2 paskaita.
*Lyginiai.*

**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 $a, b \in Z$ 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 $a \in Z$ , $a \equiv a \pmod{m}$.

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

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

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

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

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

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

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 $a, m \in Z$, ir $m > 1$. Sveikųjų skaičių aibės $Z$ poaibį

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

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

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

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

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

Svarbiausios **likinių klasių savybės** yra šios:

1. Refleksyvumas: $a \in Z \Longrightarrow a \in K_a$.

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

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

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

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

$(b)$ 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 $Z_m$.

Aibėje $Z_m$ galima apibrėžti šiuos veiksmus.

**Apibrėžimas.** $\left.\begin{array}{c} K', K'' \in Z_m \\ a \in K', b \in K'' \end{array}\right\}$, 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.**[...........]

**Pavyzdžiai.**[.........]

**Veiksmų su likinių klasėmis savybės.**

Tegu $\bar{a}, \bar{b}, \bar{c} \in Z_m$.

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 $\bar{a} + \bar{0} = \alpha$. 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: $\begin{array}{c} \bar{a} \cdot \left(\bar{b} + \bar{c}\right) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} \\ \left(\bar{a} + \bar{b}\right) \cdot \bar{c} = \bar{a} \cdot \bar{c} + \bar{b} \cdot \bar{c} \end{array}$.

*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 $\alpha$ 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 $R$, racionaliųjų skaičių aibė $Q$ yra kūnai.

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

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

4. Liekanų moduliu $m$ klasių aibė $Z_m$ yra komutatyvus žiedas su vienetu, bet ne visada kūnas, pavyzdžiui $Z_2, Z_3$ yra kūnai, bet $Z_4$ 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 $Z_m$ yra kūnas. Pradėsime apibrėžimu.

**Apibrėžimas.** Liekanų 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 $m$.

Be įrodymo.

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

Be įrodymo.

**Teorema.** Žiedas $Z_m$ yra kūnas tada ir tik tada, kada $m$ yra pirminis skaičius.

**Įrodymas.**[...........]

*Primityviųjų klasių multiplikacinė grupė.*

Tegu $U_m$ yra primityviųjų klasių moduliu $m$ aibė, t.y.

$$U_m = \{a | \, (a, m) = 1, 0 \leq a \leq m - 1\} .$$

Šios aibės elementų skaičių vadiname Oilerio funkcijos $\varphi$ $m$ reikšme : $\varphi(m)$. Pavyzdžiui, kai $p-$ pirminis skaičius, tai $\varphi(p) = p-1$. Jeigu skaičiaus $m$ kanoninis skaidinys yra $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, tai $\varphi(m) = m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_s}\right)$.

**Teiginys.** Aibė $U_m$ sandaugos atžvilgiu sudaro multiplikacinę grupę.
Be įrodymo.

Dabar be įrodymų pateiksime klasikines skaičių teoremas.

**Oilerio teorema.** Jeigu $(a, m) = 1$, tai $a^{\varphi(m)} \equiv 1 \pmod{m}$.

**Išvada.** Jeigu $(a, m) = 1$, tai $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$.

**Mažoji Ferma teorema.** Jeigu $p-$ pirminis skaičius, o $a$ nesidalija iš $p$, tai $a^{p-1} \equiv 1 \pmod{m}$.

**Vilsono teorema.** Skaičius $p$ yra pirminis tada ir tik tada, kada $(p-1)! \equiv -1 \pmod{p}$.

Naudodamiesi Vilsono teorema galima sukonstruoti funkciją

$$f(m) = \sin\left(\frac{\pi \cdot ((m-1)!+1)}{m}\right) = \left[\begin{array}{c} 0, \text{ jeigu } m - \text{ pirminis} \\ \neq 0, \text{ jeigu } m - \text{ sudėtinis} \end{array}\right. .$$

Tai savotiškas pirminio skaičiaus testas, tiesa praktiškai netaikomas, nes tenka skaičiuoti $(m-1)!$, o tai labai didelis skaičius net esant pakankamai mažiems $m$.
Baigsime šį skyrių lyginių ir lyginių sistemų sprendimu.

**Teorema( kinų teorema liekanoms).** Tegu $m_1, m_2, ..., m_k$ yra poromis tarpusavyje pirminiai skaičiai $> 1$ , t.y. $(m_i, m_j) = 1$, kai $i \neq j$, ir tegu $M = m_1 \cdot m_2 \cdots m_k$. Tada

(1) lyginių sistema $\left\{\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\cdots \\ x \equiv a_k \pmod{m_k} \end{array}\right.$ turi sprendinį $x = x_1$;

(2) jeigu $x = x_2$ yra kitas sistemos sprendinys, tai $x_1 \equiv x_2 \pmod{M}$.

Įrodymas. [..........]

*Lyginio* $ax \equiv b \pmod m$ *sprendimas.*

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

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

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

$$abc + mbq = b \Rightarrow abc = b - mbq \Rightarrow a(bc) \equiv b \pmod m.$$

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

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

Iš kitos pusės, jeigu $y \equiv x_0 \pmod m$, tai $ay \equiv ax_0 \equiv b \pmod m$ 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 $ax \equiv b \pmod m$ turėtų sprendinį būtina, kad $b$ dalytųsi iš $d$.

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

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

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

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

Tegu dabar $x = x_1$ yra lyginio $a_1 x \equiv b_1 \pmod{m_1}$ sprendinys. Tada lyginio $ax \equiv b \pmod m$ 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.**

$$6x \equiv 3 \pmod{15}, \ (6, 15) = 3 = d;$$

$$2x \equiv 1 \,(\mathrm{mod}\, 5)\,,\ (2,5) = 1;$$
$$2 \cdot 3 \equiv 1 \,(\mathrm{mod}\, 5)\,,\ \text{nes}\ 2 \cdot 3 + 5 \cdot (-1) = 1.$$

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 ${}_{15}K_{3,15}\,K_{8,15}\,K_{13}$.