir jos atvirkštinį keitinį:

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

Daugybos 2 ir 3 savybės parodo, kad keitinių negalime sukeisti vietomis, bet galime arba pirmiau atlikti pirmąjį daugybos veiksmą, o tada antrąjį, arba pirmiau atlikti antrąjį daugybos veiksmą, o tada (su pirmuoju keitiniu ir gauta sandauga) pirmąjį. Tačiau abu daugybos veiksmus patogu apjungti.

Trys duotieji keitiniai priskiria skaičius atitinkamai tokiu būdu: $4 \to 8;\ 8 \to 5;\ 5 \to 6$. Todėl trijų keitinių sandaugai turime $4 \to 8 \to 5 \to 6$, t. y. sandauga skaičiui 4 priskiria skaičių 6. Taip pat, pavyzdžiui, turime $7 \to 2 \to 2 \to 1$, t. y. sandauga skaičiui 7 priskiria skaičių 1. Panašiai mąstydami, užpildome visą lentelę ir gauname atsakymą (patikrinkite!): $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 4 & 5 & 6 & 2 & 3 & 1 & 8 \end{pmatrix}$.

Atvirkštinis keitinys gaunamas taip (žr. 5 savybės pagrindimą):

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

3 pavyzdys. Nustatykime visus tokius keitinius $u \in S_9$, kad

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 8 & 5 & 3 & 7 & 4 & 1 & 6 \end{pmatrix} \cdot u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 4 & 5 & 3 & 7 & 1 & 2 & 8 \end{pmatrix}^4.$$

Užrašykime lygtį trumpiau: $a \cdot u = c^4$. Pirmiausiai suprastinkime jos dešiniąją pusę. Kaip ir skaičiams, keitiniams užrašas c^4 reiškia $c \cdot c \cdot c \cdot c$. Taigi turime sudauginti 4 vienodus keitinius. Taigi pagal keitinį c sudarome reikiamas sekas su 4 rodyklėmis, pavyzdžiui, $1 \to 9 \to 8 \to 2 \to 6$ ir $4 \to 5 \to 3 \to 4 \to 5$. Taip gauname $b = c^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 9 & 4 & 5 & 3 & 8 & 2 & 1 & 7 \end{pmatrix}$.

Pamėginkime lygybėje $a \cdot u = b$ išreikšti u. Nederėtų rašyti $u = b\!:\!a$, nes keitinių dalybos neapibrėžėme (ir neapibrėšime). Vietoj to pasinaudokime daugybos 5 savybe. Lygybės abi puses padauginkime iš a^{-1}. Atminkime, kad dauginimo tvarka yra svarbi: $b \cdot a^{-1} = (a \cdot u) \cdot a^{-1}$ (čia dauginamieji a ir a^{-1} nesusiprastins, nes nėra greta), bet, kita vertus, $a^{-1} \cdot b = a^{-1} \cdot (a \cdot u) = (a^{-1} \cdot a) \cdot u = e_9 \cdot u = u$. Taigi $u = a^{-1} \cdot b$, ir ši reikšmė tenkina lygtį: $a \cdot u = a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = e_9 \cdot b = b$. Dabar beliko nustatyti $a^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 5 & 7 & 4 & 9 & 6 & 3 & 2 \end{pmatrix}$ ir

$$u = a^{-1} \cdot b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 6 & 3 & 2 & 5 & 7 & 8 & 4 & 9 \end{pmatrix}.$$

Apibendrinkime šį pavyzdį: jei duoti $a, b \in S_n$, tai lygtis $a \cdot u = b$ turi lygiai vieną sprendinį $u = a^{-1} \cdot b$. Panašiai nustatoma, kad lygtis $u \cdot a = b$ turi lygiai vieną sprendinį $u = b \cdot a^{-1}$ ir kad lygtis $a \cdot u \cdot b = c$ turi lygiai vieną sprendinį $u = a^{-1} \cdot c \cdot b^{-1}$ (čia $a, b, c \in S_n$ – duoti keitiniai).

Keitinio išraiška ciklais. Matėme, kad keitinį galima užrašyti dviejų eilučių lentele, pavyzdžiui, $c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 6 & 4 & 5 & 3 & 7 & 1 & 2 & 8 \end{pmatrix}$. Informaciją, vienareikšmiškai nusakančią duotą keitinį, kartais naudinga užrašyti kitokia forma. Kiekvieną keitinį galima **užrašyti** ne tik **lentele**, bet ir **ciklais**. Visų pirma, duotos lentelės informaciją pavaizduokime rodyklėmis: $1 \to 9;\ 2 \to 6;\ 3 \to 4;\ 4 \to 5;\ 5 \to 3;\ 6 \to 7;\ 7 \to 1;\ 8 \to 2;\ 9 \to 8$. Šį užrašą galima sutrumpinti, jungiant jo atskiras dalis: $1 \to 9 \to 8 \to 2 \to \cdots$. Tęsdami tokią seką bet kokiam keitiniui, neišvengiamai prieisime jau užrašytą skaičių (juk skaičių kiekis baigtinis). Jei pirmas pasikartojęs sekos skaičius x nebūtų pirmasis sekos skaičius, tai į skaičių x būtų nukreiptos dvi rodyklės, o keitinio lentelės antroje eilutėje atitinkamai būtų du skaičiai x. Vadinasi, pirmas sekoje pasikartoja tas skaičius, kuriuo seka prasideda. Taip bus ir mūsų atveju: $1 \to 9 \to 8 \to 2 \to 6 \to 7 \to 1 \to \cdots$. Toliau sekoje pirmieji jos skaičiai ima kartotis, jie sudaro lyg uždarą ratą – **ciklą**. Pasirinkę bet kurį dar nepanaudotą skaičių ir jam užrašę naują seką, gausime dar vieną ciklą: $3 \to 4 \to 5 \to 3$. Jei dar liktų neužrašytų skaičių, tai šį procesą tęstume, tačiau šiuo atveju jau gavome visus 9 skaičius. Vadinasi, keitinį c sudaro du ciklai. Ciklas užrašomas, iš eilės viena eilute surašant visus skirtingus ciklo skaičius: $(1\ \ 9\ \ 8\ \ 2\ \ 6\ \ 7)$ ir $(3\ \ 4\ \ 5)$. Ciklai parodo visą keitinio lentelės informaciją: kiekvienam ciklo skaičiui, išskyrus paskutinį, keitinys priskiria gretimą iš dešinės skaičių, o paskutiniam ciklo skaičiui priskiriamas pirmas to ciklo skaičius. Nesvarbu kuriuo skaičiumi pradėsime ciklą: pavyzdžiui, $(1\ \ 9\ \ 8\ \ 2\ \ 6\ \ 7) = (8\ \ 2\ \ 6\ \ 7\ \ 1\ \ 9)$. **Keitinio išraiškoje ciklais** jis užrašomas išvardijant visus jo ciklus: $c = (1\ \ 9\ \ 8\ \ 2\ \ 6\ \ 7)(3\ \ 4\ \ 5)$. Ciklų tvarka tokioje išraiškoje nesvarbi: pavyzdžiui, $c = (4\ \ 5\ \ 3)(8\ \ 2\ \ 6\ \ 7\ \ 1\ \ 9)$. Skaičių kiekis cikle vadinamas **ciklo ilgiu**.

4 pavyzdys. Tris dauginamuosius 2 pavyzdyje užrašykime ciklais:

$(1\ \ 7\ \ 2)(3\ \ 5\ \ 4\ \ 8\ \ 6) \cdot (1\ \ 4\ \ 8\ \ 5)(2)(3\ \ 6\ \ 7) \cdot (1\ \ 5\ \ 6\ \ 3\ \ 7\ \ 8\ \ 2)(4)$.

Išspręskime 2 pavyzdžio uždavinį, bet sandaugą ir jos atvirkštinį keitinį iš karto užrašykime ciklais, o turėdami atsakymo išraišką ciklais perrašykime jį lentele. Sandaugos ieškome taip: pradedame bet kuriuo skaičiumi (pavyzdžiui, 1) ir gauname, kurį skaičių jam priskiria sandauga: $1 \to 7 \to 3 \to 7$. Taigi pradedame ciklą: $(1\ \ 7\ \ \ldots)$. Toliau tikriname skaičių 7 ir gauname $7 \to 2 \to 2 \to 1$. Ciklas užsivėrė, todėl užskliaučiame jį ir atveriame naują ciklą, pradėdami dar nepanaudotu skaičiumi, pavyzdžiui, 2: $(1\ \ 7)(2\ \ \ldots)$. Tęsiame šį procesą ($2 \to 1 \to 4 \to 4$; $4 \to 8 \to 5 \to 6$; ...), kol užrašome visus skaičius ir gauname sandaugą $(1\quad 7)(2\quad 4\quad 6\quad 3\quad 5)(8)$. Sandaugos atvirkštinis keitinys gaunamas, kiekviename cikle skaičių tvarką pakeičiant priešinga: $\big((1\quad 7)(2\quad 4\quad 6\quad 3\quad 5)(8)\big)^{-1} = (7\quad 1)(5\quad 3\quad 6\quad 4\quad 2)(8)$. Ši išraiška rodo keitinio priskyrimus $7 \to 1$; $1 \to 7$; $8 \to 8$; ir t. t. Juos nurodome keitinio lentelėje (visus veiksmus patikrinkite savarankiškai!): $(7\quad 1)(5\quad 3\quad 6\quad 4\quad 2)(8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 5 & 6 & 2 & 3 & 4 & 1 & 8 \end{pmatrix}$.

5 pavyzdys. Keitinius $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 3 & 13 & 4 & 12 & 9 & 1 & 10 & 7 & 11 & 2 & 8 & 5 & 6 \end{pmatrix}^{2021}$ ir $b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 6 & 1 & 7 & 2 & 4 & 10 & 9 & 8 \end{pmatrix}^{2022}$ nustatysime lengviau, jei keliamus laipsniu keitinius pirma užrašysime ciklais: $a = (1\quad 3\quad 4\quad 12\quad 5\quad 9\quad 11\quad 8\quad 7\quad 10\quad 2\quad 13\quad 6)^{2021}$ ir $b = \big((1\quad 5\quad 7\quad 4)(2\quad 3\quad 6)(8\quad 10)(9)\big)^{2022}$.

Nagrinėkime keitinį a ir nustatykime, kokį skaičių jis priskiria skaičiui 1. Tai skaičius, einantis po 2021-os rodyklės sekoje $1 \to 3 \to 4 \to 12 \to \cdots$. Pirmieji 13 skaičių sekoje yra skirtingi, o po 13-tos rodyklės eina skaičius 1, ir tie patys 13 skaičių ima ta pačia tvarka kartotis. Taigi skaičių seka yra periodinė. Pavyzdžiui, po pirmos rodyklės eina skaičius 3, todėl jis eina ir po $1 + 13 = 14$-tos, $14 + 13 = 27$-tos, $27 + 13 = 40$-tos ir t. t. rodyklių. Padalykime skaičių 2021 iš 13 su liekana: $2021 = 13 \cdot 155 + 6$. Todėl po 2021-os rodyklės eina tas pats skaičius, kuris eina po $2021 - 13 - -13 - \cdots - 13 = 6$-tos. Tai yra 6-as ciklo $(1\quad 3\quad 4\quad 12\quad 5\quad 9\quad 11\quad 8\quad 7\quad 10\quad 2\quad 13\quad 6)$ skaičius, einantis po vieneto. Taigi tai skaičius $a(1) = 11$, ir turime $a = (1\quad 11\quad ...)$. Remiantis ta pačia logika, $a(11)$ yra to paties ciklo skaičius, 6-as po skaičiaus 11. Tai skaičius $a(11) = 6$. Analogiškai gauname $a(6) = 9$, $a(9) = 13$, $a(13) = 5$, $a(5) = 2$, $a(2) = 12$, ir t. t. Taip randame $a = (1\quad 11\quad 6\quad 9\quad 13\quad 5\quad 2\quad 12\quad 10\quad 4\quad 7\quad 3\quad 8)$.

Apibendrinkime: kad pakeltume keitinį dideliu laipsniu ir gautume rezultatą a, turėjome laipsnio rodiklį (čia 2021) padalyti su liekana iš ciklo ilgio (čia iš 13). Gautoji liekana (čia 6) parodė, kelintas skaičius cikle yra skaičius $a(x)$, skaičiuojant nuo skaičiaus x (čia x – bet kuris to ciklo skaičius).

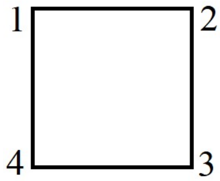
Nustatykime b. Turime ciklą $(1\quad 5\quad 7\quad 4)$, kurio ilgis yra 4. Skaičius 2022 dalijasi iš 4 su liekana 2. Todėl $b(1)$ yra šio ciklo skaičius, antras po skaičiaus 1. Taigi $b(1) = 7$. Analogiškai, $b(7) = 1$, $b(5) = 4$, $b(4) = 5$. Taigi keitinyje b ciklas $(1\quad 5\quad 7\quad 4)$ suskyla į du ciklus $(1\quad 7)$ ir $(4\quad 5)$. Turime ciklą $(2\quad 3\quad 6)$. Skaičius 2022 dalijasi iš 3 su liekana 0. Ką tai pasako apie $b(2)$? Kadangi 2022 dalijasi iš 3, tai periodinėje sekoje $2 \to 3 \to 6 \to 2 \to 3 \to 6 \to \cdots$ po 2022-os rodyklės eina skaičius 2. Taigi $b(2) = 2$. Analogiškai, $b(3) = 3$, $b(6) = 6$. Taigi keitinyje b ciklas $(2\quad 3\quad 6)$ suskyla į tris ciklus (2), (3), (6). Kadangi 2022 dalijasi ir iš 2, tai ir ciklas $(8\quad 10)$ suskyla į (8), (10) (o priešingu atveju liktų nepakitęs, nes dalybos iš 2 liekana būtų lygi 1). Žinoma, sekoje $9 \to 9 \to 9 \to \cdots$ po kiekvienos rodyklės eina skaičius 9, todėl $b(9) = 9$. Vadinasi, $b = = (1\quad 7)(4\quad 5)(2)(3)(6)(8)(10)(9)$.

Keitinio eilė. Jei 5 pavyzdyje vietoj rodiklio 2021 turėtume rodiklį 2028, kuris dalijasi iš 13, tai tokiu laipsniu keliamas vienaciklis keitinys suskiltų į 13 vienetinių ciklų, t. y. gautume $a = e_{13}$. Kad gautume $b = e_{10}$, pakeitę rodiklį 2022 į kokį nors natūralųjį skaičių k, tam į vienetinius ciklus turi suskilti ciklai $(1\quad 5\quad 7\quad 4)$, $(2\quad 3\quad 6)$, $(8\quad 10)$, kurių ilgiai yra $4, 3, 2$. Taigi skaičius k turi dalytis iš 4, 3 ir 2, t. y. iš $4 \cdot 3 = 12$. Tinka $k = 12, 24, 36, ...$

Tarkime, kad duotas bet koks $a \in S_n$. Mažiausias toks natūralusis skaičius k, kad $a^k = e_n$, vadinamas keitinio a **eile**. Apibendrinkime mūsų pastebėjimus: eilė k yra toks mažiausias natūralusis skaičius, kuris dalijasi iš visų keitinį a sudarančių ciklų ilgių, t. y. k yra visų keitinio a ciklų ilgių mažiausias bendras kartotinis. Pavyzdžiui, keitinio $(1\quad 2\quad 3\quad 4\quad 5\quad 6)(7\quad 8\quad 9\quad 10)$ eilė lygi $\mathrm{MBK}(6, 4) = 12$, o keitinio $(1\quad 2)(3\quad 4\quad 5)(6\quad 7\quad 8\quad 9\quad 10)$ eilė lygi $\mathrm{MBK}(2, 3, 5) = 30$.

6 pavyzdys. Nustatykime, kiek grupėje S_9 yra keitinių, kurių eilė yra 15. Tarkime, kad keitinio $a \in S_9$ eilė yra 15. Tada šio keitinio kiekvieno ciklo ilgis yra vienas iš skaičiaus 15 daliklių $1, 3, 5, 15$. Kita vertus, ciklų ilgių suma lygi 9. Taigi ciklų ilgiai tegali būti $1, 3, 5$. Jei ciklų ilgiai tėra lygūs 1 arba 3, tai ir šių ilgių mažiausias bendras kartotinis yra 1 arba 3. Taigi bent vieno ciklo ilgis turi būti 5. Analogiškai, bent vieno ciklo ilgis yra 3. Vadinasi, $3 + 5 = 8$ iš 9 skaičių sudaro du tokius ciklus, ir dar vienas skaičius sudaro vienetinį ciklą. Kiekvienas toks keitinys tinka, nes $\mathrm{MBK}(5, 3, 1) = 15$.

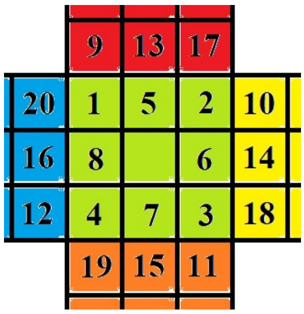
Taigi $a = (a_1)(a_2 \quad a_3 \quad a_4)(a_5 \quad a_6 \quad a_7 \quad a_8 \quad a_9)$. Skaičiui a_1 galime priskirti bet kurią iš 9 reikšmių 1, 2, ..., 9, tada skaičiui a_2 – vieną iš likusių 8 reikšmių, skaičiui a_3 – vieną iš likusių 7 reikšmių, ir t. t. Taigi pirmąjį ciklą sudaryti yra 9 būdai, tada antrąjį – $8 \cdot 7 \cdot 6$ būdų, tada trečiąjį – $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ būdų. Tačiau kai kurie iš taip sudarytų ciklų $(a_2 \quad a_3 \quad a_4)$ sutampa. Gautus $8 \cdot 7 \cdot 6$ ciklų galima suskirstyti į ciklų trejetus $(x \quad y \quad z)$, $(y \quad z \quad x)$, $(z \quad x \quad y)$. Kiekviename trejete turime tą patį ciklą, užrašytą trimis skirtingais būdais, o ciklai iš skirtingų trejetų visada skirtingi. Todėl skirtingų ciklų $(a_2 \quad a_3 \quad a_4)$ turime $\frac{8 \cdot 7 \cdot 6}{3}$. Analogiškai, skirtingų ciklų $(a_5 \quad a_6 \quad a_7 \quad a_8 \quad a_9)$ gauname ne $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$, bet $\frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{5}$. Vadinasi, tinkamų keitinių a yra $9 \cdot \frac{8 \cdot 7 \cdot 6}{3} \cdot \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{5} = 9 \cdot 112 \cdot 24 = 24\,192$.



Keitiniai ir simetrijos. Plokštumoje nagrinėkime kvadratą. Jo viršūnes iš eilės sunumeruokime (žr. pav.). Pasukę kvadratą aplink jo centrą 90° kampu pagal laikrodžio rodyklę, gausime tą patį kvadratą, tik kiekvienas skaičius užims kito skaičiaus vietą: $1 \to 2 \to 3 \to 4 \to 1$. Taigi šią kvadrato transformaciją apibūdina keitinys $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. Jei kvadratą suksime ne 90°, bet 180° kampu, tai reikš du posūkius 90° kampu, todėl posūkį 180° kampu apibūdina keitinys $a \cdot a = a^2 = (1 \quad 3)(2 \quad 4)$. Iš tiesų, po šio posūkio priešingos viršūnės (1 ir 3, 2 ir 4) susikeičia vietomis.

Geometrinės figūros (plokštumoje arba erdvėje) transformacija, kuria gaunama tokia pati (tiek forma, tiek dydžiu) figūra, užimanti tą pačią (plokštumos arba erdvės) vietą, yra vadinama tos figūros **simetrija**. Taigi kvadrato posūkiai 90° ir 180° kampais aplink jo centrą yra kvadrato simetrijos. Duotojo kvadrato simetrinis vaizdas horizontalios tiesės l, einančios per kvadrato centrą, atžvilgiu sutampa su kvadratu. Taigi turime dar vieną simetriją, kurią atitinka keitinys $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$. Tarkime, kad atlikome tokią transformaciją: kvadratą aplink jo centrą pasukome 90° kampu prieš laikrodžio rodyklę (tai tas pats kaip pasukti tris kartus pagal laikrodžio rodyklę), tada atvaizdavome simetriškai tiesės l atžvilgiu, o tada – simetriškai kvadrato centro atžvilgiu (tai tas pats kaip pasukti 180° kampu). Transformacijos tris veiksmus atitinka keitiniai a^3 (arba a^{-1}), b ir a^2. Taigi ją pačią apibūdina $a^3 \cdot b \cdot a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$. Dabar galime pastebėti: atlikti šią transformaciją trimis veiksmais yra tas pats, kaip atlikti ją tokiu vienu veiksmu: kvadratas simetriškai atvaizduojamas įstrižainės, jungiančios viršūnes 2 ir 4, atžvilgiu.

Tarkime, kad turime duotojo kvadrato simetriją, kuri kiekvieną kvadrato kraštinę perveda į jo (tą pačią ar kitą) kraštinę taip, kad kiekvieno kraštinės taško atstumai iki jos galų nepakistų. Viršūnė 1 gali būti atvaizduota į bet kurią vieną iš viršūnių 1, 2, 3, 4 (4 atvejai), o likusios trys viršūnės nuo viršūnės 1 gali iš eilės rikiuotis ratu pagal arba prieš laikrodžio rodyklę (2 atvejai). Taigi kvadratas turi tik $4 \cdot 2 = 8$ tokias simetrijas. Jas atitinka keitiniai $e_4 = a^4$, a, a^2, $a^3 = a^{-1}$ (posūkiai 0°, 90°, 180°, 270° kampais), b, $b \cdot a$, $b \cdot a^2$, $b \cdot a^3$ (kvadrato simetrijos jo keturių simetrijos ašių atžvilgiu). Tai 8 iš 24 aibės S_4 elementų. Tuo tarpu, pavyzdžiui, keitinys $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ tokios kvadrato simetrijos neapibūdina, nes čia kvadrato kraštinės galai 2 ir 3 pereina į įstrižainės galus 1 ir 3.



Keitiniais galima apibūdinti ir, pavyzdžiui, Rubiko kubo transformacijas. Kubas turi 6 sienas, kurių kiekviena padalyta į 9 langelius. Centrinis kiekvienos sienos langelis, sukiojant kubo sienas, lieka savo vietoje, todėl šių 6 langelių galima nepaisyti. Likusius $6 \cdot 9 - 6 = 48$ langelius galima bet kaip sunumeruoti skaičiais nuo 1 iki 48. Jei Rubiko kubo išklotinėje dalį langelių sunumeruosime, kaip parodyta paveikslėlyje, tai kubo sienos su žaliu centriniu langeliu posūkį 90° kampu pagal laikrodžio rodyklę atitiks keitinys
$(1 \quad 2 \quad 3 \quad 4)(5 \quad 6 \quad 7 \quad 8)(9 \quad 10 \quad 11 \quad 12)(13 \quad 14 \quad 15 \quad 16)(17 \quad 18 \quad 19 \quad 20)(21)(22) \ldots (48)$.
Atitinkamiems kitų sienų posūkiams galime priskirti dar penkis keitinius iš S_{48}. Visos įmanomos sandaugos, kur kiekvienas dauginamasis yra vienas iš šių 6 pradinių keitinių, nusakys visas įmanomas Rubiko kubo transformacijas. Šios sandaugos gali įgyti iš viso $43\,252\,003\,274\,489\,856\,000$ skirtingų reikšmių. Tai reiškia, kad sukiodami Rubiko kubo sienas galime gauti būtent tiek skirtingų Rubiko kubo pavidalų.

ANTROJI UŽDUOTIS

1. Nustatykite sandaugas $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 3 & 7 & 6 & 2 & 4 & 1 & 5\end{pmatrix} \cdot \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7\\ 4 & 1 & 3 & 6 & 2 & 7 & 5\end{pmatrix}$ ir $\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14\\ 3 & 12 & 5 & 10 & 2 & 11 & 7 & 9 & 1 & 14 & 4 & 6 & 8 & 13\end{pmatrix} \cdot \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14\\ 4 & 13 & 14 & 6 & 9 & 10 & 2 & 11 & 5 & 12 & 8 & 3 & 1 & 7\end{pmatrix}$.
Abiem atvejais atsakymą užrašykite tiek lentele, tiek ciklais.

2. Nustatykite sandaugą $a^3 \cdot b^2 \cdot a^{-1}$, kur $a = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11\\ 3 & 10 & 8 & 7 & 9 & 1 & 5 & 11 & 2 & 4 & 6\end{pmatrix}$, $b = (1 \quad 6 \quad 3 \quad 11)(2 \quad 7 \quad 5 \quad 8)(4 \quad 10 \quad 9)$. Atsakymą užrašykite tiek lentele, tiek ciklais.

3. Duoti keitiniai $a = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 2 & 4 & 1 & 3 & 5\end{pmatrix}$, $b = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 4 & 3 & 1 & 2 & 6 & 5\end{pmatrix}$, $c = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 5 & 6 & 4 & 3 & 2 & 1\end{pmatrix}$.
Nustatykite keitinio $u \in S_6$ eilę, jei $a \cdot u \cdot b = c$.

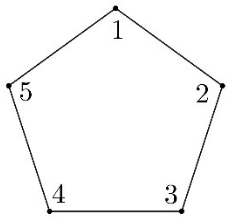
4. Duotas keitinys $a = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15\\ 13 & 11 & 9 & 1 & 14 & 3 & 8 & 4 & 2 & 10 & 15 & 5 & 7 & 12 & 6\end{pmatrix}$.
Nustatykite keitinį a^{5678}. Atsakymą užrašykite lentele.

5. Nustatykite keitinį u^{100}, jei $u \cdot a^{444} = b^{-1}$, $a = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10\\ 8 & 4 & 7 & 1 & 10 & 2 & 3 & 9 & 5 & 6\end{pmatrix}$ ir $b = (1 \quad 5 \quad 6 \quad 4 \quad 9)(2 \quad 10 \quad 7)(3 \quad 8)$. Atsakymą užrašykite ciklais.

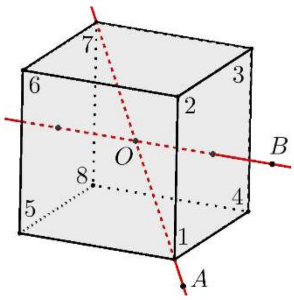
6. Nustatykite keitinio $(a^{201} \cdot b^{210})^{102} \cdot c$ eilę, kai
$a = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13\\ 4 & 11 & 5 & 1 & 13 & 7 & 8 & 2 & 3 & 12 & 10 & 9 & 6\end{pmatrix}$, $b = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13\\ 4 & 3 & 6 & 11 & 10 & 9 & 1 & 13 & 7 & 8 & 2 & 5 & 12\end{pmatrix}$,
$c = (1 \quad 2 \quad 3 \quad 4 \quad 5)(6 \quad 7 \quad 11 \quad 12)(8)(9)(10)(13)$.

7. Nustatykite, kiek grupėje S_{10} yra keitinių, kurių eilė lygi 14.

8. Nustatykite, kiek grupėje S_6 yra keitinių, kurių eilė lygi 2.



9. Vieną pavaizduoto taisyklingojo penkiakampio (su centru O) simetriją galima apibūdinti tokia trijų veiksmų seka: pasukame penkiakampį 144° kampu aplink O pagal laikrodžio rodyklę; simetriškai atvaizduojame jį vertikalios tiesės, einančios per O, atžvilgiu; pasukame jį 72° kampu aplink O prieš laikrodžio rodyklę. Ciklais užrašykite grupės S_5 keitinius, kurie apibūdina šiuos tris veiksmus, ir šių keitinių sandaugą, kuri apibūdina duotąją penkiakampio simetriją. Kokiu vienu veiksmu (posūkio arba simetriško atvaizdavimo tiesės atžvilgiu) galima nusakyti šią simetriją?



10. Pavaizduotas kubas su centru O. Kubo simetriją U, kai šis pasukamas 120° kampu aplink tiesę OA pagal laikrodžio rodyklę, žiūrint iš taško A, apibūdina keitinys $a \in S_8$. Simetriją V, kai kubas pasukamas 90° kampu aplink tiesę OB (statmeną kubo sienai) pagal laikrodžio rodyklę, žiūrint iš taško B, apibūdina keitinys $b \in S_8$. Kubas transformuotas, simetrijas pritaikant tokia tvarka: UVUUVVUUUVVVUUUUUVVVVV. (Sukant kubą, tiesės OA ir OB nejuda.) Ši kubo transformacija W – vėlgi jo simetrija. Užrašykite jos keitinį c kaip keitinių a ir b laipsnių sandaugą. Ciklais užrašykite c bei įvardykite, kokiu vienu posūkio veiksmu galima nusakyti W.

Užduoties sprendimus prašome išsiųsti iki **2022 m. vasario 4 d.** mokyklos adresu: Lietuvos jaunųjų matematikų mokykla, Matematinio švietimo centras, VU Matematikos ir informatikos fakultetas, Naugarduko g. 24, LT-03225 Vilnius. Mūsų mokyklos interneto svetainės adresas: http://mif.vu.lt/matematikos-olimpiados/ljmm/

LIETUVOS JAUNŲJŲ MATEMATIKŲ MOKYKLOS TARYBA