Algebros paskaitos informatikams.
Rimantas Grigutis

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) ($a \leq b) \wedge (b \leq a) \Longrightarrow a = b$ (nesimetriškumas) ;

iii) $(a \leq b) \wedge (b \leq c) \Longrightarrow (a \leq c)$ (tranzytivumas) .

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 $(b \leq a)$. Todėl sveikųjų skaičių aibę $\mathbf{Z}$ vadina tiesiškai sutvarkyta aibe. Su šia tvarka surišti tam tikri principai. Išvardinkime kai kuriuos iš jų.

0.1 **Visiško sutvarkymo principas(well-ordering Principle) sveikiesiems skaičiams**. *Tegu k_0- sveikasis skaičius. Bet kuris netuščias sveikųjų skaičių $\geq k_0$ $(\leq k_0)$ poaibis turi mažiausią(didžiausią) elementą.*

0.2 **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

0.3 **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 $n \in \mathbf{N}$.*

Įrodymas.Įrodysime prieštaros metodu. Nagrinėkime aibę

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

Tegu $S \neq \emptyset$. Tada egzituoja 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.

Įrodyta.

Dalumo su liekana teorema.

1.1 **Apibrėžimas**. *Tegu a ir $b \neq 0$ yra sveikieji skaičiai. Sakysime, kad a dalijasi iš b (be liekanos), jeigu egzistiuoja toks sveikasis skaičius c, kad $a = b \cdot c$. Sakome, kad skaičius b yra a daliklis. Žymėsime $a \vdots b$.*

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

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

(3) Tegu $a \in \mathbf{Z}, a \neq 0$. Tada $0 \vdots a$.

(4) Tegu $a \in \mathbf{Z}$. Tada $a \vdots 1$.

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

(6) Tegu $a \vdots b$, $b \vdots a$.Tada $a = \pm b$.

(7) Tegu $a \vdots b, a \neq 0$. Tada $|a| \geq |b|$.

1.3 **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.*

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

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

$$\ldots,\ a - 2b, a - b, a, a + b, a + 2b, \ldots .$$

Šioje sekoje yra tiek teigiami, tiek neigiami skaičiai. Pagal *1.3 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 $r_1 < r$. Tada yra teisinga $0 < r - r_1 < |b|$ ir galioja lygybė

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

Iš čia turime:
arba $r - r_1 = 0$, t.y. $r = r_1$, tada $q_1 = q$ ir vienatinumas įrodytas;

arba $r - r_1 > 0$, t.y. $r - r_1$ dalijasi iš b ir tada $|r - r_1| = r - r_1 \geq |b|$. Bet tai prieštarauja tam, kad $r - r_1 < |b|$.

Įrodyta.

1.5 **Pavyzdžiai**. 1) Kai $a = 15, b = 4$, tai $15 = 4 \cdot 3 + 3$ ir $q = 3, r = 3$.
2) Kai $a = 15, b = -4$, tai $15 = (-4) \cdot (-3) + 3$ ir $q = -3, r = 3$.
3) Kai $a = -15, b = 4$, tai $(-15) = (4) \cdot (-4) + 1$ ir $q = -4, r = 1$.
4) Kai $a = -15, b = -4$, tai $(-15) = (-4) \cdot (4) + 1$ ir $q = -4, r = 1$.

Dalybos su liekana algoritmas

Duota:	$a, b \in N$
Gauta:	$0 < q = a \text{ div } b, 0 < r = a \text{ mod } b : a = bq + r$
1.	$Q := 0, R := a$
2.	Jeigu $R < b$, tai $q = Q, r = R$
	Jeigu $R \geq b$,tai 3.
3.	$R := R - b, Q := Q + 1$ ir 2.

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

1. $a \vdots d, b \vdots d$.

2. Jeigu $a \vdots c . b \vdots c$, *tai* $d \vdots c$.

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

1.7 **Pastaba.** $(0, 0) = 0$,$(0, a) = |a|$

1.8 **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 aibės M teigiamų skaičių (kai $k_0 = 1$)poaibyje galima rasti mažiausią skaičių $d = ax_0 + by_0$. 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

$$0 \leq r = a - dq = a - (ax_0 + by_0)\, q = (1 - x_0 q)\, a + (-y_0 q)\, b \in M.$$

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

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

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

Pagal apibrėžimą $d = (a, b)$.
Įrodyta.

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

1.10 **Euklido algoritmas BDD skaičiavimui.** Turime skaičius a ir $b, b \neq 0$. Rašykime dalybos su liekana teoremą tol kol įvyks dalyba be liekanos.
Jei $a_0 = a$ ir $a_1 = b$, tai

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

Dalyba be liekanos įvyks, nes sveikieji skaičiai sudaro mažėjančią seką $|a_1| > a_2 > a_3 > \cdots > a_{k-1} > a_k > 0$.
Tada $\mathrm{BDD}(a, b) = a_k$.

1.11 **Išplėstinis Euklido algoritmas BDD tiesinei išraiškai rasti.**

$$\begin{gathered}
a_0 = a \cdot 1 + b \cdot 0 \\
a_1 = a \cdot 0 + b \cdot 1 \\
a_2 = a \cdot x_2 + b \cdot y_2 \\
a_3 = a \cdot x_3 + b \cdot y_3 \\
\cdots \\
a_k = a \cdot x_k + b \cdot y_k \\
a_j = a_{j-2} - a_{j-1} q_{j-1} = \\
(a \cdot x_{j-2} + b \cdot y_{j-2}) - (a \cdot x_{j-1} + b \cdot y_{j-1})\, q_{j-1} = \\
a\,(x_{j-2} - q_{j-1} x_{j-1}) + b\,(y_{j-2} - q_{j-1} y_{j-1}) \\
x_j = x_{j-2} - q_{j-1} x_{j-1} \\
y_j = y_{j-2} - q_{j-1} y_{j-1}
\end{gathered}$$

Euklido algoritmas

Duota:	$a, b \in N. a \geq b$
Gauta:	$d = BDD(a, b)$
1.	$A := a, B := b$
2.	$R := A \bmod B$ ir 3.
3.	Jeigu $R = 0$, tai $d = B$
	Jeigu $R \neq 0$, tai 4.
4.	$A := B, B := R$ ir 2.

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

1.13 **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 1.8 Teoremą. Tegu dabar $ax + by = 1$ ir $(a, b) = d$. Tada

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

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

1.14 **Teiginys(tarpusavyje pirminių skaičių savybė).** *Tegu* $a_1, ..., a_m$ *ir* $b_1, ..., b_n$ *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.

1.15 **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.

1.16 **Teorema.** *Jeigu sveikas skaičius* a *dalijasi iš dviejų tarpusavyje pirminių skaičių* m *ir* n, *tai* a *dalijasi ir iš jų sandaugos* mn.

Įrodymas. Skaičius a dalijasi iš m, todėl $a = m \cdot b, b \in \mathbf{Z}$.Skaičiai m ir n yra tarpusavyje pirminiai, todėl pagal 1.13 Teoremą $mx + ny = 1$.
Tada

$$\underbrace{\underbrace{bmx}_{\text{dalijasi iš } n} + \underbrace{bny}_{\text{dalijasi iš } n}}_{\text{dalijasi iš } n} = b,$$

t.y. b dalijasi iš n ir $b = n \cdot c$. Tada $a = mn \cdot c$, t.y. a dalijasi iš mn.
Įrodyta.

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

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

Be įrodymo.

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

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

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

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

1.20 **Pastabos.** (1) 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.

(2) Tegu $\pi(x)-$ pirminių skaičių nedidesnių nei x skaičius. Įrodyta, kad $\lim\limits_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$.
Beto, kai $x \geq 3$, tai $\frac{Ax}{\ln x} < \pi(x) < \frac{Bx}{\ln x}$, čia $A = \frac{1}{2}, B = 2$.
Kai $x \geq 17$, tai $\pi(x) > \frac{x}{\ln x}$, ir kai $x > 1$, tai $\pi(x) < 1,255506 \frac{x}{\ln x}$.
(3) Su visais pirminiais p skaičius $M_p = 2^p - 1$ vadinamas *Merseno skaičiumi.* Žinoma, jeigu M_p yra pirminis, tai ir p yra pirminis. Atvirkštinis teiginys neteisingas, nes, pavyzdžiui, $2^{11} - 1 = 23 \cdot 89$. Didžiausias šiuo metu žinomas pirminis skaičius kaip tik ir yra Merseno skaičius $M(47) = 2^{57885161} - 1$. Tai 17425170- ženklis skaičius, rastas 2013 01 25.

1.21 **Teiginys(pirminių skaičių savybė).** *Tegu $a_1, ..., a_m$ 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.

1.22 **Teiginys**. Jeigu skaičius n dalijasi iš skirtingų pirminių $p_1, ..., p_r$, tai n dalijasi ir iš jų sandaugos $p_1 \cdots p_r$.

Įrodymas. Teiginį įrodysime kai $r = 2$. Jeigu n dalijasi iš p_1, tai $n = p_1 \cdot m$. Bet skaičius $n = p_1 \cdot m$ dalijasi ir iš pirminio p_2, todėl pagal 1.21 Teiginį arba p_1, arba m dalijasi iš p_2. Bet $(p_1, p_2) = 1$, todėl m dalijasi iš p_2, t.y. $m = p_2 \cdot t$ ir $n = (p_1 \cdot p_2) \cdot t$.

Įrodyta.

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

Be įrodymo.