

Diskrečioji matematika, IT I kursas

Pagal Hein'o vadovėlio 2 skyrių
(Panaudoti R.Petuchovo failai)

Prof. Eugenijus Manstavičius

Vilniaus universitetas

2017

II skyrius. Funkcijos

2.1 Funkcijų apibrėžimai ir pavyzdžiai

Ap. Funkcija vadiname atvaizdį

$$f : A \rightarrow B,$$

kuris kiekvienam elementui iš A priskiria vieną vienintelį elementą iš B .

II skyrius. Funkcijos

2.1 Funkcijų apibrėžimai ir pavyzdžiai

Ap. Funkcija vadiname atvaizdį

$$f : A \rightarrow B,$$

kuris kiekvienam elementui iš A priskiria vieną vienintelį elementą iš B .

A vadiname f apibrėžimo sritimi, o B reikšmių sritimi.

II skyrius. Funkcijos

2.1 Funkcijų apibrėžimai ir pavyzdžiai

Ap. Funkcija vadiname atvaizdį

$$f : A \rightarrow B,$$

kuris kiekvienam elementui iš A priskiria vieną vienintelį elementą iš B .

A vadiname f apibrėžimo sritimi, o B reikšmių sritimi.

Jeigu funkcija f elementui $x \in A$ priskiria elementą $y \in B$, rašome

$$f(x) = y.$$

Sakome, kad „ f nuo x yra y “ arba „ f atvaizduoja x į y “.

- ▶ Tarkime $C \subset A$, tada C vaizdu f atžvilgiu vadiname aibę

$$f(C) = \{f(x) \mid x \in C\}.$$

- ▶ Tarkime $C \subset A$, tada C vaizdu f atžvilgiu vadiname aibę

$$f(C) = \{f(x) \mid x \in C\}.$$

- ▶ Funkcijos f įgyjamų reikšmių aibė yra žymima

$$\begin{aligned} \text{range}(f) &= f(A) \\ &= \{f(x) \mid x \in A\}. \end{aligned}$$

- ▶ Tarkime $C \subset A$, tada C vaizdu f atžvilgiu vadiname aibę

$$f(C) = \{f(x) \mid x \in C\}.$$

- ▶ Funkcijos f įgyjamų reikšmių aibė yra žymima

$$\begin{aligned} \text{range}(f) &= f(A) \\ &= \{f(x) \mid x \in A\}. \end{aligned}$$

- ▶ Tegul $D \subset B$. Aibės D pirmavaizdžiu vadiname aibę

$$f^{-1}(D) = \{x \mid f(x) \in D\}.$$

1 pavyzdys. Turime funkciją

$$f : \{a, b, c, d\} \rightarrow \{1, 2, 3\},$$

$f(a) = f(b) = 1$ ir $f(c) = f(d) = 3$. Iš apibrėžimo galime pasakyti, kad

1 pavyzdys. Turime funkciją

$$f : \{a, b, c, d\} \rightarrow \{1, 2, 3\},$$

$f(a) = f(b) = 1$ ir $f(c) = f(d) = 3$. Iš apibrėžimo galime pasakyti, kad

$$\text{range}(f) = \{1, 3\},$$

1 pavyzdys. Turime funkciją

$$f : \{a, b, c, d\} \rightarrow \{1, 2, 3\},$$

$f(a) = f(b) = 1$ ir $f(c) = f(d) = 3$. Iš apibrėžimo galime pasakyti, kad

$$\text{range}(f) = \{1, 3\},$$

$$f(\{a, b\}) = \{1\},$$

1 pavyzdys. Turime funkciją

$$f : \{a, b, c, d\} \rightarrow \{1, 2, 3\},$$

$f(a) = f(b) = 1$ ir $f(c) = f(d) = 3$. Iš apibrėžimo galime pasakyti, kad

$$\text{range}(f) = \{1, 3\},$$

$$f(\{a, b\}) = \{1\},$$

$$f^{-1}(\{2\}) = \emptyset,$$

1 pavyzdys. Turime funkciją

$$f : \{a, b, c, d\} \rightarrow \{1, 2, 3\},$$

$f(a) = f(b) = 1$ ir $f(c) = f(d) = 3$. Iš apibrėžimo galime pasakyti, kad

$$\text{range}(f) = \{1, 3\},$$

$$f(\{a, b\}) = \{1\},$$

$$f^{-1}(\{2\}) = \emptyset,$$

$$f^{-1}(\{1, 2, 3\}) = \{a, b, c, d\}.$$

2 pavyzdys. Tegul $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ir

$$f(x) = 2x.$$

Pažymėkime L ir N lyginių ir nelyginių skaičių aibes. Turime

2 pavyzdys. Tegul $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ir

$$f(x) = 2x.$$

Pažymėkime L ir N lyginių ir nelyginių skaičių aibes. Turime

$$\text{range}(f) = f(\mathbb{Z}) = L,$$

2 pavyzdys. Tegul $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ir

$$f(x) = 2x.$$

Pažymėkime L ir N lyginių ir nelyginių skaičių aibes. Turime

$$\text{range}(f) = f(\mathbb{Z}) = L,$$

$$f(L) = \{4k \mid k \in \mathbb{Z}\},$$

2 pavyzdys. Tegul $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ir

$$f(x) = 2x.$$

Pažymėkime L ir N lyginių ir nelyginių skaičių aibes. Turime

$$\text{range}(f) = f(\mathbb{Z}) = L,$$

$$f(L) = \{4k \mid k \in \mathbb{Z}\},$$

$$f(N) = \{4k + 2 \mid k \in \mathbb{Z}\},$$

2 pavyzdys. Tegul $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ir

$$f(x) = 2x.$$

Pažymėkime L ir N lyginių ir nelyginių skaičių aibes. Turime

$$\text{range}(f) = f(\mathbb{Z}) = L,$$

$$f(L) = \{4k \mid k \in \mathbb{Z}\},$$

$$f(N) = \{4k + 2 \mid k \in \mathbb{Z}\},$$

$$f^{-1}(L) = \mathbb{Z},$$

2 pavyzdys. Tegul $f : \mathbb{Z} \rightarrow \mathbb{Z}$ ir

$$f(x) = 2x.$$

Pažymėkime L ir N lyginių ir nelyginių skaičių aibes. Turime

$$\text{range}(f) = f(\mathbb{Z}) = L,$$

$$f(L) = \{4k \mid k \in \mathbb{Z}\},$$

$$f(N) = \{4k + 2 \mid k \in \mathbb{Z}\},$$

$$f^{-1}(L) = \mathbb{Z},$$

$$f^{-1}(N) = \emptyset.$$

Užduotis. Tegul $f : \mathbb{N} \rightarrow \mathbb{N}$ ir

$$f(x) = x + 1, \text{ jei } x \text{ yra nelyginis,}$$

ir

$$f(x) = x \text{ priešingu atveju.}$$

Apibūdinkite aibes:

$$f(L), \quad f(N), \quad \text{range}(f), \quad f^{-1}(\mathbb{N}), \quad f^{-1}(L), \quad f^{-1}(N).$$

Užduotis. Tegul $f : \mathbb{N} \rightarrow \mathbb{N}$ ir

$$f(x) = x + 1, \text{ jei } x \text{ yra nelyginis,}$$

ir

$$f(x) = x \text{ priešingu atveju.}$$

Apibūdinkite aibes:

$$f(L), \quad f(N), \quad \text{range}(f), \quad f^{-1}(\mathbb{N}), \quad f^{-1}(L), \quad f^{-1}(N).$$

Ats.: $f(L) = L,$

$$f(N) = L - \{0\},$$

$$\text{range}(f) = L,$$

$$f^{-1}(\mathbb{N}) = \mathbb{N},$$

$$f^{-1}(L) = \mathbb{N},$$

$$f^{-1}(N) = \emptyset.$$

„Grindys" ir „lubos" (Floor ir Ceiling)

Funkcijos *Floor* ir *Ceiling* yra $\mathbb{R} \rightarrow \mathbb{Z}$;

$\text{floor}(x)$ - didžiausias sveikasis skaičius $\leq x$,

$\text{ceiling}(x)$ - mažiausias sveikasis skaičius $\geq x$.

Pavyzdžiai:

$$\text{floor}(2.6) = 2,$$

$$\text{floor}(-2.1) = -3,$$

$$\text{ceiling}(2.6) = 3,$$

$$\text{ceiling}(-2.1) = -2.$$

Kiti žymenys: $\text{floor}(x) = \lfloor x \rfloor$, $\text{ceiling}(x) = \lceil x \rceil$.

Skaičiaus „lubos" = skaičiaus „sveikoji dalis".

1 teiginys. Turime, kad

$$-\lfloor x \rfloor = \lceil -x \rceil.$$

Irodymas: Kai $x \in \mathbb{Z}$, tai

$$-\lfloor x \rfloor = -x = \lceil -x \rceil.$$

Jeigu $x \notin \mathbb{Z}$, tai $\exists n \in \mathbb{Z}$ toks, kad

$$n < x < n + 1$$

ir todėl $\lfloor x \rfloor = n$. Padauginę nelygybę iš -1 , gauname

$$-(n + 1) < -x < -n,$$

iš to išplaukia, kad $\lceil -x \rceil = -n$. Todėl $-\lfloor x \rfloor = -n = \lceil -x \rceil$. \square

2 teiginys. Turime, kad

$$\lceil x + 1 \rceil = \lceil x \rceil + 1.$$

Irodymas: Egzistuoja toks $n \in \mathbb{Z}$, kad

$$n < x \leq n + 1.$$

Pridedam vienetą ir gauname

$$n + 1 < x + 1 \leq n + 2.$$

Todėl

$$\lceil x + 1 \rceil = n + 2,$$

kai $\lceil x \rceil = n + 1$. Iš to išplaukia, kad $\lceil x + 1 \rceil = \lceil x \rceil + 1$. □

Didžiausias bendrasis daliklis

Jeigu x ir y yra sveikieji skaičiai ir $x^2 + y^2 \neq 0$, tai

$\gcd(x, y)$ – didžiausias skaičius, kuris dalija x ir y .

Pavyzdžiui, $\gcd(12, 15) = 3$, o $\gcd(-12, -8) = 4$.

Didžiausias bendrasis daliklis

Jeigu x ir y yra sveikieji skaičiai ir $x^2 + y^2 \neq 0$, tai

$\gcd(x, y)$ – didžiausias skaičius, kuris dalija x ir y .

Pavyzdžiui, $\gcd(12, 15) = 3$, o $\gcd(-12, -8) = 4$.

Funkcijos \gcd savybės:

Didžiausias bendrasis daliklis

Jeigu x ir y yra sveikieji skaičiai ir $x^2 + y^2 \neq 0$, tai

$\gcd(x, y)$ – didžiausias skaičius, kuris dalija x ir y .

Pavyzdžiui, $\gcd(12, 15) = 3$, o $\gcd(-12, -8) = 4$.

Funkcijos \gcd savybės:

1. $\gcd(a, b) = \gcd(b, a) = \gcd(a, -b)$.

Didžiausias bendrasis daliklis

Jeigu x ir y yra sveikieji skaičiai ir $x^2 + y^2 \neq 0$, tai

$\gcd(x, y)$ – didžiausias skaičius, kuris dalija x ir y .

Pavyzdžiui, $\gcd(12, 15) = 3$, o $\gcd(-12, -8) = 4$.

Funkcijos \gcd savybės:

1. $\gcd(a, b) = \gcd(b, a) = \gcd(a, -b)$.
2. $\gcd(a, b) = \gcd(a - bq, b)$ su bet kuriuo $q \in \mathbb{Z}$.

Didžiausias bendrasis daliklis

Jeigu x ir y yra sveikieji skaičiai ir $x^2 + y^2 \neq 0$, tai

$\gcd(x, y)$ – didžiausias skaičius, kuris dalija x ir y .

Pavyzdžiui, $\gcd(12, 15) = 3$, o $\gcd(-12, -8) = 4$.

Funkcijos \gcd savybės:

1. $\gcd(a, b) = \gcd(b, a) = \gcd(a, -b)$.
2. $\gcd(a, b) = \gcd(a - bq, b)$ su bet kuriuo $q \in \mathbb{Z}$.
3. $\gcd(a, b) = ma + nb$ su kažkuriais $m, n \in \mathbb{Z}$.

Didžiausias bendrasis daliklis

Jeigu x ir y yra sveikieji skaičiai ir $x^2 + y^2 \neq 0$, tai

$\gcd(x, y)$ – didžiausias skaičius, kuris dalija x ir y .

Pavyzdžiui, $\gcd(12, 15) = 3$, o $\gcd(-12, -8) = 4$.

Funkcijos \gcd savybės:

1. $\gcd(a, b) = \gcd(b, a) = \gcd(a, -b)$.
2. $\gcd(a, b) = \gcd(a - bq, b)$ su bet kuriuo $q \in \mathbb{Z}$.
3. $\gcd(a, b) = ma + nb$ su kažkuriais $m, n \in \mathbb{Z}$.
4. Jeigu $d|ab$ ir $\gcd(d, a) = 1$, tai $d|b$.

Dalybos taisyklė

Tegul $a, b \in \mathbb{Z}$, $b \neq 0$, tada \exists tokie vieninteliai q ir $r \in \mathbb{Z}$, kad

$$a = bq + r,$$

kai $0 \leq r < |b|$.

Dalybos taisyklė

Tegul $a, b \in \mathbb{Z}$, $b \neq 0$, tada \exists tokie vieninteliai q ir $r \in \mathbb{Z}$, kad

$$a = bq + r,$$

kai $0 \leq r < |b|$.

Euklido algoritmas didžiausiam bendrajam dalikliui rasti:

Tarkime $a, b \in \mathbb{N}$, $a \neq 0$ ir $b \neq 0$.

while $b > 0$ **do**

find q, r so that $a = bq + r$ and $0 \leq r < b$;

$a := b$;

$b := r$;

od

Output(a).

Pavyzdys. Rasime $\gcd(189, 33)$:

$$189 = 33 \cdot 5 + 24$$

$$33 = 24 \cdot 1 + 9$$

$$24 = 9 \cdot 2 + 6$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2 + 0$$

Output(3).

Klausimas. Kiek žingsnių vykdys Euklido algoritmas ieškodamas $\gcd(117, 48)$?

Pavyzdys. Rasime $\text{gcd}(189, 33)$:

$$189 = 33 \cdot 5 + 24$$

$$33 = 24 \cdot 1 + 9$$

$$24 = 9 \cdot 2 + 6$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2 + 0$$

Output(3).

Klausimas. Kiek žingsnių vykdys Euklido algoritmas ieškodamas $\text{gcd}(117, 48)$?

Atsakymas: Keturis žingsnius.

Funkcija mod

Tegul $a, b \in \mathbb{Z}$ ir $b > 0$. Pritaikę dalybos taisyklę, gauname

$$a = bq + r,$$

$$0 \leq r < b.$$

Funkcija mod

Tegul $a, b \in \mathbb{Z}$ ir $b > 0$. Pritaikę dalybos taisyklę, gauname

$$a = bq + r,$$

$0 \leq r < b$. Kad išreikštume r per a ir b , išspręsimė lygtį

$$q = a/b - r/b.$$

Funkcija mod

Tegul $a, b \in \mathbb{Z}$ ir $b > 0$. Pritaikę dalybos taisyklę, gauname

$$a = bq + r,$$

$0 \leq r < b$. Kad išreikštume r per a ir b , išspręsimė lygtį

$$q = a/b - r/b.$$

Kadangi $q \in \mathbb{Z}$ ir $0 \leq r/b < 1$, tai $q = \lfloor a/b \rfloor$.

Funkcija mod

Tegul $a, b \in \mathbb{Z}$ ir $b > 0$. Pritaikę dalybos taisyklę, gauname

$$a = bq + r,$$

$0 \leq r < b$. Kad išreikštume r per a ir b , išspręsimė lygtį

$$q = a/b - r/b.$$

Kadangi $q \in \mathbb{Z}$ ir $0 \leq r/b < 1$, tai $q = \lfloor a/b \rfloor$. Gauname

$$r = a - bq = a - b\lfloor a/b \rfloor.$$

Funkcija mod

Tegul $a, b \in \mathbb{Z}$ ir $b > 0$. Pritaikę dalybos taisyklę, gauname

$$a = bq + r,$$

$0 \leq r < b$. Kad išreikštume r per a ir b , išspręsimė lygtį

$$q = a/b - r/b.$$

Kadangi $q \in \mathbb{Z}$ ir $0 \leq r/b < 1$, tai $q = \lfloor a/b \rfloor$. Gauname

$$r = a - bq = a - b\lfloor a/b \rfloor.$$

Skaičius r rašomas kaip $a \bmod b$. Todėl

$$a \bmod b = a - b\lfloor a/b \rfloor.$$

Klausimas. Kokie elementai sudaro aibę $\{x \bmod 5 \mid x \in \mathbb{Z}\}$?

Klausimas. Kokie elementai sudaro aibę $\{x \bmod 5 \mid x \in \mathbb{Z}\}$?

Atsakymas: $\{0, 1, 2, 3, 4\}$.

Klausimas. Kokie elementai sudaro aibę $\{x \bmod 5 \mid x \in \mathbb{Z}\}$?

Atsakymas: $\{0, 1, 2, 3, 4\}$.

Toliau žymėsime

$$\mathbb{N}_n = \{0, 1, \dots, n - 1\}.$$

Klausimas. Kokie elementai sudaro aibę $\{x \bmod 5 \mid x \in \mathbb{Z}\}$?

Atsakymas: $\{0, 1, 2, 3, 4\}$.

Toliau žymėsime

$$\mathbb{N}_n = \{0, 1, \dots, n-1\}.$$

Jeigu n yra fiksuotas, $x \in \mathbb{Z}$, tai

$$\text{range}(x \bmod n) = \mathbb{N}_n.$$

Klausimas. Paryžiuje yra antra nakties. Kiek laiko yra
Portlande? (devynių valandų skirtumas)

Klausimas. Paryžiuje yra antra nakties. Kiek laiko yra Portlande? (devynių valandų skirtumas)

Sprendimas:

12-os valandų laikrodis:

$$\begin{aligned}(2 - 9) \bmod 12 &= (-7) \bmod 12 \\ &= -7 - 12 \lfloor -7/12 \rfloor \\ &= -7 - 12(-1) \\ &= 5;\end{aligned}$$

Klausimas. Paryžiuje yra antra nakties. Kiek laiko yra Portlande? (devynių valandų skirtumas)

Sprendimas:

12-os valandų laikrodis:

$$\begin{aligned}(2 - 9) \pmod{12} &= (-7) \pmod{12} \\ &= -7 - 12 \lfloor -7/12 \rfloor \\ &= -7 - 12(-1) \\ &= 5;\end{aligned}$$

24-ių valandų laikrodis:

$$\begin{aligned}(2 - 9) \pmod{24} &= (-7) \pmod{24} \\ &= -7 - 24 \lfloor -7/24 \rfloor \\ &= -7 - 24(-1) \\ &= 17.\end{aligned}$$

Atsakymas: Penkta valanda dienos.

Užduotis. Parašykite skaičių **13** dvejetainėje sistemoje.

Sprendimas: Kiekvieną $x \in \mathbb{N}$ mes galime užrašyti kaip

$$x = 2 \lfloor x/2 \rfloor + x \bmod 2.$$

Turime algoritmą dvejetainiam skaičiui rasti:

$$\begin{aligned} 13 &= 2 \cdot 6 + 1 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

Atsakymas: 1101.

Logaritmo funkcija

Jeigu x ir b yra teigiami realieji skaičiai ir $b > 1$, tai

$$\log_b x = y$$

reiškia

$$b^y = x.$$

Logaritmo funkcija yra monotoniškai didėjanti, t.y.

$$s < t \implies \log_b s < \log_b t.$$

Logaritmo savybės:

1) $\log_b 1 = 0,$

2) $\log_b b = 1,$

3) $\log_b b^x = x,$

4) $\log_b xy = \log_b x + \log_b y,$

5) $\log_b x^y = y \log_b x,$

6) $\log_a x = (\log_a b)(\log_b x);$ čia $a > 1.$

Užduotis. Įvertinsime $\log_2(5^2 2^5)$, t.y., rasime apatinį ir viršutinį įverčius šiam logaritmui.

$$9 < \log_2(5^2 2^5) = 2 \log_2 5 + 5 < 11,$$

nes $2^2 < 5 < 2^3$. Arba tikslesnis įvertis

$$9 < \log_2(5^2 2^5) = \log_2 5^2 + 5 < 10,$$

nes $2^4 < 5^2 < 2^5$.

2.2 Funkcijų konstravimas

Kompozicija

Ap. Jeigu $f : B \rightarrow C$ ir $g : A \rightarrow B$, tada reiškiny

$$f(g(x))$$

turi prasmę ir yra vadinamas funkcijų f ir g kompozicija.

Rašome

$$f \circ g : A \rightarrow C$$

ir žymime $(f \circ g)(x) = f(g(x))$.

Pavyzdžiai:

$$\text{floor}(\log_2 20) = \text{floor}(4.32) = 4,$$

$$\text{ceiling}(\log_2 20) = \text{ceiling}(4.32) = 5,$$

$$\text{head}(\text{tail}(\langle a, b, c \rangle)) = \text{head}(\langle b, c \rangle) = b.$$

Funkcijos **seq** ir **dist**

Funkcijos **seq** apibrėžimas:

$$\text{seq} : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$$

ir

$$\text{seq}(n) = \langle 0, 1, \dots, n \rangle.$$

Funkcijos **dist** apibrėžimas:

$$\text{dist} : A \times \text{lists}(B) \rightarrow \text{lists}(A \times B)$$

ir

$$\text{dist}(a, \langle x_1, \dots, x_k \rangle) = \langle (a, x_1), \dots, (a, x_k) \rangle.$$

Klausimas. Kaip galime aprašyti funkciją

$$f(x) = \langle 1, 2, \dots, x + 1 \rangle$$

(programavimo požiūriu)?

Klausimas. Kaip galime aprašyti funkciją

$$f(x) = \langle 1, 2, \dots, x + 1 \rangle$$

(programavimo požiūriu)?

Atsakymas: $f(x) = \text{tail}(\text{seq}(x + 1))$.

Klausimas. Kaip galime aprašyti funkciją

$$f(x) = \langle 1, 2, \dots, x + 1 \rangle$$

(programavimo požiūriu)?

Atsakymas: $f(x) = \text{tail}(\text{seq}(x + 1))$.

Klausimas. Kaip galime aprašyti funkciją

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N} \times \mathbb{N})$$

ir

$$f(x) = \langle (x, 1), (x, 2), \dots, (x, x) \rangle$$

naudojant kitas funkcijas?

Klausimas. Kaip galime aprašyti funkciją

$$f(x) = \langle 1, 2, \dots, x + 1 \rangle$$

(programavimo požiūriu)?

Atsakymas: $f(x) = \text{tail}(\text{seq}(x + 1))$.

Klausimas. Kaip galime aprašyti funkciją

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N} \times \mathbb{N})$$

ir

$$f(x) = \langle (x, 1), (x, 2), \dots, (x, x) \rangle$$

naudojant kitas funkcijas?

Atsakymas:

$$f(x) = \text{dist}(x, \text{tail}(\text{seq}(x))) \quad \text{arba} \quad \text{tail}(\text{dist}(x, \text{seq}(x))).$$

Funkcija map

Apibrėžiama poroms $(f, \text{sąrašas})$, čia f - funkcija, apibrėžta sąrašo elementams.

Funkcija **map** paima f -ją f ir sąrašą ir grąžina sąrašą reikšmių, gautų kiekvienam sąrašo elementui pritaikius funkciją f . Taigi,

$$\text{map}(f, \langle x_1, x_2, \dots, x_k \rangle) = \langle f(x_1), \dots, f(x_k) \rangle.$$

Funkcija map

Apibrėžiama poroms $(f, \text{sąrašas})$, čia f - funkcija, apibrėžta sąrašo elementams.

Funkcija **map** paima f -ją f ir sąrašą ir grąžina sąrašą reikšmių, gautų kiekvienam sąrašo elementui pritaikius funkciją f . Taigi,

$$\text{map}(f, \langle x_1, x_2, \dots, x_k \rangle) = \langle f(x_1), \dots, f(x_k) \rangle.$$

Užduotis. Apskaičiuokite, kam bus lygu

$$\text{map}(\text{floor} \circ \log_2, \text{tail}(\text{seq}(8))).$$

Funkcija map

Apibrėžiama poroms $(f, \text{sąrašas})$, čia f - funkcija, apibrėžta sąrašo elementams.

Funkcija **map** paima f -ją ir sąrašą ir grąžina sąrašą reikšmių, gautų kiekvienam sąrašo elementui pritaikius funkciją f . Taigi,

$$\text{map}(f, \langle x_1, x_2, \dots, x_k \rangle) = \langle f(x_1), \dots, f(x_k) \rangle.$$

Užduotis. Apskaičiuokite, kam bus lygu

$$\text{map}(\text{floor} \circ \log_2, \text{tail}(\text{seq}(8))).$$

Atsakymas: $\langle 0, 1, 1, 2, 2, 2, 2, 3 \rangle$.

Užduotis:

Turime

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$$

ir

$$f(n) = \langle 0, 2, 4, \dots, 2n \rangle.$$

Aprašykite f naudodami kitas funkcijas.

Užduotis:

Turime

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$$

ir

$$f(n) = \langle 0, 2, 4, \dots, 2n \rangle.$$

Aprašykite f naudodami kitas funkcijas.

Sprendimas:

$$f(n) = \langle 0, 2, 4, \dots, 2n \rangle$$

Užduotis:

Turime

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$$

ir

$$f(n) = \langle 0, 2, 4, \dots, 2n \rangle.$$

Aprašykite f naudodami kitas funkcijas.

Sprendimas:

$$\begin{aligned} f(n) &= \langle 0, 2, 4, \dots, 2n \rangle \\ &= \langle 2 \cdot 0, 2 \cdot 1, 2 \cdot 2, \dots, 2 \cdot n \rangle \end{aligned}$$

Užduotis:

Turime

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$$

ir

$$f(n) = \langle 0, 2, 4, \dots, 2n \rangle.$$

Aprašykite f naudodami kitas funkcijas.

Sprendimas:

$$\begin{aligned} f(n) &= \langle 0, 2, 4, \dots, 2n \rangle \\ &= \langle 2 \cdot 0, 2 \cdot 1, 2 \cdot 2, \dots, 2 \cdot n \rangle \\ &= \text{map}(\cdot, \langle (2, 0), (2, 1), \dots, (2, n) \rangle) \end{aligned}$$

Užduotis:

Turime

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$$

ir

$$f(n) = \langle 0, 2, 4, \dots, 2n \rangle.$$

Aprašykite f naudodami kitas funkcijas.

Sprendimas:

$$\begin{aligned} f(n) &= \langle 0, 2, 4, \dots, 2n \rangle \\ &= \langle 2 \cdot 0, 2 \cdot 1, 2 \cdot 2, \dots, 2 \cdot n \rangle \\ &= \text{map}(\cdot, \langle (2, 0), (2, 1), \dots, (2, n) \rangle) \\ &= \text{map}(\cdot, \text{dist}(2, \langle 0, 1, 2, \dots, n \rangle)) \end{aligned}$$

Užduotis:

Turime

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$$

ir

$$f(n) = \langle 0, 2, 4, \dots, 2n \rangle.$$

Aprašykite f naudodami kitas funkcijas.

Sprendimas:

$$\begin{aligned} f(n) &= \langle 0, 2, 4, \dots, 2n \rangle \\ &= \langle 2 \cdot 0, 2 \cdot 1, 2 \cdot 2, \dots, 2 \cdot n \rangle \\ &= \text{map}(\cdot, \langle (2, 0), (2, 1), \dots, (2, n) \rangle) \\ &= \text{map}(\cdot, \text{dist}(2, \langle 0, 1, 2, \dots, n \rangle)) \\ &= \text{map}(\cdot, \text{dist}(2, \text{seq}(n))). \end{aligned}$$

Užduotis:

Turime

$$f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$$

ir

$$f(n) = \langle 0, 2, 4, \dots, 2n \rangle.$$

Aprašykite f naudodami kitas funkcijas.

Sprendimas:

$$\begin{aligned} f(n) &= \langle 0, 2, 4, \dots, 2n \rangle \\ &= \langle 2 \cdot 0, 2 \cdot 1, 2 \cdot 2, \dots, 2 \cdot n \rangle \\ &= \text{map}(\cdot, \langle (2, 0), (2, 1), \dots, (2, n) \rangle) \\ &= \text{map}(\cdot, \text{dist}(2, \langle 0, 1, 2, \dots, n \rangle)) \\ &= \text{map}(\cdot, \text{dist}(2, \text{seq}(n))). \end{aligned}$$

Atsakymas: $f(n) = \text{map}(\cdot, \text{dist}(2, \text{seq}(n)))$.

Užduotis:

Aprašykite $f : \mathbb{N} \rightarrow \mathbf{lists}(\mathbb{N})$ kitomis funkcijomis, kai

$$f(n) = \langle 5, 9, \dots, 5 + 4n \rangle.$$

Užduotis:

Aprašykite $f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$ kitomis funkcijomis, kai

$$f(n) = \langle 5, 9, \dots, 5 + 4n \rangle.$$

Sprendimas:

$$f(n) = \langle 5 + 4 \cdot 0, 5 + 4 \cdot 1, 5 + 4 \cdot 2, \dots, 5 + 4 \cdot n \rangle$$

Užduotis:

Aprašykite $f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$ kitomis funkcijomis, kai

$$f(n) = \langle 5, 9, \dots, 5 + 4n \rangle.$$

Sprendimas:

$$\begin{aligned} f(n) &= \langle 5 + 4 \cdot 0, 5 + 4 \cdot 1, 5 + 4 \cdot 2, \dots, 5 + 4 \cdot n \rangle \\ &= \text{map}(+, \langle (5, 4 \cdot 0), (5, 4 \cdot 1), (5, 4 \cdot 2), \dots, (5, 4 \cdot n) \rangle) \end{aligned}$$

Užduotis:

Aprašykite $f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$ kitomis funkcijomis, kai

$$f(n) = \langle 5, 9, \dots, 5 + 4n \rangle.$$

Sprendimas:

$$\begin{aligned} f(n) &= \langle 5 + 4 \cdot 0, 5 + 4 \cdot 1, 5 + 4 \cdot 2, \dots, 5 + 4 \cdot n \rangle \\ &= \text{map}(+, \langle (5, 4 \cdot 0), (5, 4 \cdot 1), (5, 4 \cdot 2), \dots, (5, 4 \cdot n) \rangle) \\ &= \text{map}(+, \text{dist}(5, \langle 4 \cdot 0, 4 \cdot 1, 4 \cdot 2, \dots, 4 \cdot n \rangle)) \end{aligned}$$

Užduotis:

Aprašykite $f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$ kitomis funkcijomis, kai

$$f(n) = \langle 5, 9, \dots, 5 + 4n \rangle.$$

Sprendimas:

$$\begin{aligned} f(n) &= \langle 5 + 4 \cdot 0, 5 + 4 \cdot 1, 5 + 4 \cdot 2, \dots, 5 + 4 \cdot n \rangle \\ &= \text{map}(+, \langle (5, 4 \cdot 0), (5, 4 \cdot 1), (5, 4 \cdot 2), \dots, (5, 4 \cdot n) \rangle) \\ &= \text{map}(+, \text{dist}(5, \langle 4 \cdot 0, 4 \cdot 1, 4 \cdot 2, \dots, 4 \cdot n \rangle)) \\ &= \text{map}(+, \text{dist}(5, \text{map}(\cdot, \text{dist}(4, \langle 0, 1, 2, \dots, n \rangle)))) \end{aligned}$$

Užduotis:

Aprašykite $f : \mathbb{N} \rightarrow \text{lists}(\mathbb{N})$ kitomis funkcijomis, kai

$$f(n) = \langle 5, 9, \dots, 5 + 4n \rangle.$$

Sprendimas:

$$\begin{aligned} f(n) &= \langle 5 + 4 \cdot 0, 5 + 4 \cdot 1, 5 + 4 \cdot 2, \dots, 5 + 4 \cdot n \rangle \\ &= \text{map}(+, \langle (5, 4 \cdot 0), (5, 4 \cdot 1), (5, 4 \cdot 2), \dots, (5, 4 \cdot n) \rangle) \\ &= \text{map}(+, \text{dist}(5, \langle 4 \cdot 0, 4 \cdot 1, 4 \cdot 2, \dots, 4 \cdot n \rangle)) \\ &= \text{map}(+, \text{dist}(5, \text{map}(\cdot, \text{dist}(4, \langle 0, 1, 2, \dots, n \rangle)))) \\ &= \text{map}(+, \text{dist}(5, \text{map}(\cdot, \text{dist}(4, \text{seq}(n)))). \end{aligned}$$

Užduotis:

Aprašykite $f : \mathbb{N}^3 \rightarrow \mathbf{lists}(\mathbb{N})$ per kitas funkcijas, kai

$$f(a, b, n) = \langle a, a + b, a + 2b, \dots, a + nb \rangle.$$

Užduotis:

Aprašykite $f : \mathbb{N}^3 \rightarrow \text{lists}(\mathbb{N})$ per kitas funkcijas, kai

$$f(a, b, n) = \langle a, a + b, a + 2b, \dots, a + nb \rangle.$$

Sprendimas:

Tai paskutinio uždavinio, kuriame turėjome $a = 5$, o $b = 4$, abstrakcija. Todėl

$$f(n) = \text{map}(+, \text{dist}(a, \text{map}(\cdot, \text{dist}(b, \text{seq}(n)))))).$$

2.3 Funkcijų savybės

Tegul $f : A \rightarrow B$ yra funkcija. Yra trys savybės, kuriomis gali pasižymėti f .

2.3 Funkcijų savybės

Tegul $f : A \rightarrow B$ yra funkcija. Yra trys savybės, kuriomis gali pasižymėti f .

Ap. f vadiname injekcija, kai skirtingi elementai iš A atvaizduojami į skirtingus elementus iš B . Kitais žodžiais,

$$x \neq y \quad \Rightarrow \quad f(x) \neq f(y)$$

arba

$$f(x) = f(y) \quad \Rightarrow \quad x = y.$$

2.3 Funkcijų savybės

Tegul $f : A \rightarrow B$ yra funkcija. Yra trys savybės, kuriomis gali pasižymėti f .

Ap. f vadiname injekcija, kai skirtingi elementai iš A atvaizduojami į skirtingus elementus iš B . Kitais žodžiais,

$$x \neq y \Rightarrow f(x) \neq f(y)$$

arba

$$f(x) = f(y) \Rightarrow x = y.$$

Pavyzdys. Tegul $f : \mathbb{N}_8 \rightarrow \mathbb{N}$ ir

$$f(x) = 2x \pmod{8}.$$

Pastebime, kad f yra ne injekcija, nes $f(0) = f(4)$.

1 klausimas. Tegul $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = x^2$. Ar f yra injekcija?

1 klausimas. Tegul $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = x^2$. Ar f yra injekcija?

Atsakymas: Ne, nes $f(2) = f(-2)$.

1 klausimas. Tegul $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = x^2$. Ar f yra injekcija?

Atsakymas: Ne, nes $f(2) = f(-2)$.

2 klausimas. Ar kuri nors iš f-jų \log_2 , floor arba ceiling, apibrėžtų teigiamų skaičių aibėje, yra injekcija?

1 klausimas. Tegul $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = x^2$. Ar f yra injekcija?

Atsakymas: Ne, nes $f(2) = f(-2)$.

2 klausimas. Ar kuri nors iš f-jų \log_2 , floor arba ceiling, apibrėžtų teigiamų skaičių aibėje, yra injekcija?

Atsakymas: \log_2 yra injekcija, bet floor ir ceiling nėra injekcijos.

Ap. Funkcija $f : A \rightarrow B$ yra vadinama siurjekcija, kai

$$\text{range}(f) = B.$$

Kitais žodžiais tariant, kai kiekvienam $b \in B$ egzistuoja toks $a \in A$, kad $b = f(a)$.

Ap. Funkcija $f : A \rightarrow B$ yra vadinama siurjekcija, kai

$$\text{range}(f) = B.$$

Kitais žodžiais tariant, kai kiekvienam $b \in B$ egzistuoja toks $a \in A$, kad $b = f(a)$.

3 klausimas. Jeigu $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = x^2$, ar f yra siurjekcija?

Ap. Funkcija $f : A \rightarrow B$ yra vadinama siurjekcija, kai

$$\text{range}(f) = B.$$

Kitais žodžiais tariant, kai kiekvienam $b \in B$ egzistuoja toks $a \in A$, kad $b = f(a)$.

3 klausimas. Jeigu $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = x^2$, ar f yra siurjekcija?

Atsakymas: Ne, nes, pavyzdžiui, 2 nėra sveiko skaičiaus kvadratas.

Ap. Funkcija $f : A \rightarrow B$ yra vadinama siurjeksija, kai

$$\text{range}(f) = B.$$

Kitais žodžiais tariant, kai kiekvienam $b \in B$ egzistuoja toks $a \in A$, kad $b = f(a)$.

3 klausimas. Jeigu $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = x^2$, ar f yra siurjeksija?

Atsakymas: Ne, nes, pavyzdžiui, 2 nėra sveiko skaičiaus kvadratas.

4 klausimas. Jeigu $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = |x|$, ar f yra siurjeksija, injeksija?

Ap. Funkcija $f : A \rightarrow B$ yra vadinama siurjekcija, kai

$$\text{range}(f) = B.$$

Kitais žodžiais tariant, kai kiekvienam $b \in B$ egzistuoja toks $a \in A$, kad $b = f(a)$.

3 klausimas. Jeigu $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = x^2$, ar f yra siurjekcija?

Atsakymas: Ne, nes, pavyzdžiui, 2 nėra sveiko skaičiaus kvadratas.

4 klausimas. Jeigu $f : \mathbb{Z} \rightarrow \mathbb{N}$ ir $f(x) = |x|$, ar f yra siurjekcija, injekcija?

Atsakymas: Siurjekcija, bet ne injekcija.

Ap. Funkcija vadiname bijekcija, jeigu ji injekcija ir surjekcija.

Ap. Funkcija vadiname bijekcija, jeigu ji injekcija ir surjekcija.

5 klausimas. Jeigu

$$f : \mathbb{N} \rightarrow \{a\}^*$$

ir

$$f(n) = a^n,$$

ar f yra bijekcija?

Ap. Funkcija vadiname bijekcija, jeigu ji injekcija ir siurjekcija.

5 klausimas. Jeigu

$$f : \mathbb{N} \rightarrow \{a\}^*$$

ir

$$f(n) = a^n,$$

ar f yra bijekcija?

Ats.: Taip.

Ap. Funkcija vadiname bijekcija, jeigu ji injekcija ir siurjekcija.

5 klausimas. Jeigu

$$f : \mathbb{N} \rightarrow \{\mathbf{a}\}^*$$

ir

$$f(n) = \mathbf{a}^n,$$

ar f yra bijekcija?

Ats.: Taip.

6 klausimas. Tegul

$$f : \mathbb{R} \rightarrow \mathbb{R}$$

ir

$$f(x) = x^3.$$

Ar f yra bijekcija?

Ap. Funkcija vadiname bijekcija, jeigu ji injekcija ir siurjekcija.

5 klausimas. Jeigu

$$f : \mathbb{N} \rightarrow \{\mathbf{a}\}^*$$

ir

$$f(n) = \mathbf{a}^n,$$

ar f yra bijekcija?

Ats.: Taip.

6 klausimas. Tegul

$$f : \mathbb{R} \rightarrow \mathbb{R}$$

ir

$$f(x) = x^3.$$

Ar f yra bijekcija?

Ats.: Taip.

Pavyzdys. Funkcija $f : (0, 1) \rightarrow (2, 5)$ apibrėžta kaip

$$f(x) = 3x + 2$$

yra bijekcija.

Irodymas: Turime

$$f(x) = f(y) \Rightarrow 3x + 2 = 3y + 2 \Rightarrow x = y,$$

todėl f yra injekcija. Patikrinsime, ar $\forall y \in (2, 5) \exists$ toks x , kad

$$y = f(x) = 3x + 2?$$

Išsprendę x atžvilgiu, gauname $x = (y - 2)/3$. Kadangi

$$y \in (2, 5) \Rightarrow y - 2 \in (0, 3) \Rightarrow x = (y - 2)/3 \in (0, 1),$$

tai f yra surjekcija ir (kadangi injekcija) bijekcija. □

Atvirkštinė funkcija

Ap. Jeigu

$$f : A \rightarrow B$$

yra bijekcija, tada egzistuoja f atvirkštinė funkcija $g : B \rightarrow A$ tokia, kad

$$g(b) = a \Leftrightarrow f(a) = b.$$

Funkcijos f atvirkštinę funkciją dažniausiai žymime f^{-1} .

Atvirkštinė funkcija

Ap. Jeigu

$$f : A \rightarrow B$$

yra bijekcija, tada egzistuoja f atvirkštinė funkcija $g : B \rightarrow A$ tokia, kad

$$g(b) = a \Leftrightarrow f(a) = b.$$

Funkcijos f atvirkštinę funkciją dažniausiai žymime f^{-1} .

Jei $f : X \rightarrow Y$ turi atvirkštinę, $x \in X$, $y \in Y$, tai

$$(f \circ f^{-1})(y) = y, \quad (f^{-1} \circ f)(x) = x.$$

Dažniau vartojamas užrašas $f^{-1}(x)$ su x -u, o ne $f^{-1}(y)$.

Pavyzdys. Mes jau parodėme, jeigu $f : (0, 1) \rightarrow (2, 5)$ ir

$$f(x) = 3x + 2,$$

tai f yra bijekcija. Todėl $\exists f^{-1} : (2, 5) \rightarrow (0, 1)$ ir

$$f^{-1}(x) = (x - 2)/3 \quad (\text{užrašas } f^{-1}(x) \text{ su } x \in (2, 5).)$$

Pavyzdys. Mes jau parodėme, jeigu $f : (0, 1) \rightarrow (2, 5)$ ir

$$f(x) = 3x + 2,$$

tai f yra bijekcija. Todėl $\exists f^{-1} : (2, 5) \rightarrow (0, 1)$ ir

$$f^{-1}(x) = (x - 2)/3 \quad (\text{užrašas } f^{-1}(x) \text{ su } x \in (2, 5).)$$

Pavyzdys. Turime, kad $f : \mathbb{N}_5 \rightarrow \mathbb{N}_5$,

$$f(x) = (4x + 1) \pmod{5},$$

yra bijekcija. Todėl $\exists f$ atvirkštinė f-ja. Norint patikrinti, kad ši f-ja yra bijekcija ir rasti jai atvirkštinę f-ją, patogu naudoti teoremą, esančią kitoje skaidrėje.

[Teorema] Tegul $n \geq 2$, $f : \mathbb{N}_n \rightarrow \mathbb{N}_n$ ir

$$f(x) = (ax + b) \pmod{n}.$$

Tada

- f yra bijekcija $\Leftrightarrow \gcd(a, n) = 1$.
- Jeigu f bijekcija, tai

$$f^{-1}(x) = (kx + c) \pmod{n};$$

čia $k, c \in \mathbb{Z}$, $f(c) = 0$, o k randamas iš lygybės

$$ak + nm = 1,$$

kuri teisinga su koku nors $m \in \mathbb{Z}$.

Pavyzdys. Tegul $f : \mathbb{N}_5 \rightarrow \mathbb{N}_5$ ir

$$f(x) = (4x + 1) \pmod{5}.$$

Pavyzdys. Tegul $f : \mathbb{N}_5 \rightarrow \mathbb{N}_5$ ir

$$f(x) = (4x + 1) \pmod{5}.$$

Dël

$$\gcd(4, 5) = 1,$$

iš teoremos turime, kad f yra bijekcija.

Pavyzdys. Tegul $f : \mathbb{N}_5 \rightarrow \mathbb{N}_5$ ir

$$f(x) = (4x + 1) \pmod{5}.$$

Dël

$$\gcd(4, 5) = 1,$$

iš teoremos turime, kad f yra bijekcija. Ieškome \mathbf{c} reikšmës, su kuria $f(\mathbf{c}) = \mathbf{0}$. Matome,

$$f(1) = \mathbf{0},$$

todël $\mathbf{c} = 1$.

Pavyzdys. Tegul $f : \mathbb{N}_5 \rightarrow \mathbb{N}_5$ ir

$$f(x) = (4x + 1) \pmod{5}.$$

Dël

$$\gcd(4, 5) = 1,$$

iš teoremos turime, kad f yra bijekcija. Ieškome \mathbf{c} reikšmës, su kuria $f(\mathbf{c}) = \mathbf{0}$. Matome,

$$f(1) = \mathbf{0},$$

todël $\mathbf{c} = 1$. Pastebime, kad

$$4(-1) + 5(1) = 1.$$

Todël $k = -1$.

Pavyzdys. Tegul $f : \mathbb{N}_5 \rightarrow \mathbb{N}_5$ ir

$$f(x) = (4x + 1) \pmod{5}.$$

Dël

$$\gcd(4, 5) = 1,$$

iš teoremos turime, kad f yra bijekcija. Ieškome \mathbf{c} reikšmës, su kuria $f(\mathbf{c}) = \mathbf{0}$. Matome,

$$f(1) = \mathbf{0},$$

todël $\mathbf{c} = 1$. Pastebime, kad

$$4(-1) + 5(1) = 1.$$

Todël $k = -1$. Taigi, remdamiesi teorema, gauname

$$f^{-1}(x) = (-x + 1) \pmod{5}.$$

Užduotis. Tegul $f : \mathbb{N}_{13} \rightarrow \mathbb{N}_{13}$ ir

$$f(x) = (7x + 5) \pmod{13}.$$

Raskite f^{-1} jei tokia \exists .

Užduotis. Tegul $f : \mathbb{N}_{13} \rightarrow \mathbb{N}_{13}$ ir

$$f(x) = (7x + 5) \pmod{13}.$$

Raskite f^{-1} jei tokia \exists .

Sprendimas: Kadangi $\gcd(7, 13) = 1$, remiantis teorema f yra bijekcija ir $\exists f^{-1}$. Turime

$$f(3) = 0$$

ir

$$7(2) + 13(-1) = 1.$$

Todėl, pagal teoremą, gauname

$$f^{-1}(x) = (2x + 3) \pmod{13}.$$

Dirichlė principas

Jeigu m daiktų įdėti į n dėžių ir $m > n$, tai vienoje dėžėje bus ne mažiau nei du daiktai. Kitaip sakant, jeigu A ir B yra baigtinės aibės ir $|A| > |B|$, tai \nexists injekcija iš A į B .

1 pavyzdys. Jeigu $f : \mathbb{N}_7 \rightarrow \mathbb{N}_6$ ir

$$f(x) = x \pmod{6},$$

tai $f(0) = f(6)$.

2 pavyzdys. Pagrįsime, kad Meksiko mieste yra du žmonės, kurie turi vienodą skaičių plaukų ant galvos.

Argumentas: Kiekvienas žmogus turi mažiau nei 10 milijonų plaukų ant galvos, o Meksiko mieste gyvena daugiau nei 10 milijonų žmonių. Turime Dirichlė taisyklę.

3 pavyzdys. Kokius 11 skaičių pasirinktume iš

$$S = \{1, 2, 3, \dots, 19, 20\}$$

visada gausime, kad du iš jų bus tokie, kad vienas iš jų dalins kitą.

Irodymas. Kiekvienas natūralus skaičius $x \geq 1$ gali būti vieninteliu būdu užrašytas kaip

$$x = 2^k m,$$

kai $k \in \mathbb{N}$, o m nelyginis skaičius. Todėl skaičiai iš S gali būti užrašyti kaip:

$$\begin{array}{llll} 1 = 2^0 \cdot 1, & 2 = 2^1 \cdot 1, & 3 = 2^0 \cdot 3, & 4 = 2^2 \cdot 1, \\ 5 = 2^0 \cdot 5, & \dots, & 12 = 2^2 \cdot 3, & \dots, \\ 19 = 2^0 \cdot 19, & 20 = 2^2 \cdot 5. & & \end{array}$$

Pastebime, kad m įgyja reikšmes iš aibės

$$\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19\},$$

kuri turi 10 elementų. Todėl, remiantis Dirichlė principu, du iš 11 atrinktų skaičių turės tą patį daugiklį m . Pavyzdžiui,

$$x = 2^k m$$

ir

$$y = 2^j m,$$

$k \neq j$. Gauname $x|y$ arba $y|x$. □

Pastebime, kad m įgyja reikšmes iš aibės

$$\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19\},$$

kuri turi 10 elementų. Todėl, remiantis Dirichlė principu, du iš 11 atrinktų skaičių turės tą patį daugiklį m . Pavyzdžiui,

$$x = 2^k m$$

ir

$$y = 2^j m,$$

$k \neq j$. Gauname $x|y$ arba $y|x$. □

Užduotis. Įrodykite, kad bet koks n , $n \geq 2$, eilės grafas turi bent dvi vienodo laipsnio viršūnes.

Šifrai ir mod funkcija (truputis kriptologijos)

Eilės tvarka pažymėkime anglų kalbos abėcėlės raides skaičiais

$$0, 1, \dots, 25$$

atitinkamai. Kiekviena bijekcija $f : \mathbb{N}_{26} \rightarrow \mathbb{N}_{26}$ gali būti panaudota kaip šifras, o jos atvirkštinė f^{-1} kaip raktas.

Šifrai ir mod funkcija (truputis kriptologijos)

Eilės tvarka pažymėkime anglų kalbos abėcėlės raides skaičiais

$$0, 1, \dots, 25$$

atitinkamai. Kiekviena bijekcija $f : \mathbb{N}_{26} \rightarrow \mathbb{N}_{26}$ gali būti panaudota kaip šifras, o jos atvirkštinė f^{-1} kaip raktas.

Adityvusis šifras:

$$f(x) = (x + 2) \pmod{26} \quad \text{ir} \quad f^{-1}(x) = (x + 24) \pmod{26}.$$

Šifrai ir mod funkcija (truputis kriptologijos)

Eilės tvarka pažymėkime anglų kalbos abėcėlės raides skaičiais

$$0, 1, \dots, 25$$

atitinkamai. Kiekviena bijekcija $f : \mathbb{N}_{26} \rightarrow \mathbb{N}_{26}$ gali būti panaudota kaip šifras, o jos atvirkštinė f^{-1} kaip raktas.

Adityvusis šifras:

$$f(x) = (x + 2) \pmod{26} \quad \text{ir} \quad f^{-1}(x) = (x + 24) \pmod{26}.$$

Multiplikatyvusis šifras:

$$f(x) = 3x \pmod{26} \quad \text{ir} \quad f^{-1}(x) = 9x \pmod{26}.$$

Šifrai ir mod funkcija (truputis kriptologijos)

Eilės tvarka pažymėkime anglų kalbos abėcėlės raides skaičiais

$$0, 1, \dots, 25$$

atitinkamai. Kiekviena bijekcija $f: \mathbb{N}_{26} \rightarrow \mathbb{N}_{26}$ gali būti panaudota kaip šifras, o jos atvirkštinė f^{-1} kaip raktas.

Adityvusis šifras:

$$f(x) = (x + 2) \pmod{26} \quad \text{ir} \quad f^{-1}(x) = (x + 24) \pmod{26}.$$

Multiplikatyvusis šifras:

$$f(x) = 3x \pmod{26} \quad \text{ir} \quad f^{-1}(x) = 9x \pmod{26}.$$

Mišrusis šifras:

$$f(x) = (5x + 1) \pmod{26} \quad \text{ir} \quad f^{-1}(x) = (-5x + 5) \pmod{26}.$$

Kai kuriuose šifruose viena ar daugiau raidžių lieka nepakeistos. Pavyzdžiui, šifras $f(x) = 3x \pmod{26}$ nepakeičia raidės **a**, nes $f(0) = 0$. Kita teorema reikalinga norint sukurti šifrą be nepakitusių žymėjimų.

[Teorema (mod ir fiksuoti taškai)] Tegul $n > 0$. Tariame, kad $f : \mathbb{N}_n \rightarrow \mathbb{N}_n$ ir

$$f(x) = (ax + b) \pmod{n}.$$

Tokiu atveju, f neturės fiksuotų taškų tada ir tik tada, kai

$$\gcd(a - 1, n) \nmid b.$$

Pavyzdys. Šifrai

$$f(x) = (x + 2) \pmod{26} \quad \text{ir} \quad f(x) = (5x + 1) \pmod{26}$$

neturi fiksuotų taškų, o šifras $f(x) = 3x \pmod{26}$ turi.

Hash funkcijos

Tikslas, neatliekant paieškos, panaudojus kažkurį raktą, rasti informaciją lentelėje. Funkcija **hash** atvaizduoja raktų aibę S į lentelės indeksų aibę \mathbb{N}_n , t.y.,

$$\text{hash} : S \rightarrow \mathbb{N}_n.$$

Ieškoma lentelė vadinama **hash** lentele.

Jeigu **hash** nėra injekcija, įvyksta kolizijos. Jeigu nėra kolizijų, tai bet kuris raktas iš S atvaizduojamas į skirtingą indeksą, kuriame informacija pasiekama be paieškos.

Pavyzdys. Tegul S yra auditorijoje esančių studentų aibė. Funkcija

$$\text{hash} : S \rightarrow \mathbb{N}_{366}$$

nurodo studento gimimo dieną. Jeigu du studentai gimę tą pačią dieną, tai turime koliziją.

Kolizijų išsprendimas tiesiniu zondavimu

Jeigu turime koliziją indekse k , tai pirmesnis raktas atvaizduojamas į k , o kitas turi būti atvaizduotas kitur.

Tiesinis zondavimas yra paieškos (zondavimo) technika, skirta atrasti laisvas vietas lentelėse. Ji veikia tokiu būdu. Tiesiškai tikrina tolimesnes vietas su fiksuotu tarpu g (gap = g):

$$(k + g) \bmod n,$$

$$(k + 2g) \bmod n,$$

...

$$(k + (n - 1)g) \bmod n;$$

kol neatranda laisvo indekso arba nepatikrina visų prieinamų indeksų.

Pavyzdys. Tegul

$$S = \{jan, feb, mar, apr, may, jun\}.$$

Turime

$$h : S \rightarrow \mathbb{N}_6$$

ir

$$h(xyz) = p(x) \pmod{6};$$

čia $p(x)$ yra raidės x pozicija abėcėlėje

$$(p(a) = 1, \dots, p(z) = 26).$$

Talpinsim raktus iš S į hash lentelę pradėdami nuo *jan*, po to *feb* ir t.t. Turime, kad

$$\begin{aligned} h(jan) &= p(j) \pmod{6} \\ &= 10 \pmod{6} \\ &= 4, \end{aligned}$$

taigi *jan* priskiriam 4 poziciją hash lentelėje.

Tęsdami gauname

$$h(\textit{feb}) = 0,$$

$$h(\textit{mar}) = 1,$$

$$h(\textit{apr}) = 1 \text{ (kolizija su } \textit{mar}),$$

$$h(\textit{may}) = 1 \text{ (kolizija su } \textit{mar} \text{ ir } \textit{apr}),$$

$$h(\textit{jun}) = 4 \text{ (kolizija su } \textit{jan}).$$

Tęsdami gauname

$$h(\text{feb}) = 0,$$

$$h(\text{mar}) = 1,$$

$$h(\text{apr}) = 1 \text{ (kolizija su } \textit{mar}\text{)},$$

$$h(\text{may}) = 1 \text{ (kolizija su } \textit{mar} \text{ ir } \textit{apr}\text{)},$$

$$h(\text{jun}) = 4 \text{ (kolizija su } \textit{jan}\text{)}.$$

Panaudoję tiesinio zondavimo techniką su tarpu 1 ($\text{gap}=1$), gauname

$$\textit{feb} \mapsto 0$$

$$\textit{mar} \mapsto 1$$

$$\textit{apr} \mapsto 2$$

$$\textit{may} \mapsto 3$$

$$\textit{jan} \mapsto 4$$

$$\textit{jun} \mapsto 5$$

1 užduotis. Išspręskite kolizijas su $\text{gap}=2$.

Atsakymas: *feb, mar, jun, apr, jan, may*.

2 užduotis. Išspręskite kolizijas su $\text{gap}=3$.

Atsakymas: *feb, mar, blank, blank, jan, blank*.

(*apr, may* ir *jun* šiuo atveju neatranda sau vietos)

Savybė:

Jeigu n yra lentelės dydis, $\text{gap} = g$ ir $\text{gcd}(n, g) = 1$, kolizijos išsprendžiamos tiesinio zondavimo būdu.

Išvada:

Jeigu lentelės dydis yra pirminis skaičius p , tai su bet kuriuo tarpu $1 \leq \text{gap} < p$ būsime užtikrinti, kad visiems raktams teks po lentelę.

Rekomenduojamos literatūros sąrašas

-  James L. Hein, "Discrete Structures, Logic, and Computability"
-  + StudentStudyGuide.pdf