Diskrečioji matematika, IT 1 kursas

Dr. Robertas Petuchovas

Vilniaus universitetas

2016 - 2017 m.

II skyrius. Faktai apie funkcijas

2.1 Funkcijų apibrėžimai ir pavyzdžiai

Ap. Funkcija vadiname atvaizdį

$$f : A \to B,$$

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

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

- Funkcijos f įgyjamų reikšmių aibė yra žymima

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

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

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

1 pavyzdys. Turime funkciją

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

$f(a) = f(b) = 1$ 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 $f : \mathbb{Z} \to \mathbb{Z}$ ir

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

Pažymėkime L ir N lyginių ir nelyginių skaičių aibes. Turime

$$\begin{aligned}
&\mathrm{range}(f) = f(\mathbb{Z}) = L,\\
&f(L) = \{4k \mid k \in \mathbb{Z}\},\\
&f(N) = \{4k + 2 \mid k \in \mathbb{Z}\},\\
&f^{-1}(L) = \mathbb{Z},\\
&f^{-1}(N) = \emptyset.
\end{aligned}$$

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

$$f(x) = \text{ if } x \text{ is odd then } x+1 \text{ else } x.$$

Apibūdinkite aibes:

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

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

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

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

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

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

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

Floor ir Ceiling funkcijos

Funkcijos floor ir ceiling yra $\mathbb{R} \to \mathbb{Z}$;

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

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

1 teiginys. Turime, kad

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

Įrodymas: 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

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

Įrodymas: 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 bendras daliklis

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

$$\gcd(x, y) - \text{didžiausias skaičius, kuris dalina } x \text{ ir } y.$$

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

Funkcijos gcd savybės:

- $\gcd(a, b) = \gcd(b, a) = \gcd(a, -b)$.
- $\gcd(a, b) = \gcd(a - bq, b)$ su bet kuriuo $q \in \mathbb{Z}$.
- $\gcd(a, b) = ma + nb$ su kažkuriais $m, n \in \mathbb{Z}$.
- 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 $0 \leq r < |b|$.

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 $\gcd(189, 33)$:

$$\begin{aligned} 189 &= 33 \cdot 5 + 24 \\ 33 &= 24 \cdot 1 + 9 \\ 24 &= 9 \cdot 2 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0 \\ & \text{Output}(3). \end{aligned}$$

Klausimas. Kiek iteracijų turės Euklido algoritmas ieškant $\gcd(117, 48)$?

Atsakymas: Keturias iteracijas.

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, išspręsime 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 $a \mod b$. Todėl

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

Klausimas. Kokie elementai sudaro aibę $\{x \mod 5 \mid x \in \mathbb{Z}\}$?
Atsakymas: $\{0, 1, 2, 3, 4\}$.

Toliau žymėsime

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

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

$$\mathrm{range}(x \mod n) = \mathbb{N}_n.$$

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

Sprendimas:

12-os valandų laikrodis:

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

24-ių valandų laikrodis:

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

Atsakymas: Penkta valanda dienos.

Užduotis. Parašykite skaičių 13 dvejetainėje sistemoje.

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

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

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.

$$s < t \quad \Longrightarrow \quad \log_b s < \log_b t.$$

Logaritmo savybės:

$$\log_b 1 = 0,$$

$$\log_b b = 1,$$

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

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

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

$$\log_a x = (\log_a b)(\log_b x); \text{ čia } a > 1.$$

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 $f : B \to C$ ir $g : A \to B$, tada reiškinys

$$f(g(x))$$

turi prasmę ir yra vadinamas funkcijų f ir g kompozicija.

Rašome

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

ir žymime $(f \circ g)(x) = f(g(x))$.

Pavyzdžiai:

$$\mathsf{floor}(\log_2 20) = \mathsf{floor}(4\ldots) = 4,$$
$$\mathsf{ceiling}(\log_2 20) = \mathsf{ceiling}(4\ldots) = 5,$$
$$\mathsf{head}(\mathsf{tail}(\langle \mathsf{a}, \mathsf{b}, \mathsf{c}\rangle)) = \mathsf{head}(\langle \mathsf{b}, \mathsf{c}\rangle) = \mathsf{b}.$$

Funkcijos seq ir dist

Funkcijos seq apibrėžimas:

$$\mathsf{seq} : \mathbb{N} \to \mathsf{lists}(\mathbb{N})$$

ir

$$\mathsf{seq}(n) = \langle 0, 1, \ldots, n \rangle.$$

Funkcijos dist apibrėžimas:

$$\mathsf{dist} : A \times \mathsf{lists}(B) \to \mathsf{lists}(A \times B)$$

ir

$$\mathsf{dist}(a, \langle x_1, \ldots, x_k \rangle) = \langle (a, x_1), \ldots, (a, x_k) \rangle.$$

Klausimas. Kaip galime aprašyti funkciją

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

(programavimo požiūriu)?

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

Klausimas. Kaip galime aprašyti funkciją

$$f : \mathbb{N} \to \mathsf{lists}(\mathbb{N} \times \mathbb{N})$$

ir

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

kitų funkcijų pagalba?

Atsakymas:

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

Funkcija map

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

$$\mathsf{map}(\mathsf{f}, \langle \mathsf{x}_1, \mathsf{x}_2, \ldots, \mathsf{x}_k \rangle) = \langle \mathsf{f}(\mathsf{x}_1), \ldots, \mathsf{f}(\mathsf{x}_k) \rangle.$$

Užduotis. Apskaičiuokite, kam bus lygu

$$\mathsf{map}(\mathsf{floor} \circ \mathsf{log}_2, \mathsf{tail}(\mathsf{seq}(8))).$$

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

Užduotis:

Turime

$$\mathsf{f} : \mathbb{N} \to \mathsf{lists}(\mathbb{N})$$

ir

$$\mathsf{f}(\mathsf{n}) = \langle 0, 2, 4, \ldots, 2\mathsf{n} \rangle.$$

Aprašykite f kitų funkcijų pagalba.

Sprendimas:

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

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

Užduotis:

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

$$\mathsf{f}(n) = \langle 5, 9, \ldots, 5 + 4n \rangle.$$

Sprendimas:

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

Atsakymas: $\mathsf{f}(n) = \mathsf{map}(+, \mathsf{dist}(5, \mathsf{map}(\cdot, \mathsf{dist}(4, \mathsf{seq}(n))))).$

Užduotis:

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

$$\mathsf{f}(\mathsf{a}, \mathsf{b}, \mathsf{n}) = \langle \mathsf{a}, \mathsf{a} + \mathsf{b}, \mathsf{a} + 2\mathsf{b}, \ldots, \mathsf{a} + \mathsf{nb} \rangle.$$

Sprendimas:

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

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

2.3 Funkcijų savybės

Tegul $f : A \to B$ 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

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

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

$$f(x) = 2x \mod 8.$$

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

1 klausimas. Tegul $f : \mathbb{Z} \to \mathbb{N}$ 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 yra injekcija?

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

Ap. Funkcija $f : A \to B$ 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 $f : \mathbb{Z} \to \mathbb{N}$ ir $f(x) = x^2$, ar f yra siurjekcija?

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

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

Atsakymas: Siurjekcija, bet ne injekcija.

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

5 klausimas. Jeigu

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

ir

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

ar f yra bijekcija?

Ats.: Taip.

6 klausimas. Tegul

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

ir

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

Ar f yra bijekcija?

Ats.: Taip.

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

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

yra bijekcija.

Įrodymas: Turime

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

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

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

tai f yra siurjekcija ir (kadangi injekcija) bijekcija. $\square$

Atvirkštinė funkcija

Ap. Jeigu

$$f : A \to B$$

yra bijekcija, tada egzistuoja f atvirkštinė funkcija

$$g : B \to A$$

tokia, kad

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

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

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

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

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

$$f^{-1}(x) = (x-2)/3.$$

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

$$f(x) = (4x+1) \mod 5,$$

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 $n \geq 2$,

$$f : \mathbb{N}_n \to \mathbb{N}_n$$

ir

$$f(x) = (ax + b) \mod n.$$

Tada

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

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

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

$$ak + nm = 1,$$

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

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

$$f(x) = (4x + 1) \mod 5.$$

Kadangi

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

iš teoremos turime, kad f bijekcija. Ieškome c reikšmės, su kuria $f(c) = 0$. Matome, $f(1) = 0$, todėl $c = 1$. Pastebime, kad

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

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

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

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

$$f(x) = (7x + 5) \mod 13.$$

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

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

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.

Pavyzdys. Jeigu $f : \mathbb{N}_7 \to \mathbb{N}_6$ ir

$$f(x) = x \mod 6,$$

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

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.

Pavyzdys. Kokius 11 skaičių bepasirinktume iš

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

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

Įrodymas. 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:

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

Pastebim, 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. Raskite 10 skaičių iš S, kurie nedalina vienas kito.

Atsakymas: $6, 7, 8, 9, 11, 13, 15, 17, 19, 20$.

Šifrai ir mod funkcija (truputis kriptologijos)

Eilės tvarka pažymėkime anglų kalbos abėcėlės raides skaičiais

$$0, 1, \ldots, 25$$

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

Adityvus šifras:

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

Multiplikatyvus šifras:

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

Mišrus šifras:

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

Kai kuriuose šifruose viena ar daugiau raidžių lieka nepakeistos. Pavyzdžiui, šifras $f(x) = 3x \mod 26$ 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 $f : \mathbb{N}_n \to \mathbb{N}_n$ ir

$$f(x) = (ax + b) \mod n.$$

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

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

Pavyzdys. Šifrai

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

neturi fiksuotų taškų, o šifras $f(x) = 3x \mod 26$ 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.,

$$\mathsf{hash} : \mathsf{S} \to \mathbb{N}_{\mathsf{n}}.$$

Menama 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 pasiekiama be paieškos.

Pavyzdys. Tegul S yra auditorijoje esančių studentų aibė. Funkcija

$$\mathsf{hash} : \mathsf{S} \to \mathbb{N}_{366}$$

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 $= g$):

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

...

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

kol neatranda laisvo indekso arba nepatikrina visų prieinamų indeksų.

Pavyzdys. Tegul

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

Turime

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

ir

$$h(xyz) = p(x) \mod 6;$$

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

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

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

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

taigi *jan* užims 4 poziciją lentelėje.

Tęsdami gauname

$h(feb) = 0$,
$h(mar) = 1$,
$h(apr) = 1$ (kolizija su *mar*),
$h(may) = 1$ (kolizija su *mar* ir *apr*),
$h(jun) = 4$ (kolizija su *jan*).

Panaudoję tiesinio zondavimo techniką su tarpu 1 (gap=1), gauname

$$
\begin{aligned}
feb &\longmapsto 0 \\
mar &\longmapsto 1 \\
apr &\longmapsto 2 \\
may &\longmapsto 3 \\
jan &\longmapsto 4 \\
jun &\longmapsto 5
\end{aligned}
$$

1 užduotis. Išspręskite kolizijas su gap=2.

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

2 užduotis. Išpręskite kolizijas su gap=3.

Atsakymas: *feb*, *mar*, *blank*, *blank*, *jan*, *blank*.
(*apr*, *may* ir *jun* šiuo atveju neatranda sau vietos)

Savybė:
Jeigu n yra lentelės dydis, o gap= g, tada atveju $\gcd(n, g) = 1$ turėsime, kad su tarpu g visi indeksai nuzonduojami.

Išvada:
Jeigu lentelės dydis yra pirminis skaičius p, tai su bet kuriuo tarpu $1 \leq \text{gap} < p$ būsime užtikrinti, kad visi raktai pateks į lentelę.

Rekomenduojamos literatūros sąrašas


James L. Hein, "Discrete Structures, Logic, and Computability"


+ StudentStudyGuide.pdf