2 paskaita. *Lyginiai.Likinių klasių žiedas. Baigtiniai kūnai. Pirmojo laipsnio lyginių sprendimas.*

Apibrėžimas. *Tegu $m \geq 1$ yra sveikasis skaičius. Sakysime, kad du sveikieji skaičiai a ir b lygsta moduliu m, jeigu skaičius $a - b$ dalijasi iš m. Rašysime: $a \equiv b \pmod{m}$. Šį užrašą vadinsime lyginiu.*

Pastaba. Su visais $a, b \in \mathbf{Z}$ yra teisinga $a \equiv b \pmod{1}$.

Pavyzdys. $a \equiv b \pmod{2}$ tada ir tik tada, kada arba a ir b yra abu lyginiai, arba abu yra nelyginiai skaičiai.

Pagringinės lyginių savybės yra šios:

1. *Refleksyvumas: su visais* $a \in \mathbf{Z}$, $a \equiv a \pmod{m}$.

2. *Simetriškumas:* $\left.\begin{array}{c} a, b \in \mathbf{Z} \\ a \equiv b \pmod{m} \end{array}\right\} \Longleftrightarrow b \equiv a \pmod{m}$.

3. *Tranzityvumas:* $\left.\begin{array}{c} a, b, c \in \mathbf{Z} \\ a \equiv b \pmod{m} \\ b \equiv c \pmod{m} \end{array}\right\} \Longrightarrow a \equiv c \pmod{m}$.

4. $\left.\begin{array}{c} a, b, c, d \in \mathbf{Z} \\ a \equiv c \pmod{m} \\ b \equiv d \pmod{m} \end{array}\right\} \Longrightarrow a \pm b \equiv c \pm d \pmod{m}$.

5. $\left.\begin{array}{c} a, b, c, d \in \mathbf{Z} \\ a \equiv c \pmod{m} \\ b \equiv d \pmod{m} \end{array}\right\} \Longleftrightarrow a \cdot b \equiv c \cdot d \pmod{m}$.

6. $\left.\begin{array}{c} a, b \in \mathbf{Z} \\ m, c > 1 \\ ac \equiv bc \pmod{mc} \end{array}\right\} \Longrightarrow a \equiv b \pmod{m}$.

7. $\left.\begin{array}{c} a, b \in \mathbf{Z} \\ (m, c) = 1 \\ ac \equiv bc \pmod{m} \end{array}\right\} \Longrightarrow a \equiv b \pmod{m}$.

Pastaba. $3 \equiv 15 \pmod{6} \not\Longrightarrow 1 \equiv 5 \pmod{6}$, nes $1 \not\equiv 5 \pmod{6}$.

8. *Kiekvienas sveikasis skaičius* a *lygsta mod* $m > 1$ *su vienu ir tik vienu skaičiumi iš aibės* $\{0, 1, 2, ..., m-1\}$.

Likinių klasės.

Apibrėžimas. *Tegu* $a, m \in \mathbf{Z}$, *ir* $m > 1$. *Sveikųjų skaičių aibės* $\mathbf{Z}$ *poaibį*

$$\{b \in \mathbf{Z} | b \equiv a \,(\mathrm{mod}\, m)\}$$

vadinsime **likinių klase moduliu** m, *kuriai atstovauja* a, *arba tiesiog likinių klase, ir žymėsime* ${}_mK_a$, *arba* K_a, *arba* $\bar{a}$.

Pavyzdžiai. 1. $m = 2, a = 0 : K_0 = \bar{0} = \{b \in \mathbf{Z} | b \equiv 0 \,(\mathrm{mod}\, 2)\} = 2\mathbf{Z}$ yra visų lyginių skaičių poaibis.

2. $m = 2, a = 1 : K_1 = \bar{1} = \{b \in \mathbf{Z} | b \equiv 1 \,(\mathrm{mod}\, 2)\}$ yra visų nelyginių skaičių poaibis.

3. $m = 2, a = 2 : K_2 = \bar{2} = \{b \in \mathbf{Z} | b \equiv 2 \,(\mathrm{mod}\, 2)\} = 2\mathbf{Z}$ yra visų lyginių skaičių poaibis.

Svarbiausios **likinių klasių savybės** yra šios:

1. *Refleksyvumas*: $a \in \mathbf{Z} \Longrightarrow a \in K_a$.

2. *Simetriškumas*: $a \in K_b \Longrightarrow b \in K_a$.

3. *Tranzityvumas*: $\left.\begin{array}{c} a \in K_b \\ b \in K_c \end{array}\right\} \Longrightarrow a \in K_c$.

4. *Tegu* $m > 1$. *Tada likinių klasės* $K_0, K_1, K_2, ..., K_{m-1}$ *yra sveikųjų skaičių aibės* $\mathbf{Z}$ ***skaidinys***, *t.y.*

(a) $\mathbf{Z} = K_0 \cup K_1 \cup K_2 \cup ... \cup K_{m-1}$;

(b) *jeigu* $K_a \cap K_b \neq \emptyset$, tai $K_a = K_b$, $0 \leq a, b \leq m-1$.

Apibrėžimas. *Tegu* $m > 1$. Aibę $\{K_0, K_1, K_2, ..., K_{m-1}\}$ *vadinsime likinių klasių aibe moduliu* m *ir žymėsime* $\mathbf{Z}_m$.

Aibėje $\mathbf{Z}_m$ galima apibrėžti šiuos veiksmus.

Apibrėžimas. $\left.\begin{array}{c} K', K'' \in \mathbf{Z}_m \\ a \in K', b \in K'' \end{array}\right\}$, *tada* $\begin{array}{c} K' + K'' \stackrel{\text{def}}{=} K_{a+b} \\ K' \cdot K'' \stackrel{\text{def}}{=} K_{a\cdot b} \end{array}$.

Teiginys. *Sudėties ir sandaugos veiksmai likinių klasėms apibrėžti korektiškai, t.y. jie nepriklauso nuo klasių atstovų a ir b parinkimo.*

Įrodymas. Tegu $a, a' \in K'$ ir $b, b' \in K''$, t.y. $a \equiv a' \pmod m$ ir $b \equiv b' \pmod m$. Tada tiek $a + b = a' + b' \pmod m$, tiek $a \cdot b \equiv a' \cdot b' \pmod m$ ir todėl $K_{a+b} = K_{a'+b'}$ ir $K_{a\cdot b} = K_{a'\cdot b'}$.

Įrodyta.

Pavyzdžiai. Pateiksime veiksmų lenteles $\mathbf{Z}_3$ ir daugybos lentelę $\mathbf{Z}_6$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Veiksmų su likinių klasėmis savybės.

Tegu $\bar{a}, \bar{b}, \bar{c} \in \mathbf{Z}_m$.

1. Sudėties asociatyvumas: $\left(\bar{a} + \bar{b}\right) + \bar{c} = \bar{a} + \left(\bar{b} + \bar{c}\right)$.

2. Neutralaus elemento sudėties atžvilgiu egzistavimas: egzistuoja tokia klasė $\bar{0}$, kad $\bar{a} + \bar{0} = \bar{a}$. Ši klasė vadinama nuline klase.

3. Atvirkštinės klasės sudėties atžvilgiu egzistavimas: su visais $\bar{a}$ egzistuoja toks $\bar{b}$, kad $\bar{a} + \bar{b} = \bar{0}$. Elementas $\bar{b}$ vadinamas atvirkštiniu elementui $\bar{a}$ sudėties atžvilgiu ir žymimas: $-\bar{a}$.

4. Sudėties komutatyvumas: $\bar{a} + \bar{b} = \bar{b} + \bar{a}$.

5. Sandaugos asociatyvumas: $\left(\bar{a} \cdot \bar{b}\right) \cdot \bar{c} = \bar{a} \cdot \left(\bar{b} \cdot \bar{c}\right)$.

6. Sandaugos komutatyvumas: $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$.

7. Neutralaus elemento sandaugos atžvilgiu egzistavimas: egzistuoja tokia klasė $\bar{1}$, kad $\bar{a} \cdot \bar{1} = \bar{a}$. Ši klasė vadinama nuline klase.

8. Distributyvumas: $\begin{array}{l} \bar{a} \cdot \left(\bar{b} + \bar{c}\right) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} \\ \left(\bar{a} + \bar{b}\right) \cdot \bar{c} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c} \end{array}.$

Algebrinės struktūros.

Apibrėžimai. 1.Aibė, kurioje apibrėžtas sudėties veiksmas ir teisingos 1-3 savybės, vadinama **adicine grupe** (arba tiesiog, **grupe**); jeigu teisinga ir 4 savybė, tai vadiname **komutatyviąja grupe**(analogiškai yra apibrėžiama grupė sandaugos veiksmo atžvilgiu arba **multiplikacinė grupė**).

2. Aibė, kurioje apibrėžti ir sudėties, ir sandaugos veiksmai ir

- teisingos 1-5 ir 8 savybės, vadinama **žiedu**;
- teisingos 1-6 ir 8 savybės, vadinama **komutatyviu žiedu**;
- teisingos 1-5 ir7,8 savybės, vadinama **žiedu su vienetu.**

3. Tegu $A-$ komutatyvus žiedas su vienetu (teisingos 1-8 savybės). Jeigu elementui $\alpha \in A$ egzistuoja toks elementas $\beta \in A$, kad $\alpha \cdot \beta = \bar{1}$ ($\bar{1}-$ neutralusis A elementas sandaugos atžvilgiu), tai sakome, kad elementas α turi atvirkštinį sandaugos atžvilgiu ir žymime $\beta = \alpha^{-1}$. Jeigu visi nenuliniai komutatyvaus su vienetu žiedo elementai turi atvirkštinius sandaugos atžvilgiu, tai toks žiedas vadinamas **kūnu**.

Pavyzdžiai. 1. Realiųjų skaičių aibė $\mathbf{R}$, racionaliųjų skaičių aibė $\mathbf{Q}$ yra kūnai.

2. Sveikųjų skaičių aibė $\mathbf{Z}$ yra komutatyvus žiedas su vienetu, bet ne kūnas, nes visi sveikieji skaičiai $\neq \pm 1$ neturi atvirkštinių sandaugos atžvilgiu.

3. Lyginių sveikųjų skaičių aibė $2\mathbf{Z}$ yra komutatyvus žiedas be vieneto, nes 1 yra nelyginis skaičius.

4. Likinių moduliu m klasių aibė $\mathbf{Z}_m$ yra komutatyvus žiedas su vienetu, bet ne visada kūnas, pavyzdžiui $\mathbf{Z}_2, \mathbf{Z}_3$ yra kūnai, bet $\mathbf{Z}_4$ nėra kūnas, nes $\bar{2} \cdot \bar{1} = \bar{2} \neq \bar{1}$; $\bar{2} \cdot \bar{2} = \bar{0} \neq \bar{1}$; $\bar{2} \cdot \bar{3} = \bar{2} \neq \bar{1}$.

Nustatysime sąlygas, kurioms esant $\mathbf{Z}_m$ yra kūnas. Pradėsime apibrėžimu.

Apibrėžimas. *Likinių moduliu m klasė K vadinama **primityviąja klase**, jeigu egzistuoja toks $a \in K$, kad $(a, m) = 1$.*

Lema. *Primityvioje klasėse moduliu m visi skaičiai yra tarpusavyje pirminiai* *su m.*

Įrodymas. Tegu $K-$ primityvioji klasė moduliu m ir a- toks šios klasės skaičius, kad $(a,m)=1$, t.y. $ax+my=1$, čia $x,y\in \mathbf{Z}$. Jei $b\in K$, tai $a\equiv b\,(\mathrm{mod}\,m)$ ir $a-b=mt$ su $t\in\mathbf{Z}$, ir $a=b+mt$. Tada $ax+my=(b+mt)\,x+my=bx+m\,(tx+y)=1$ ir todėl $(b,m)=1$.

Įrodyta.

Teorema. *Likinių moduliu m klasė K yra primityvioji tada ir tik tada, kada K turi atvirkštinę sandaugos atžvilgiu klasę žiede Z_m.*

Įrodymas. Tegu $K-$ primityvioji klasė moduliu m ir $a\in K$. Tada $K=K_a$ ir $(a,m)=1$, t.y. $ax+my=1$. Turime

$$\begin{gathered} K_{ax+my}=K_1 \\ K_aK_x+K_mK_y=K_1 \\ K_aK_x=K_1 \text{ , nes } K_m=K_0. \end{gathered}$$

Priešingai, jei klasė K_a turi atvirkštinę klasę K_b, t.y. $K_a\cdot K_b=K_1$, tai

$$\begin{gathered} K_{ab}=K_1 \\ ab-1=mt \text{ , čia } t \text{ - sveikas skaičius} \\ ab-mt=1 \\ (a,m)=1. \end{gathered}$$

Įrodyta.

Teorema. *Žiedas $\mathbf{Z}_m$ yra kūnas tada ir tik tada, kada m yra pirminis skaičius.*

Įrodymas. Tegu skaičius $m-$ pirminis. Tada $(1,m)=(2,m)=\cdots=(m-1,m)=1$ ir todėl visos nenulinės klasės moduliu m yra primityviosios ir turi atvirkštines klases.

Tegu $m-$ sudėtinis skaičius, t.y. $m=a\cdot b$, čia $a>1$ ir $b>1$. Tada nenulinė klasė K_a nėra primityvi, nes $(a,m)=a>1$.

Įrodyta.

Lyginio $ax\equiv b\,(\mathrm{mod}\,m)$ sprendimas.

Nagrinėkime du atvejus: $(a,m)=1$ ir $(a,m)=d>1$.

1. $(a,m)=1$.

Šiuo atveju, naudodamiesi Euklido algoritmu, galime rasti tokius $c, q \in \mathbf{Z}$, kad $ac + mq = 1$. Tada

$$abc + mbq = b \Rightarrow abc = b - mbq \Rightarrow a\,(bc) \equiv b\,(\mathrm{mod}\, m)\,.$$

Gavome, kad $x_0 = bc$ yra lyginio sprendinys.

Tegu dabar $x = x_1$ yra kitas šio lyginio sprendinys, t.y. $ax_1 \equiv b\,(\mathrm{mod}\, m)$. Tada $\left.\begin{array}{c} ax_0 \equiv ax_1\,(\mathrm{mod}\, m) \\ (a, m) = 1 \end{array}\right\} \Rightarrow x_0 \equiv x_1\,(\mathrm{mod}\, m)$.

Iš kitos pusės, jeigu $y \equiv x_0\,(\mathrm{mod}\, m)$, tai $ay \equiv ax_0 \equiv b\,(\mathrm{mod}\, m)$ ir todėl y yra lyginio sprendinys.

Taigi, jeigu x_0 yra lyginio sprendinys, tai kitais lyginio sprendiniais yra skaičiai iš ${}_mK_{x_0}$ ir tik jie.

2. $(a, m) = d > 1$.

Tam, kad lyginys $ax \equiv b\,(\mathrm{mod}\, m)$ turėtų sprendinį būtina, kad b dalytųsi iš d.

Tikrai, jeigu $x = x_1$ yra lyginio sprendinys, tai

$$\left.\begin{array}{c} ax_1 \equiv b\,(\mathrm{mod}\, m) \\ (a, m) = d \end{array}\right\} \Rightarrow \left.\begin{array}{c} ax_1 - b = mq, q \in \mathbf{Z} \\ a \vdots d, m \vdots d \end{array}\right\} \Rightarrow \left.\begin{array}{c} ax_1 - mq = b \\ a = a_1 d; m = m_1 d \end{array}\right\}$$

$\Rightarrow a_1 d x_1 - m_1 d q = b \Rightarrow d\,(a_1 x_1 - m_1 q) = b \Rightarrow b \vdots d$.

Taigi, turime $\left.\begin{array}{c} b = b_1 d \\ m = m_1 d \\ a_1 = a_1 d \end{array}\right\} \Rightarrow a_1 d x \equiv b_1 d\,(\mathrm{mod}\, m_1 d) \Longleftrightarrow a_1 x \equiv b_1\,(\mathrm{mod}\, m_1)$ ir $(a_1, m_1) = 1$.

Tegu dabar $x = x_1$ yra lyginio $a_1 x \equiv b_1\,(\mathrm{mod}\, m_1)$ sprendinys. Tada lyginio $ax \equiv b\,(\mathrm{mod}\, m)$ skirtingais sprendiniais mod m yra $x_1, x_1 + \frac{m}{d}, x_1 + 2 \cdot \frac{m}{d}, ..., x_1 + (d-1)\,\frac{m}{d}$, visi sprendiniai yra klasėse ${}_mK_{x_1}, {}_mK_{x_1 + \frac{m}{d}}, ..., {}_mK_{x_1 + (d-1)\frac{m}{d}}$.

Pavyzdys.

$$\begin{gathered} 6x \equiv 3\,(\mathrm{mod}\, 15)\,,\ (6, 15) = 3 = d; \\ 2x \equiv 1\,(\mathrm{mod}\, 5)\,,\ (2, 5) = 1; \\ 2 \cdot 3 \equiv 1\,(\mathrm{mod}\, 5)\,,\ \text{nes } 2 \cdot 3 + 5 \cdot (-1) = 1. \end{gathered}$$

Gavome, kad lyginio sprendiniai yra $x_1 = 3$, $x_1 + \frac{m}{d} = 3 + 5 = 8, x_1 + 2 \cdot \frac{m}{d} = 3 + 10 = 3 + 10 = 13$. Visi sprendiniai yra klasėse ${}_{15}K_3, {}_{15}K_8, {}_{15}K_{13}$.