

## Paskaita 2 (i pratybos)

### Liekamų klasės (aritmetika)

$a \equiv b \pmod{m}$ , jei  $a-b$  dalijasi  
iš  $m$ .

Pv  $11 \equiv 5 \pmod{6}$ ,  $-3 \equiv 18 \pmod{21}$ .

$\mathbb{Z}$  Lyginimas moduliu  $m$  yra  
ekvivalentumo sąryšis

- $\triangle$  1. Refleksyvumas.  $a \equiv a \pmod{m}$ .  
2. Simetriškumas.  $a \equiv b \pmod{m}$   
(*įrodymas!*)  $\Rightarrow b \equiv a \pmod{m}$ .  
3. Transityvumas

$$(a \equiv b \pmod{m}) \wedge (b \equiv c \pmod{m}) \Rightarrow (a \equiv c \pmod{m})$$

Saunama ekvivalentu klases.  
jos īprasta zīmēti

$$a + m\mathbb{Z} \quad ([a]_m, Ka).$$

$$1 + 5\mathbb{Z} = \{1, 1 \pm 5, 1 \pm 2.5, \dots\}$$

1, 6, -4, 11, -9, ...

1) Ja klasē vārda, bet galimē  
nosoloti bet kuru klases elementu  
kaps vārda.

Faktoriāle

$(A|S)$  zīmēti.

Tada  ~~$\mathbb{Z} | m\mathbb{Z}$~~   $\mathbb{Z} | m\mathbb{Z}$ . ja  
faktoriāle  
likums mod m klases arbi.

I. Ja šurme līgumē

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m}, \quad \text{tai}$$

teirings šedgimā:

- 1)  $-a \equiv -b \pmod{m}$
- 2)  $a + c \equiv b + d \pmod{m}$
- 3)  $a \cdot c \equiv b \cdot d \pmod{m}$ . (šodēti)

(šodēti?)

$$a - b = mk \Rightarrow a = b + mk$$

Nagrinėjus  $(-a + b)$  skaičių

$$(-a) - (-b)$$

$$-a = -b - mk$$

— pagrindinės lygties

$$-a + b = -mk$$

$\in \mathbb{Z}$ .

$$(-a) - (-b) = -mk = m(-k)$$

$$\Rightarrow -a \equiv -b \pmod{m}$$

Algoritmai. Natūraliųjų skaičių  
Aksiomai. Matematinės indukcijos  
principas

Def. Natūraliųjų skaičių  $\mathbb{N}$  vedusiu  
elementu kuriam netiesiai arba, kuris  
apibrėžtas sąryšiu „eina po“, kuris  
savybės:

P1. Yra toks skaičius (vadiname 1),  
kuris neina po jokio kito skaičiaus.

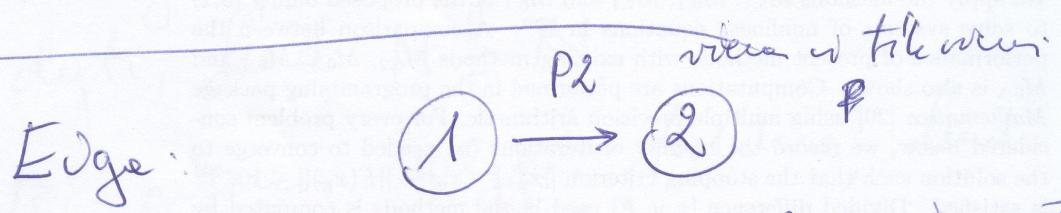
P2. Po kelerius skaičius eina vėnas ir  
šile vėnas skaičius.

P3. Kelerius skaičius eina ne daugiau  
kaip po vieno skaičiaus (1 neuka  
po jėlio k)

(P4) Bet kuris  $N$  poarbes  $M \subset N$ ,  
Turintis sąrybes

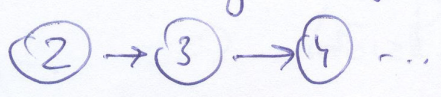
a)  $1 \in M$

b) Jeigu skaičius  $a \in M$ , tai  $a$  po  
jo einantis skaičius priklauso  $M$ ,  
sutaupa su  $N$ .



$P1 \uparrow$   
egzistuoja

$2$  ~~ne~~ eina šilė po  $1$ .  
ir neuka po jėlio k  
skaičius



P4 yra mat induktyvioji pagreidetas. Jeigu  
priešime nuo  $1$  ir po  $\&$  chisine  
~~po~~ skaičius, einauėnis po jam ~~įvardintu~~,  
tai gausime  $N$ .

(Matematinių indukcijos principas).

Teiginys  $T(n)$  yra teisingas  $\forall n \in \mathbb{N}$ ,  
jeigu:

1)  $T(1)$  yra teisingas teiginys  $m'$   
" "

2)  $\forall m \in \mathbb{N} \quad T(m) \text{ teisingas} \Rightarrow T(m+1)$   
~~natūraliajam skaičiui teisingas.~~

$m'$  elementas einauotis po  $m$ .

▶ Pažymėjime  $M \subset \mathbb{N}$  su bet kokiais  
teiginys  $T$  yra teisingas. Reikia įro-  
dyti, kad  $M = \mathbb{N}$ .

1) pirmos sąlygos turime, kad  $1 \in M$ .  
1) antros sąlygos  
Jeigu  $T(m)$  teisingas, tai  $\forall T(m')$  yra  
teisingas  $\Rightarrow$  1) p4 akstomas  $M = \mathbb{N}$ . ▽

Apibendrinimas

T2. (Mažiausio skaičiaus principas)  
Liekvienas netuščias natūraliųjų skaičių  
aibis  $N$  poaibis turi mažiausią elementą.

T3. (Didžiausio skaičiaus principas)  
Kiekvienas netuščias baigtinis natūraliųjų  
skaičių aibis  $N$  poaibis turi didžiausią  
elementą.

T4. (surtįpintas matematinis indukcijos  
principas) - Teorema

1)  $T(1)$  teisinga arba visų teigiamų  
teisingumas

2)  $(\forall k \in N) (T(1) \wedge \dots \wedge T(k)) \Rightarrow T(k+1)$

teisinga teigimui, tai  ~~$\forall n \in N$~~

$(\forall n \in N) T(n)$  yra teisingas

~~Pažymėjus aibį  $A$ , kur~~

$\triangleleft A$  yra aibis ~~te~~ natūraliųjų skaičių, kur  
 $T(n)$  yra teisingas. Parodysime, kad  $A = \emptyset$ .  
Tarkime, kad  $A \neq \emptyset$ .

arip  
~~kur~~

$A \subset \mathbb{N}$ , tai  $\exists$  masivumas  $m \in A$

$m > 1$ , nes  $T(1)$  yra teisingas. ~~bet~~

$(\forall k < m) T(k)$  yra teisingas. Bet

fada is 2 slygos gauname, kad kada  $k = m - 1$ ,

~~kuris~~  $T(m)$  yra teisingas  $\Rightarrow$  pakeiskime  $\Rightarrow$

Indukcija galime pradeti is nuo  $m \neq 1$

1)  $T(m)$  yra teisingas

Par  $k_0 = 2, k_1 = 3$ . ~~Fada  $\forall n \in \mathbb{N}$~~

~~A~~ Nupisime seką

$$k_{n+1} = 3k_n - 2k_{n-1}$$

Parodyti, kad  $k_n = 2^n + 1$

~~$\mathbb{N} = \mathbb{N} + \mathbb{P} = \mathbb{Z}$~~

$$k_0 = 2 = 2^0 + 1$$
$$k_1 = 3 = 2^1 + 1$$

- 8 -

$$k_{n+1} = 3k_n - 2k_{n-1} = 3 \cdot (2^n + 1) - 2(2^{n-1} + 1)$$

$$= 3 \cdot 2^n - 2 \cdot 2^{n-1} + 1 = (3-1) \cdot 2^n + 1 = 2^{n+1} + 1$$

---