Paskaita 2 (ir pratybos)

Liekanų klasės (aritmetika)

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

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

T. Lyginimas moduliu m yra ekvivalentumo sąryšis

Δ 1. Refleksyvumas. $a \equiv a \pmod m$.

2. Simetriškumas. $a \equiv b \pmod m \Rightarrow b \equiv a \pmod m$.

(įrodymas!)

3. Tranzityvumas

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

Gauname ekvivalentumo klases. Jos įprasta žymėti

$a+m\mathbb{Z}$ ($[a]_S$, K_a).

$1+5\mathbb{Z} = \{1,\ 1\pm5,\ 1\pm2\cdot5,\ \dots\}$

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

1 yra klasės vardas, bet galime naudoti bet kurį klasės elementą kaip vardą. | Primename, kad aibę klasių į kurias suskirstome aibę A pagal ekvivalentumo sąryšį S, vadinam

Faktoraibe ir (A|S) žymima.

Tada $\mathbb{Z}|m\mathbb{Z}$ yra faktoraibė liekanų mod m klasių aibė

I. Jei turime lygines

$a\equiv b \mod m$, $c\equiv d \mod m$, tai

teisingi teiginiai:

1) $-a \equiv -b \mod m$
2) $a+c \equiv b+d \mod m$
3) $a\cdot c \equiv b\cdot d \mod m$. (Įrodyti)

Įrodyti!

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

Nagrinėkime $(-a+b)$ skaičių $= (-a)-(-b)$

$$-a=-b-mk$$ iš pagrindinės lygybės

$$-a+b=-mk \in \mathbb{Z}$$

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

$$\Rightarrow -a \equiv -b \mod m.$$

Algoritmai. Natūralieji skaičiai

Aksiomos. Matematinės indukcijos principas

Def. Natūraliaisiais skaičiais ($\mathbb{N}$) vadiname elementus kiekvienos netuščios aibės, kurioje apibrėžtas sąryšis „eina po", turintis savybes:

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

P2. Po kiekvieno skaičiaus eina vienas ir tik vienas skaičius.

P3. Kiekvienas skaičius eina ne daugiau kaip po vieno skaičiaus (1 neina po jokio).

P4. Bet kuris N poaibis $M \subset N$, turintis savybes

a) $1 \in M$

b) jeigu skaičius $a \in M$, tai ir po jo einantis skaičius priklauso M,

sutampa su N.

Eilė: (1) → (2) (P2: vienas ir tik vienas)

P1 ↑ egzistuoja

2 eina tik po 1. ir neina po jokio kito skaičiaus

(2) → (3) → (4) ...

P4 yra matematinės indukcijos pagrindas. Jeigu pradedame nuo 1 ir po to einame į skaičius, einančius po jau įvardintų, tai gauname N.

. (Matematinės indukcijos principas).

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

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

2) $\forall m \in \mathbb{N}$ $T(m)$ teisingas $\Rightarrow T(m+1)$

~~natūralusis skaičius teisingas.~~

" m' elementas einantis po m.

◀ Pažymėkime $M \subset \mathbb{N}$ su kuriais teiginys T yra teisingas. Reikia įrodyti, kad $M = \mathbb{N}$.

Is pirmos sąlygos žinome, kad $1 \in M$.

Is antros sąlygos

Jeigu $T(m)$ teisingas, tai ir $T(m')$ yra teisingas $\Rightarrow$ Is PĮ aksiomos $M = \mathbb{N}$. ▶

Apibendrinimai

T2. (Mažiausio skaičiaus principas) Kiekvienas netuščias natūraliųjų skaičių aibės $\mathbb{N}$ poaibis turi mažiausią elementą.

T3. (Didžiausio skaičiaus principas) Kiekvienas netuščias baigtinis natūraliųjų skaičių aibės $\mathbb{N}$ poaibis turi didžiausią elementą.

T4. (sustiprintas matematinės indukcijos principas). Jeigu

1) $T(1)$ teisingas

2) $(\forall k \in \mathbb{N})(T(1) \wedge \ldots \wedge T(k)) \Rightarrow T(k+1)$ (reiškia visų teiginių teisingumą)

teisingi teiginiai, tai ~~$\forall n \in \mathbb{N}$~~ $(\forall n \in \mathbb{N})\, T(n)$ yra teisingas.

~~Pažymėkime aibę A, kuri~~

△ A yra aibė ~~tų~~ natūraliųjų skaičių, kur $n \in A$ $T(n)$ yra neteisingas. Parodysime, kad $A = \emptyset$. Tarkime, kad $A \neq \emptyset$.

~~Tarkime~~ jeigu $A \subset \mathbb{N}$, tai $\exists$ mažiausias $m \in A$ ~~Tarkime~~ ~~Bet~~

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

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

tada iš 2 sąlygos gauname, kad ir imdami $k = m-1$,

~~turime~~ ~~paro~~ $T(m)$ yra teisingas $\Rightarrow$ prieštaravimas $\square$

Indukcija galime pradėti ir nuo $m \neq 1$

1) $T(m)$ yra teisingas

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

Apibrėžkime seką

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

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

~~$k_0 = 1 + 1 = 2$~~ $k_0 = 2 = 2^0 + 1$

$k_1 = 3 = 2^1 + 1$

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

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