

1 Paskaita.

Matematinės indukcijos metodas. Dalumo su liekana teorema. Didžiausias bendras daliklis. Euklido algoritmas. Tarpusavyje pirminiai skaičiai. Pirminiai skaičiai. Pagrindinė aritmetikos teorema.

Matematinės indukcijos metodas.

Tai vienas dažnai naudojamas būdas teiginiams įrodinėti.

Nagrinėkime sveikųjų skaičių aibę \mathbf{Z} ir tvarkos sąryšį \leq šioje aibėje. .

Sakysime, kad $a \leq b$, jei $b - a \geq 0$. Šis dviejų sveikųjų skaičių sąryšis pasižymi savybėmis:

- i) $a \leq a$ (refleksyvumas);
- ii) $(a \leq b) \wedge (b \leq a) \implies a = b$ (nesimetriškumas);
- iii) $(a \leq b) \wedge (b \leq c) \implies (a \leq c)$ (tranzityvumas).

Tuo atveju, kai $a \leq b$ ir $a \neq b$ rašome $a < b$.

Aišku, kad bet kuriai sveikųjų skaičių porai a ir b teisinga arba $(a \leq b)$, arba $(b < a)$. Todėl sveikųjų skaičių aibę \mathbf{Z} vadina tiesiškai sutvarkyta aibe. Su šia tvarka surišti tam tikri principai. Išvardinkime kai kuriuos iš jų.

Visiško sutvarkymo principas (well-ordering Principle) *sveikiesiems skaičiams*. Tegu a - sveikasis skaičius. Bet kuris netuščias sveikųjų skaičių $\geq a$ ($\leq a$) poaibis turi mažiausią (didžiausią) elementą.

Visiško sutvarkymo principas (well-ordering Principle) *natūraliesiems skaičiams*. Bet kuris netuščias natūraliųjų skaičių poaibis turi mažiausią elementą.

Natūraliuosius skaičius apibrėžia G.Peano(1858-1932) aksiomų sistema. Iš šios sistemos išplaukia taip pat ir

Matematinės indukcijos principas: *tegu su kiekvienu $n \in \mathbf{N}$ turime teiginį $T(n)$. Sakykime, kad žinome būdą teiginio $T(l)$, $\forall l$, teisingumui nustatyti, jeigu teisingi teiginiai $T(k)$ su visais $k < l$ (tame tarpe teisingas $T(1)$ teiginys). Tada teisingas ir teiginys $T(n)$ su visais $n \in \mathbf{N}$.*

Irodymas. Irodysime prieštaros metodu. Nagrinėkime aibę

$S = \{s \mid s \in \mathbf{N}, \text{ teiginys } T(s) \text{ neteisingas}\} \subseteq \mathbf{N}$.

Tegu $S \neq \emptyset$. Tada egzistuoja mažiausias aibės S elementas s_0 , t.y. teiginys $T(s_0)$ neteisingas. Jeigu $s_0 = 1$, tai prieštarauja indukcijos bazei, o jeigu $s_0 > 1$, tai visi teiginiai $T(s), s < s_0$, yra teisingi ir todėl žinome būdą teiginio $T(s_0)$ teisingumui nustatyti.

Prieštaravimas įrodo matematinės indukcijos metodą.

Irodyta.

Dalumo su liekana teorema.

Apibrėžimas. Tegu a ir b yra sveikieji skaičiai. Sakysime, kad a dalijasi iš b (be liekanos), jeigu egzistuoja toks sveikasis skaičius c , kad $a = b \cdot c$. Sakome, kad skaičius b yra a daliklis. Žymėsime $a:b$.

Išvados. 1. Tegu $a, b, c \in \mathbf{Z}$ ir $a:c, b:c$. Tada $(a \pm b):c$.

2. Tegu $a, b, c \in \mathbf{Z}$ ir $a:c$. Tada $ab:c$.

3. Tegu $a \in \mathbf{Z}, a \neq 0$. Tada $0:a$.

4. Tegu $a \in \mathbf{Z}$. Tada $a:1$.

5. Tegu $a \in \mathbf{Z}, 1:a$. Tada $a = \pm 1$.

Visiško sutvarkymo principas. Tegu k_0 – sveikasis skaičius. Bet kuris netuščias sveikųjų skaičių ne mažesnių už k_0 ($\geq k_0$) poaibis turi mažiausią elementą. Bet kuris netuščias sveikųjų skaičių ne didesnių už k_0 ($\leq k_0$) poaibis turi didžiausią elementą.

Teorema (dalybos su liekana teorema). Tegu a ir b – sveikieji skaičiai ir $b \neq 0$. Tada egzistuoja vieninteliai sveikieji skaičiai q ir r su kuriais teisinga lygybė $a = bq + r$, čia $0 \leq r < |b|$.

Irodymas. Nagrinėkime sveikųjų skaičių seką $\{a - k \cdot b \mid k \in \mathbf{Z}\}$:

$$\dots, a - 2b, a - b, a, a + b, a + 2b, \dots$$

Šioje sekoje yra tiek teigiami, tiek neigiami skaičiai. Pagal Visiško sutvarkymo principą neneigiamų (kai $k_0 = 0$) sekos narių posekyje galima rasti mažiausią skaičių $r = a - qb \geq 0$. Tada

$$a = bq + r \text{ ir } 0 \leq r < |b|.$$

Parodysime, kad taip parinktas r yra vienintėtis. Tegu turime

$$a = bq_1 + r_1 \text{ ir } 0 \leq r_1 < |b|$$

ir tegu $r \neq r_1$, beto $r_1 < r$. Tada yra teisinga $0 < r - r_1 < |b|$ ir galioja lygybė

$$r - r_1 = (q_1 - q)b,$$

t.y. $r - r_1$ dalijasi iš b , o tai prieštarauja tam, kad $0 < r - r_1 < |b|$.

Įrodyta.

Apibrėžimas. Tegu $a, b \in \mathbf{Z}$. Sveikasis skaičius $d > 0$ vadinamas skaičių a ir b didžiausiu bendru dalikliu, jeigu

1. $a:d, b:d$.
2. Jeigu $a:c, b:c$, tai $d:c$.

Didžiausio bendro daliklio žymuo: $d = BDD(a, b) = (a, b)$.

Pastaba. $(0, 0) = 0$.

Teorema. Su visais $a, b \in \mathbf{Z}, a \neq 0, b \neq 0$ egzistuoja tokie sveikieji skaičiai x_0 ir y_0 , kad $(a, b) = ax_0 + by_0$.

Įrodymas. Nagrinėkime sveikųjų skaičių aibę $M = \{ax + by | x, y \in \mathbf{Z}\}$. Ši aibė yra netuščia, nes $a, b \in M$. Aibėje M yra tiek teigiami, tiek neigiami skaičiai. Pagal Visiško sutvarkymo principą teigiamų (kai $k_0 = 1$) aibės M poaibyje galima rasti mažiausią skaičių $0 \neq d = ax_0 + by_0$. Parodysime, kad skaičius d ir yra didžiausias bendras a ir b daliklis: $d = (a, b)$. Parašykime skaičių porai a ir d dalybos su liekana lygybę:

$$a = dq + r, 0 \leq r < d.$$

Tada

$$0 \leq r = a - dq = a - (ax_0 + by_0)q = (1 - x_0q)a + (-y_0q)b \in M.$$

Bet d yra mažiausias teigiamas skaičius iš M , todėl $r = 0$, t.y. $a:d$. Panašiai galima parodyti, kad ir $b:d$.

Tegu dabar yra toks sveikas c , kad $a:c$ ir $b:c$. Tada

$$d = \underbrace{a \cdot x_0}_{\text{dalinasi iš } c} + \underbrace{b \cdot y_0}_{\text{dalinasi iš } c} .$$

dalinasi iš c

Pagal apibrėžimą $d = (a, b)$.

Įrodyta.

Nevienintėlis reiškimas: $6 = (12, -30) = 12 \cdot 3 + (-30) \cdot 1 = 12 \cdot (-2) + (-30) \cdot (-1)$.

Euklido algoritmas BDD skaičiavimui. Turime skaičius a ir $b, b \neq 0$. Rašysime dalybos su liekana teoremą:

Tegu $a_0 = a$ ir $a_1 = b$. Tada

$$\begin{aligned} a_0 &= a_1 q_1 + a_2 & 0 < a_2 < |a_1| \\ a_1 &= a_2 q_2 + a_3 & 0 < a_3 < a_2 \\ &\dots & \dots \\ a_{k-2} &= a_{k-1} q_{k-1} + a_k & 0 < a_k < a_{k-1} \\ a_{k-1} &= a_k q_k \end{aligned}$$

Sveikieji skaičiai sudaro mažėjančią seką $|a_1| > a_2 > a_3 > \dots > a_{k-1} > a_k > 0$. Tada $(a, b) = a_k$.

Apibrėžimas. Du skaičiai $a, b \in \mathbf{Z}$ vadinami tarpusavyje pirminiais, jeigu $(a, b) = 1$.

Teorema. Skaičiai $a, b \in \mathbf{Z}$ yra tarpusavyje pirminiai tada ir tik tada, kada egzistuoja tokie $x, y \in \mathbf{Z}$, kad $ax + by = 1$.

Įrodymas. Teiginys iš kairės į dešinę yra teisingas pagal apibrėžimą. Tegu dabar $ax + by = 1$ ir $(a, b) = d$. Tada

$$1 = \underbrace{\underbrace{a \cdot x}_{\text{daliyasi iš } d} + \underbrace{b \cdot y}_{\text{daliyasi iš } d}}_{\text{daliyasi iš } d},$$

t.y. 1 dalijasi iš d ir todėl $d = 1$.

Įrodyta.

Teiginys (tarpusavyje pirminių skaičių savybė). Tegu a_1, \dots, a_m ir b_1, \dots, b_n yra dvi tokios sveikųjų skaičių sekos, kad $(a_i, b_j) = 1$ su visais $1 \leq i \leq m, 1 \leq j \leq n$. Tada $(a_1 \cdots a_m, b_1 \cdots b_n) = 1$.

Be įrodymo.

Išvados. 1. Jeigu $\frac{a}{b}$ yra nesuprastinama trupmena, tai ir trupmena $\frac{a^n}{b^n}$ yra nesuprastinama su visais natūraliaisiais n .

2. Tegu $c \in \mathbf{Z}$ ir $n > 1$. Tada $\sqrt[n]{c}$ yra arba sveikasis skaičius, arba iracionalusis skaičius.

Apibrėžimas. Skaičius $n \in \mathbf{N}, n > 1$ vadinamas pirminiu skaičiumi, jeigu jis turi tik šiuos daliklius: $\pm 1, \pm n$.

Teiginys. Bet kuris sveikasis skaičius, nelygus ± 1 , dalijasi iš kurio nors pirminio skaičiaus.

Teorema (Euklidas). Yra be galo daug pirminių skaičių.

Įrodymas. Įrodysime prieštaros būdu. Sakykime, egzistuoja baigtinis pirminių skaičių kiekis: p_1, p_2, \dots, p_m . Skaičius $n = p_1 p_2 \cdots p_m + 1$ dalijasi iš pirminio, taigi egzistuoja toks $i, 1 \leq i \leq m$, kad $n : p_i$. Tada

$$1 = \underbrace{\underbrace{n}_{\text{daliyasi iš } p_i} - \underbrace{p_1 p_2 \cdots p_m}_{\text{daliyasi iš } p_i}}_{\text{daliyasi iš } p_i},$$

t.y. $1 : p_i$, o tai prieštarauja pirminio skaičiaus apibrėžimui ($p_i > 1$).

Įrodyta.

Pastaba. Pastebėsime, kad pirmieji pavidalo $p_1 p_2 \cdots p_m + 1$ skaičiai yra pirminiai: $2+1 = 3$, $2 \cdot 3 + 1 = 7$, $2 \cdot 3 \cdot 5 + 1 = 31$, $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$. Tačiau skaičius $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ yra sudėtinis.

Teiginys(pirminių skaičių savybė). Tegu a_1, \dots, a_m yra tokia sveikųjų skaičių seka, kad skaičius $a_1 \cdots a_m$ dalijasi iš pirminio p . Tada egzistuoja toks j , $1 \leq j \leq m$, kad a_j dalijasi iš p .

Be įrodymo.

Pagrindinė aritmetikos teorema. Su kiekvienu natūraliuoju $n > 1$ egzistuoja tokie pirminiai p_1, p_2, \dots, p_s (tarp jų gali būti sutampančių), kad $n = p_1 \cdot p_2 \cdot \cdots \cdot p_s$.

Be įrodymo.