Primož Potočnik

Zapiski predavanj predmeta Proseminar

Ljubljana, marec 2011

Naslov: Zapiski predavanj predmeta Proseminar
Avtor: Primož Potočnik
1. izdaja
Dostopno na spletnem naslovu `www.fmf.uni-lj.si/~potocnik`

CIP – Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

511(0.034.2)

POTOČNIK, Primož, 1971 –

Zapiski predavanj predmeta Proseminar [Elektronski vir]

Primož Potočnik. - 1. izd. – El. knjiga. – Ljubljana : samozal., 2011

Način dostopa (URL):
http://www.fmf.uni-lj.si/∼potocnik/Ucbeniki/Proseminar-izrocki.pdf

ISBN 978-961-93056-3-8

255520256

Kazalo

1 Osnovno o množicah

1.1 Relacije vsebovanosti in enakosti

Za naše potrebe *množica* pomeni *skupino* (*zbirko, družino, nabor,...*) nekih *objektov*. Če množica A vsebuje objekt x, pravimo, da je x *element* množice A in zapišemo

$$x \in A.$$

Dve množici sta *enaki* natanko tedaj, ko *vsebujeta* iste elemente. To zapišemo takole:

$$A = B \equiv \forall x(x \in A \Leftrightarrow x \in B).$$

Če množica A vsebuje vse elemente množice B (in morda še kakšnega za povrh), pravimo, da je B *podmnožica* množice A in to zapišemo kot $B \subseteq A$:

$$B \subseteq A \equiv \forall x(x \in B \Rightarrow x \in A).$$

Množici A in B sta torej enaki natanko tedaj, ko velja tako $A \subseteq B$ kot $B \subseteq A$. S simboli to zapišemo kot

$$\forall A \forall B(A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A)$$

Končne množice lahko določimo tako, da naštejemo vse njene elemente. Na primer,

$$A := \{2, 3, 5, 7\} \text{ ali } X := \{\text{Sonce}, \text{Zemlja}, \text{Mesec}\}.$$

V splošnem množice podamo tako, da podamo *pogoj za pripadnost*. Na primer,

$$\mathbb{P} := \{x \mid x \text{ je naravno število, deljivo le z } 1 \text{ in samim seboj}\}.$$

1.2 Operacije z množicami

Za dani dve množici A in B lahko definiramo njuno *unijo* in *presek*:

$$A \cup B = \{x \mid x \in A \vee x \in B\}, \qquad A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

Če množici A in B nimata nobenega skupnega elementa, je njun presek množica, ki ne vsebuje nobenega elementa. Takšni množici pravimo *prazna množica* in jo označimo s simbolom $\emptyset$.

Za vsako množico A velja

$$\emptyset \subseteq A,\ A \cup \emptyset = A \ \text{ in } \ A \cap \emptyset = \emptyset.$$

Poleg operacij unije in preseka omenimo še operaciji *razlike* in *simetrične razlike* množic

$$A - B = \{x \mid x \in A \wedge x \notin B\}, \qquad A \oplus B = (A \cup B) - (A \cap B).$$

Mnogokrat je udobno v naprej izbrati množico vseh objektov, o katerih želimo govoriti. Takšni množici rečemo *univerzalna množica* in jo označimo z $\mathcal{U}$. Vse ostale množice so tedaj podmnožice množice $\mathcal{U}$. S pomočjo univerzalne množice definiramo operacijo *komplementa*. Komplement množice A vsebuje natanko tiste elemente univerzalne množice, ki jih A ne vsebuje:

$$A^c = \{x \mid x \notin A\}.$$

Navedimo nekaj zanimivih lastnosti zgoraj definiranih operacij:

$A \cap B = B \cap A$	komutativnost preseka
$A \cup B = B \cup A$	komutativnost unije
$(A \cap B) \cap C = A \cap (B \cap C)$	asociativnost preseka
$(A \cup B) \cup C = A \cup (B \cup C)$	asociativnost unije
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	distributivnost unije
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	distributivnost preseka
$(A \cap B)^c = A^c \cup B^c$	1. de Morganov zakon
$(A \cup B)^c = A^c \cap B^c$	2. de Morganov zakon
$A \cap (A \cup B) = A$	1. absorbcijsko pravilo
$A \cup (A \cap B) = A$	2. absorbcijsko pravilo
$A \cap A = A$	idempotentnost preseka
$A \cup A = A$	idempotentnost unije
$A \cap \emptyset = \emptyset$	presek s prazno množico
$A \cup \emptyset = A$	unija s prazno množico

1.3 Presek in unija družine množic

Poleg preseka in unije dveh množic v matematiki pogosto uporabljamo presek in unijo *družine množic*. Naj bo $\mathcal{D}$ množica, katere elementi so množice (takšni množici ponavadi rečemo *družina množic*. Tedaj *unijo družine* $\mathcal{D}$ definiramo kot množico vseh tistih objektov, ki se pojavijo v vsaj eni od množic iz $\mathcal{D}$:

$$\bigcup \mathcal{D} = \bigcup_{A \in \mathcal{D}} A = \{x \mid \exists A (A \in \mathcal{D} \wedge x \in A)\}.$$

Presek družine $\mathcal{D}$ pa definiramo množic kot množico vseh tistih objektov, ki so vsebovani v prav vsaki množici iz družine $\mathcal{D}$:

$$\bigcap \mathcal{D} = \bigcap_{A \in \mathcal{D}} A = \{x \mid \forall A (A \in \mathcal{D} \Rightarrow x \in A)\}.$$

ZGLED. *Naj bo* $\mathcal{D} = \{\{1,2,3\},\{2,3,4\},\{3,4,5\}\}$. *Tedaj je*

$$\bigcap \mathcal{D} = \{3\} \quad \textit{in} \quad \bigcup \mathcal{D} = \{1,2,3,4,5\}.$$

Dalje, za naravno število n *definirajmo* $A_n = \{x \mid x \in \mathbb{N} \wedge x \geq n\}$. *Tedaj je*

$$\bigcap_{n \in \mathbb{N}} A_n = \emptyset \quad \textit{in} \quad \bigcup_{n \in \mathbb{N}} A_n = \mathbb{N}.$$

■

1.4 Intervali v $\mathbb{R}$

V matematični analizi igrajo pomembno vlogo množice realnih števil, ki ležijo med dvema predpisanima realnima številoma. Takšnim množicam pravimo intervali. Definiramo več vrst intervalov, ki se ločijo glede na to, ali vsebujejo svoja mejna števila ali ne. Naj bosta a in b realni števili in naj bo $a < b$. Tedaj definiramo:

$[a,b] = \{x \mid x \in \mathbb{R} \wedge a \leq x \leq b\}$	zaprti interval
$(a,b) = \{x \mid x \in \mathbb{R} \wedge a < x < b\}$	odprti interval
$(a,b] = \{x \mid x \in \mathbb{R} \wedge a < x \leq b\}$	navzgor polzaprti interval
$[a,b) = \{x \mid x \in \mathbb{R} \wedge a \leq x < b\}$	navzdol polzaprti interval
$[a,\infty) = \{x \mid x \in \mathbb{R} \wedge a \leq x\}$	navzgor neomejeni zaprti interval
$(a,\infty) = \{x \mid x \in \mathbb{R} \wedge a \leq x\}$	navzgor neomejeni odprti interval
$(-\infty,b] = \{x \mid x \in \mathbb{R} \wedge a \leq x\}$	navzdol neomejeni zaprtii interval
$(-\infty,b) = \{x \mid x \in \mathbb{R} \wedge a \leq x\}$	navzdol neomejeni odprtii interval

ZGLED. *Preveri, da velja*

$$\bigcap_{n \in \mathbb{N}} [0, \frac{1}{n}) = \{0\}, \quad \textit{in} \quad \bigcap_{n \in \mathbb{N}} (0, \frac{1}{n}] = \emptyset$$

■

ZGLED. *Preveri, da velja*

$$\bigcup_{n\in\mathbb{N}} [\frac{1}{n}, 1] = (0, 1]$$

■

1.5 Potenčna množica

Naj bo A dana množica. Množici, katere elementi so natanko vse podmnožice množice A (vključno s podmnožicama A in $\emptyset$) rečemo *potenčna množica množice A*. Označimo jo z oznako $\mathcal{P}A$. Na primer, če je $A = \{1, 2\}$, potem je

$$\mathcal{P}A = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}.$$

Ni se težko prepričati, da potenčna množica množice z n elementi šteje natanko 2^n elementov.

1.6 Množice – vaje

1. Z matematičnimi simboli zapiši naslednje množice:
   (a) množico vseh lihih naravnih števil;
   (b) množico vseh racionalnih števil, večjih od 1, katerih tretja potenca je manjša od 100;
   (c) množico skupnih večkratnikov števil 12 in 20;
   (d) množico vseh naravnih števil, ki so enaka kvadratu kakega celega števila;
   (e) množico vseh podmnožic množice naravnih števil, ki vsebujejo $\{0\}$ kot svojo podmonožico.
2. S pomočjo standardnih računskih zakonov za presek, unijo in komplement poenostavi naslednje izraze:
   (a) $(A \cap (B \cup A^C)) \cup B$;
   (b) $((A \cap B \cap C) \cup (B \cap A))^C \cap B$;
   (c) $((A - B) \cup B) - (A \cap B)$.
3. Izračunaj naslednje preseke in unije neskončnih družin množic (odgovore utemelji):
   - $\bigcup_{n\in\mathbb{Z}}\{x : x \in \mathbb{Z} \wedge 1 - 2n \leq x \leq 1 + 2n\}$;
   - $\bigcap_{n\in\mathbb{Z}}\{x : x \in \mathbb{Z} \wedge 1 - 2n \leq x \leq 1 + 2n\}$;
   - $\bigcup_{n\in\mathbb{N}}[\frac{n+1}{n}, \frac{n^2+1}{n}]$;
   - $\bigcap_{n\in\mathbb{N}}[\frac{n+1}{n}, \frac{n^2+1}{n}]$;
   - $\bigcap_{n\in\mathbb{N}}(\frac{n-1}{n}, \frac{n+1}{n})$;
   - $\bigcap_{n\in\mathbb{N}}[\frac{n-1}{n}, \frac{n+1}{n}]$.
4. Naj bo $A = \{1, 2, 3, 4, \}$ in $B = \{3, 4, 5, 6\}$. Zapiši presek potenčnih množic množic A in B.
5. Dokaži ali ovrži naslednje trditve:
   (a) $\mathcal{P}(A \cap B) = \mathcal{P}A \cap \mathcal{P}B$;
   (b) $\mathcal{P}(A \cup B) = \mathcal{P}A \cup \mathcal{P}B$;
   (c) $\mathcal{P}(A - B) = \mathcal{P}A - \mathcal{P}B$.

2 Odprtost, zaprtost kompaktnost

V tem razdelku bomo opazovali množice v ravnini in prostoru, oziroma splošneje, v n-razsežnem prostoru $\mathbb{R}^n$. Točke prostora $\mathbb{R}^n$ so urejene n-terice $(x_1, \ldots, x_n)$ realnih števil x_i. Če je $n = 2$, si lahko takšne n-terice (x_1, x_2) predstavljamo kot točke v ravnini, opremljeni s pravokotnim koordinatnim sistemom. Podobno, če je $n = 3$, si jih lahko predstavljamo kot točke v trirazsežnem prostoru.

2.1 Razdalja in krogle v evklidskem prostoru

Če sta $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ in $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ dve točki v $\mathbb{R}^n$, potem je *razdalja* med njima enaka

$$d(\mathbf{x}, \mathbf{y}) = \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2 + \ldots + (y_n - x_n)^2}.$$

Množici $\mathbb{R}^n$, opremljeni s tako definirano razdaljo, rečemo tudi *evklidski prostor*. Za tako definirano razdaljo velja tako imenovana *trikotniška neenakost*:

$$d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \geq d(\mathbf{x}, \mathbf{z}).$$

Množici točk, ki so od kake dane točke $\mathbf{x} \in \mathbb{R}^n$ oddaljene za manj (ali enako) od kakega danega pozitivnega števila r, pravimo krogle. Natančneje, množici

$$K_r(\mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^n \mid d(\mathbf{x}, \mathbf{y}) < r\}$$

rečemo *odprta krogla* s *polmerom* r in *središčem* $\mathbf{x}$. Besedica *odprta* je dodana zato, da poudari, da h krogli ne štejemo tudi točk *na robu*, tj. točk, ki so od $\mathbf{x}$ oddaljene natanko r. Če želimo takšne točke dodati, potem definiramo

$$\bar{K}_r(\mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^n : d(\mathbf{x}, \mathbf{y}) \leq r\}$$

in govorimo o *zaprti krogli*.

2.2 Rob, notranjost, zunanjost

Naj bo A poljubna podnožica v $\mathbb{R}^n$. Tedaj za točko $\mathbf{x} \in \mathbb{R}^n$ rečemo, da je

- *notranja v* A, brž ko obstaja $r > 0$, za katereka je $K_r(\mathbf{x}) \subseteq A$;
- *zunanja za* A, brž ko obstaja $r > 0$, za katerega je $K_r(\mathbf{x}) \subseteq A^C$;
- *na robu* A, če sta za vsak $r > 0$ preseka $A \cap K_r(\mathbf{x})$ in $A^C \cap K_r(\mathbf{x})$ neprazna.

Enostaven logičen premislek pokaže, da je vsaka točka bodisi notranja bodisi zunanja bodisi leži na robu A. Množici vseh notranjih točk množice A rečemo *notranjost* A (oznaka: $\mathrm{int}(A)$), množici vseh zunanjih točk rečemo *zunanjost* A (oznaka: $\mathrm{ext}(A)$), množici robnih točk pa *rob* A (oznaka: ∂A).

Oglejmo si zgleda, ki pokažeta, da lahko se za robno točko množice A lahko zgodi tako, da leži v A, kot da leži v A^C.

ZGLED. *Vzemimo množico* $A = \{(x, y) \mid -1 \leq x \leq 1 \wedge -1 < y < 1\} \subseteq \mathbb{R}^2$. *Premislimo, da sta točki* $\mathbf{x} = (0, 1) \in A^C$ *in* $\mathbf{y} = (1, 0) \in A$ *na robu množice* A.

Vzemimo poljuben $r > 0$ in si oglejmo krogli $K_r(\mathbf{x})$ in $K_r(\mathbf{y})$. Krogla $K_r(\mathbf{x})$ vsebuje točki $(0, 1 - r/2)$ in $(0, 1 + r/2)$, od katerih je prva v A, druga pa v A^C. To pomeni, da res za vsak $r > 0$ krogla $K_r(\mathbf{x})$ seka tako A kot A^C. Točka $\mathbf{x}$ je zato na robu A. Podobno krogla $K_r(\mathbf{y})$ vsebuje točki $(1 - r/2, 0)$ in $(1 + r/2, 0)$, od katerih je prva v A, druga pa v A^C. Zato je tudi točka $\mathbf{y}$ na robu A. ∎

Množica $A \subseteq \mathbb{R}^n$ je:

- *odprta*, če je vsaka njena točka notranja (tj. če ne vsebuje nobene robne točke);
- *zaprta*, če vsebuje ves svoj rob.

Večina (karkoli že to pomeni) množic ni niti zaprtih niti odprtih, saj se lahko zgodi, da množica vsebujo kako svojo robno točko, ne pa vseh. Takšna je, na primer, množica $\{(x, y) \mid -1 \leq x \leq 1 \wedge -1 < y < 1\} \subseteq \mathbb{R}^2$.

ZGLED. *Odprta krogla* $K_r(\mathbf{x})$ *je odprta množica, zaprta krogla* $\bar{K}_r(\mathbf{x})$ *pa zaprta množica.*

Vzemimo poljubno točko $\mathbf{y} \in K_r(\mathbf{x})$. Po definiciji krogle je $d(\mathbf{x}, \mathbf{y}) < r$. Naj bo $r' = \frac{1}{2}(r - d(\mathbf{x}, \mathbf{y}))$. Trdimo, da je $K_{r'}(\mathbf{y}) \subseteq K_r(\mathbf{x})$. Res: vzemimo poljuben $\mathbf{z} \in K_{r'}(\mathbf{y})$. Iz trikotniške neenakosti sledi:

$$d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) < d(\mathbf{x}, \mathbf{y}) + \frac{1}{2}(r - d(\mathbf{x}, \mathbf{y})) = \frac{1}{2}(d(\mathbf{x}, \mathbf{y}) + r) < r.$$

To pomeni, da je $\mathbf{z}$ notranja točka množice $K_r(\mathbf{x})$. Ker je bila $\mathbf{z}$ poljubna točka množice $K_r(\mathbf{x})$, je le-ta odprta množica.

Da dokažemo, da je $\bar{K}_r(\mathbf{x})$ zaprta množica, je dovolj dokazati, da so vse točke izven $\bar{K}_r(\mathbf{x})$ zunanje, saj bo to pomenilo, da je vsaka morebitna robna točka vsebovana v $\bar{K}_r(\mathbf{x})$. Vzemimo poljuben $\mathbf{y} \notin \bar{K}_r(\mathbf{x})$ in definirajmo

$r' = \frac{1}{2}(d(\mathbf{x},\mathbf{y}) - r)$. S podobnim premislekom kot zgoraj dokažemo, da je $K_{r'}(\mathbf{y}) \subseteq \bar{K}_r(\mathbf{x})^C$. To pa že pomeni, da je $\bar{K}_r(\mathbf{x})$ zaprta množica.

Za vajo premisli še, da je rob krogle $\bar{K}_r(\mathbf{x})$ ravno krožnica $S_r(\mathbf{x}) = \{\mathbf{y} : d(\mathbf{x},\mathbf{y}) = r\}$. ∎

Naj bo $A \subseteq \mathbb{R}^n$ poljubna množica. Tedaj množici $A \cup \partial A$ pravimo *zaprtje množice* A. Ni težko videti, da je zaprtje množice A zaprta množica in da nobena njena prava podmnožica, ki še vsebuje A, ni zaprta. Zaprtje množice A je torej najmanjša zaprta množica, ki vsebuje A.

2.3 Kompaktnost

Za podmnožice v $\mathbb{R}^n$, ki so vsebovane v kaki krogli $K_r(\mathbf{x})$, rečemo, da so omejene. Ostale množice so *neomejene*. Množicam, ki so tako zaprte kot omejene, rečemo, da so kompaktne. Nekaj zgledov kompaktnih množic:

- zaprte krogle $\bar{K}_r(\mathbf{x})$;
- krožnice $S_r(\mathbf{x})$;
- daljice.

In še nekaj množic, ki niso kompaktne:

- odprte krogle $K_r(\mathbf{x})$; (niso zaprte)
- polravnine v $\mathbb{R}^n$; (niso omejene)
- premice. (niso omejene)

2.4 Odprtost, zaprtost, kompaktnost – vaje

1. Določi notranjost, rob in zunanjost naslednjih podmnožic v $\mathbb{R}^2$. Katere od njih so zaprte, odprte, omejene, kompaktne? Določi njihova zaprtja.
   (a) $\{(x,y) \mid -1 < x < y \wedge -1 < y < 1\}$;
   (b) $\{(x,y) \mid -1 \leq x \leq y \wedge -1 \leq y \leq 1\}$;
   (c) $\{(x,x) \mid x \in \mathbb{R}\}$;
   (d) $\{(x,x) \mid x \in [-1,1)$;
   (e) $\{(x,y) \mid x,y \in \mathbb{Q}\}$;

Dokaži naslednje:

2. (a) Unija dveh zaprtih množic je zaprta množica;
   (b) Unija poljubne družine odprtih množic je odprta množica;
   (c) Unija poljubne družine zaprtih množic ni nujno zaprta množica;
   (d) Množica je odprta, če in samo če je njen komplement zaprta množica.

3 Funkcije

V tem razdelku se bomo ukvarjali predvsem z *realnimi funkcijami*, torej funkcijami, ki slikajo v množico realnih števil. Vsaka funkcija je podana z dvema parametroma: *definicijskim območjem* in *funkcijskim pravilom*, pri čemer je definicijsko območje poljubna množica (navadno podmnožica v $\mathbb{R}$ ali $\mathbb{R}^n$), funkcijsko pravilo pa napotek, ki vsakemu elementu iz definicijskega območja priredi neki element iz $\mathbb{R}$. Na primer, običajna kvadratna funkcija je definirana nad definicijskim območjem $\mathbb{R}$ in s pravilom $x \mapsto x^2$, ki smo ga vajeni pisati tudi kot $f(x) = x^2$.

Če želimo poudariti, da ima funkcija s funkcijskim predpisom f definicijsko območje enako $\mathcal{D}$, napišemo:

$$f\colon \mathcal{D} \to \mathbb{R}.$$

Domenimo se še, da funkcijam, ki so definirane na kaki podmnožici $\mathbb{R}^n$, rečemo funkcije n spremenljivk.

Kot vemo, pa v praksi definicijskega območja funkcije niti ne navajamo eksplicitno. Na primer, če napišemo $f(x) = x^2$, potihem že predpostavimo, da za definicijsko območje vzamemo največjo podmnožico množice realnih števil, za katere je zgornji predpis smiselen. Takšnemu območju rečemo tudi *naravno definicijsko območje*. Ker je kvadrat x^2 definiran za vsako realno število x, je tako naravno definicijsko območje predpisa $f(x) = x^2$ enako množici $\mathbb{R}$.

Funkciji $f\colon \mathcal{D} \to \mathbb{R}$ lahko priredimo graf

$$\Gamma f = \{(x, f(x)) \mid x \in \mathcal{D}\}.$$

Če je $\mathcal{D} \subseteq \mathbb{R}$, potem je graf Γf podmnožica ravnine $\mathbb{R}^2$, ki ima lastnost, da jo vsaka navpična premica seka seka v največ eni točki. Po drugi strani pa je vsaka podmnožica $\mathbb{R}^2$, ki ima to lastnost, graf kake funkcije.

Seveda je s funkcijo njen graf natanko določen. Velja pa tudi obratno: funkcija je natanko določena s svojim grafom. Zato je v matematiki navada, da pojem funkcije in njenega grafa kar enačimo. Če želimo pojem funkcije vpeljati povsem formalno, tedaj definiramo kar na takšen način:

Podmnožici f ravnine $\mathbb{R}^2$, za katero velja, da za vsak $c \in \mathbb{R}$ premica z enačbo $x = c$ seka f v največ eni točki, rečemo *funkcija*.

Poleg definicijskega območja $\mathcal{D}_f$ funkcije f, opazujemo tudi njeno *zalogo vrednosti*, definirano takole:

$$\mathcal{Z}_f = \{f(x) \mid x \in \mathcal{D}\},$$

oziroma splošneje, za $A \subseteq \mathcal{D}$ definiramo f-sliko množice A takole:

$$f^{\rightarrow}(A) = \{f(x) \mid x \in A\}.$$

Če je f funkcija ene spremenljivke in poznamo njen graf (kot množico v $\mathbb{R}^2$), potem definicijsko območje $\mathcal{D}_f$ dolobimo kot pravokotno projekcijo grafa na x-os, zalogo vrednosti $\mathcal{Z}_f$ pa kot pravokotno projekcijo grafa na y-os.

3.1 Injektivnost in inverz

Če je f funkcija n spremenljivk, potem že po definiciji velja, da za vsak $x \in \mathbb{R}^n$ obstaja največ en $y \in \mathbb{R}$, da je $y = f(x)$. Pri tem pa ni nujno res, da bi za vsak $y \in \mathbb{R}$ obstajal največ en x, za katerega je $y = f(x)$. Funkcijam, ki vseeno imajo to lasntost, rečemo, da so *injektivne*.

Definicija 3.1 Če za funkcijo n spremenljivk f velja, da za vsak $y \in \mathbb{R}$ obstaja največ en $x \in \mathbb{R}^n$, za katerega je $y = f(x)$, potem rečemo, da je funkcija f *injektivna*.

Funkcija f ene spremenljivke je injektivna, če vsaka vodoravna premica seka graf Γf v največ eni točki.

Pojem injektivnosti funkcije je tesno povezan tudi s pojmom *praslike*. Naj bo f funkcija in $b \in \mathbb{R}$. Tedaj množici

$$f^{\leftarrow}(b) = \{x \colon f(x) = b\}$$

rečemo f-praslika števila y. Podobno, če je $B \subseteq \mathbb{R}$, potem definiramo

$$f^{\leftarrow}(B) = \{x \colon f(x) \in B\}.$$

Zgled. *Naj bo* $f \colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. *Določi praslike elementov* $-1, 0$ *in* 4 *ter intervala* $[-4, 4]$.

Rešitev: $f^{\leftarrow}(-1) = \emptyset$, $f^{\leftarrow}(0) = \{0\}$, $f^{\leftarrow}(4) = \{-2, 2\}$ in $f^{\leftarrow}([-4, 4]) = [0, 2]$. ∎

Praslika $f^{\leftarrow}(b)$ je lahko prazna (če $b \notin \mathcal{Z}_f$), lahko vsebuje en sam element, lahko pa tudi več. Očitno velja, da je f injektivna, če in samo če za vsak $b \in \mathbb{R}$ praslika $f^{\leftarrow}(b)$ vsebuje največ en element.

Od tod sledi, da lahko vsaki injektivni funkciji f priredimo *inverzno funkcijo* f^{-1}, ki dani element $y \in \mathcal{Z}_f$ preslika v tisti natanko določeni element $x \in \mathbb{R}$, za katerega je $f^{\leftarrow}(y) = \{x\}$, oziroma $f(x) = y$.

Definicijsko območje inverzne funkcije f^{-1} je ravno $\mathcal{Z}_f$, njena zaloga vrednosti pa je $\mathcal{D}_f$:

$$\mathcal{Z}_{f^{-1}} = \mathcal{D}_f, \qquad \mathcal{D}_{f^{-1}} = \mathcal{Z}_f$$

Če je injektivna funkcija ene spremenljivke predstavljena z njenim grafom, potem njen inverz dobimo tako, da jo prezrcalimo preko simetrale lihih kvadrantov.

ZGLED. *Naj bo*

$$f\colon \mathbb{R} \to \mathbb{R}, \qquad f(x) = 2x - 1.$$

Iz formule vidimo, da gre za premico, ki gre skozi točki $T_1(0, -1)$ *in* $T_2(1, 1)$. *Sledi, da je* $\mathcal{D}_f = \mathcal{Z}_f = \mathbb{R}$. *Če takšno premico sekamo s poljubno vodoravno premico, dobimo v preseku natanko eno točko. Torej je* f *injektivna. Poiščimo ji inverz.*

Inverzna funkcija f^{-1} preslika v izbrani x ravno vrednost funkcije $f(x)$, torej $2x - 1$. Se pravi $f^{-1}(2x - 1) = x$ za vsak $x \in \mathcal{Z}_f = \mathbb{R}$. Če označimo $y = 2x - 1$ in izrazimo x z y, dobimo $x = \frac{y+1}{2}$. Se pravi, $f^{-1}(2x - 1) = f^{-1}(y) = x = \frac{y+1}{2}$. Če spremenljivko y preimenujemo v x, dobimo:

$$f^{-1}\colon \mathbb{R} \to \mathbb{R}, \qquad f^{-1}(x) = \frac{x+1}{2}.$$

Torej inverzna funkcija je spet premica, ki pa gre tokrat skozi točki $(-1, 0)$ in $(1, 1)$ (torej ravno skozi točki, ki ju dobimo iz T_1 in T_2 z zrcaljenjm preko simetrale lihih kvadrantov). Prepričajmo se še, da je $(f^{-1})^{-1} = f$. Po definiciji inverzne funkcije, preslika funkcija $(f^{-1})^{-1}$ v izbrani $x \in \mathbb{R}$ ravno vrednost funkcije $(f^{-1})(x)$, torej $\frac{x+1}{2}$. Če označimo $y = \frac{x+1}{2}$ in izrazimo x z y, dobimo $x = 2y - 1$. Se pravi, $(f^{-1})^{-1}(y) = 2y - 1$ in če preimenujemo spremenljivko y v x, ugotovimo, da je $(f^{-1})^{-1}(x) = f(x)$ za vsak $x \in \mathbb{R}$. Se pravi, $(f^{-1})^{-1} = f$. ∎

3.2 Operacije nad funkcijami

V tem razdelku si bomo ogledali več načinov, kako iz ene ali dveh funkcij dobiti novo funkcijo. Pričnimo z operacijo *skrčitve funkcije*.

Skrčitev funkcije

Če je f funkcija in A podmnožica defincijskega območja $\mathcal{D}_f$, potem lahko definiramo novo funkcijo

$$f|_A = \{(x, y) \colon x \in A, (x, y) \in f\},$$

ki ji rečemo *skrčitev funkcije f na množico A*. Ker je skčritev $f|_A$ očitno podmnožica funkcije f, to pomeni, da ostane funkcijsko pravilo funkcije f veljavno tudi pri njeni skrčitvi. Pri tem pa zmanjšamo definicijsko območje funkcije f. Skrčitev funkcije se od funkcije torej razlikuje le po tem, da ima manjše definicijsko območje.

Na prvi pogled operacija skrčitve nima pravega smisla: Zakaj bi krčili definicijsko območje funkcije? Glavni razlog tiči v tem, da lahko funkcija, ki ni injektivna, po skrčitvi postane injektivna. Injektivnim funkcijam pa lahko iščemo inverzne funkcije.

Zgled. *Oglejmo si funkcijo $f \colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, in ji skrčimo definicijsko območje tako, da bo postala injektivna. Kaj je inverz tako skrčene funkcije?*

Funkcija f ni injektivna, kot smo ugotovili v enem od prejšnjih zgledov. Če pa jo skrčimo na interval $[0, \infty)$, dobimo funkcijo

$$f|_{[0,\infty)} \colon [0, \infty) \to \mathbb{R}, \quad f(x) = x^2,$$

ki je injektivna. Njen inverz je običajna korenska funkcija, ki nenegativno realno število x preslika v kvadratni koren $\sqrt{x}$. Korenska funkcija $\sqrt{\ }$ torej ni inverz kvadratne funkcije f, kot bi kdo mislil, temveč njene skrčitve $f|_{[0,\infty)}$. Ker je $\mathcal{D}_{f|_{[0,\infty)}} = [0, \infty)$ in je $\mathcal{Z}_{f|_{[0,\infty)}} = [0, \infty)$, je tudi $\mathcal{D}_{\sqrt{\ }} = [0, \infty)$ in $\mathcal{Z}_{\sqrt{\ }} = [0, \infty)$. Graf funkcije $\sqrt{\ }$ dobimo tako, da graf skrčene kvadratne funkcije $f|_{[0,\infty)}$ prezrcalimo preko simetrale lihih kvadrantov. ∎

Kompozitum funkcij

Če sta $f \colon A \to \mathbb{R}$ in $g \colon B \to \mathbb{R}$ dve funkciji, lahko definiramo novo funkcijo z definicijskim območjem $C = g^{\leftarrow}(\mathcal{D}_f \cap \mathcal{Z}_g)$ in predpisom

$$(f \circ g)(x) = f(g(x)).$$

ZGLED. *Naj bo* $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ *in* $g\colon \mathbb{R} \to \mathbb{R}$, $g(x) = x + 1$. *Kakšni funkciji sta kompozita* $f \circ g$ *in* $g \circ f$*?*

Poiščimo najprej definicisjko območje kompozita $f \circ g$. Ker je $\mathcal{D}_f \cap \mathcal{Z}_g = \mathbb{R}$, je $g^{\leftarrow}(\mathcal{D}_f \cap \mathcal{Z}_g) = g^{\leftarrow}(\mathbb{R}) = \mathbb{R}$ in zato $\mathcal{D}_{f\circ g} = \mathbb{R}$. Funkcijsko pravilo dobimo tako, da v funkcijsko pravilo za f namesto x vstavimo $g(x) = x+1$. Dobimo

$$(f \circ g)(x) = (x + 1)^2 = x^2 + 2x + 1.$$

Oglejmo si že kompozitum v obratnem vrstnem redu, $g \circ f$. Ker je $\mathcal{D}_g \cap \mathcal{Z}_f = [0, \infty)$ in ker je $f^{\leftarrow}([0, \infty)) = \mathbb{R}$, je $\mathcal{D}_{g\circ f} = \mathbb{R}$. Funkcijsko pravilo funkcije $g \circ f$ dobimo tako, da v pravilo za g vstavimo $f(x) = x^2$ namesto. Dobimo:

$$(g \circ f)(x) = x^2 + 1.$$

■

Definicijsko območje in zalogo vrednosti kompozita najlažje določimo, če zaloga vrednosti druge funkcije sovpada z definicijskim območjem prve. Torej, če je $\mathcal{D}_f = \mathcal{Z}_g$, potem je $\mathcal{D}_{f\circ g} = \mathcal{D}_g$ in $\mathcal{Z}_{f\circ g} = \mathcal{Z}_f$.

Kompozitum inverzne funkcije f^{-1} z originalno funkcijo f je vedno identična funkcija. Natančneje, če je $f\colon A \to \mathbb{R}$ in je $B = \mathcal{Z}_f$, potem je

$$f \circ f^{-1} = \mathrm{id}_B \qquad \text{in} \qquad f^{-1} \circ f = \mathrm{id}_A.$$

Vsota, produkt in kvocient funkcij

Dvema realnima funkcijama realne spremenljivke pa lahko priredimo novo funkcijo tudi na drugačne načine. Naj bosta $f\colon A \to \mathbb{R}$ in $g\colon B \to \mathbb{R}$ funkciji in označimo $C = A \cap B$. Tedaj lahko definiramo:

- $(f + g) : C \to \mathbb{R}, \quad (f + g)(x) = f(x) + g(x),$
- $(fg) : C \to \mathbb{R}, \quad (fg)(x) = f(x) \cdot g(x),$
- $\frac{f}{g} : C \setminus \{x \mid g(x) = 0\} \to \mathbb{R}, \quad (\frac{f}{g})(x) = \frac{f(x)}{g(x)}.$

ZGLED. *Naj bosta f in g funkciji podani z definicijskim območji in predpisom takole:*

$$f\colon [0,\infty) \to \mathbb{R},\ f(x) = x+2; \qquad g\colon \mathbb{R} \to \mathbb{R},\ g(x) = x^2 - 1.$$

Poišči njuni vsoto, produkt in oba kvocienta.

Očitno je:

- $(f+g)\colon [0,\infty) \to \mathbb{R}, \qquad (f+g)(x) = x + 2 + x^2 - 1 = x^2 + x - 1,$
- $(fg)\colon [0,\infty) \to \mathbb{R}, \qquad (fg)(x) = (x+2)(x^2-1) = x^3 + 2x^2 - x - 2,$
- $\frac{f}{g}\colon [0,\infty) \setminus \{1\} \to \mathbb{R}, \qquad \frac{f}{g}(x) = \frac{x+2}{x^2-1}.$

■

3.3 Vaje iz funkcij na splošno

1. Določi naravna definicisjka območja naslednjih predpisov:
   (a) $f(x) = \frac{2-x}{1-x^2}$;
   (b) $f(x) = \sqrt{x^2-1}$;
   (c) $f(x) = \log(x^2 - 3x - 4)$;
   (d) $f(x,y) = \frac{x+y}{x-y}$;
   (e) $f(x,y) = \sqrt{1-x^2-y^2}$.

2. Naj bo $f\colon \mathcal{D} \to \mathbb{R}$ poljubna funkcija ene spremenljivke. Za vajo premisli ali za poljubni množici $A, B \subseteq \mathbb{R}$ velja naslednje. Za enakosti, ki ne držijo, poišči protiprimer in morebitno dodatno lastnost f, ki bi zagotovila enakost. Ali velja vsaj vsebovanost v kako od obeh smeri?
   (a) $f^{\leftarrow}(A \cap B) = f^{\leftarrow}(A) \cap f^{\leftarrow}(B)$;
   (b) $f^{\leftarrow}(A \cup B) = f^{\leftarrow}(A) \cup f^{\leftarrow}(B)$;
   (c) $f^{\rightarrow}(A \cap B) = f^{\rightarrow}(A) \cap f^{\rightarrow}(B)$;
   (d) $f^{\rightarrow}(A \cup B) = f^{\rightarrow}(A) \cup f^{\rightarrow}(B)$.

   NAMIG: Veljajo točke (a), (b) in (d), točka (c) pa velja le kot vsebovanost z leve proti desni, v celoti (kot enakost) pa le v primeru, ko je f injektivna.

3. Za naslednje funkcije ugotovi, ali so injektivne. Če so, jim poišči inverz. Če niso, jim smiselno skrči definicijsko območje, da postanejo injektivne, ter poišči inverzne funkcije le-tem skrčenim funkcijam.

   (a) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = \frac{1}{1+x^2}$;

   (b) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 - x - 2$;

   (c) $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = \log(1 + x^2)$.

3.4 Pregled elementarnih funkcij

Konstantne funkcije

Za vsako število $c \in \mathbb{R}$ lahko definiramo *konstantno funkcijo* $\gamma_c \colon \mathbb{R} \to \mathbb{R}$, definirano s predpisom $\gamma_c(x) = c$.

Konstantne funkcije niso niti injektivne niti surjektivne. Zaloga vrednosti vsebuje natanko eno število: c.

Identična funkcija

Identična funkcija $\mathrm{id} \colon \mathbb{R} \to \mathbb{R}$ je definirana s predpisom $\mathrm{id}(x) = x$. Identična funkcija je bijektivna in je enaka svojemu inverzu: $\mathrm{id}^{-1} = \mathrm{id}$.

Potenčne funkcije in korenske funkcije

Prudukt identične funkcije s seboj je *kvadratna funkcija*:

$$\mathrm{id} \cdot \mathrm{id} \colon \mathbb{R} \to \mathbb{R}\,, \qquad (\mathrm{id} \cdot \mathrm{id})(x) = \mathrm{id}(x) \cdot \mathrm{id}(x) = x \cdot x = x^2\,.$$

Če tako dobljeno kvadratno funkcijo še enkrat pomnožimo z identiteto, dobimo *kubično funkcijo*:

$$\mathrm{id} \cdot \mathrm{id} \cdot \mathrm{id} \colon \mathbb{R} \to \mathbb{R}\,, \qquad (\mathrm{id} \cdot \mathrm{id} \cdot \mathrm{id})(x) = \mathrm{id}(x) \cdot \mathrm{id}(x) \cdot \mathrm{id}(x) = x \cdot x \cdot x = x^3\,.$$

V splošnem, če identiteto n-krat pomnožimo samo s seboj, dobimo *potenčno funkcijo* eksponenta $n \in \mathbb{N}$.

Potenčna funkcija f_{2n-1} z lihim ekponentom

$$f_{2n-1} \colon \mathbb{R} \to \mathbb{R}, \qquad x \mapsto x^{2n-1},$$

je injektivna, zato ji lahko poiščemo inverzno funkcijo, ki jo imenujemo *korenska funkcija* stopnje $2n-1$ in označimo takole:

$$\sqrt[2n-1]{\ } \colon \mathbb{R} \to \mathbb{R}\,.$$

Potenčna funkcija f_{2n} s sodim eksponentom

$$f_{2n} \colon \mathbb{R} \to \mathbb{R}, \qquad x \mapsto x^{2n},$$

ni injektivna. Slika $\mathcal{Z}_{f_{2n}}$ je enaka množici $[0, \infty)$. Če funkciji skrčimo definicijsko območje na interval $[0, \infty)$, dobimo injektivno funkcijo

$$f_{2n}|_{[0,\infty)} \colon [0, \infty) \to \mathbb{R}, \qquad x \mapsto x^{2n},$$

katere inverzna funkcija je korenska funkcija sode stopnje:

$$\sqrt[2n]{\ } : [0, \infty) \to \mathbb{R}\,.$$

Z nekaj dela bi se prepričali, da pri poljubnih $a > 0$ in $m, n \in \mathbb{N}$ velja naslednja enakost:

$$\sqrt[m]{a^n} = \sqrt[m]{a}^n.$$

To nas napelje na naslednjo poenostavitev zapisa kompozita korenske in potenčne funkcije:

$$a^{\frac{n}{m}} := \sqrt[m]{a^n} = \sqrt[m]{a}^n.$$

S tem smo razširili pojem potence pozitivnega realnega števila z naravnih eksponentov na pozitivne racionalne potence. Z dogovoroma

$$a^0 := 1 \quad \text{in} \quad a^{-r} := \frac{1}{a^r}\,, \qquad a, r > 0,\ r \in \mathbb{Q}$$

razširimo definicijo potence a^r pozitivnega realnega števila a na vse racionalne eksponente r.

Naj bo nazadnje x poljubno realno število. Naj bo $R_x = \{r \in \mathbb{Q} \mid r < x\}$ in označimo z a^{R_x} množico $\{a^r \mid r \in R_x\}$. Če je $a < 1$, je množica a^{R_x} navzdol omejena, če pa je $a \geq 1$, je a^{R_x} navzgor omejena. V prvem primeru definiramo $a^x := \inf a^{R_x}$, v drugem pa $a^x := \sup a^{R_x}$. S tem smo definicijo potence a^x pozitivnega realnega števila a razširili z racioanlnih na poljubne realne eksponente x.

Ni se težko prepričati, da pri tem ostanejo v veljavi vsa običajna računska pravila - pri poljubnih $a, b > 0$, $x, y \in \mathbb{R}$ velja:

$$(a^x)^y = a^{xy}\,, \qquad a^x \cdot a^y = a^{x+y}\,, \qquad \frac{a^x}{a^y} = a^{x-y}\,, \qquad (ab)^x = a^x b^x.$$

Polinomi

Če nekaj funkcij $f_1, f_2, \ldots, f_n$ pomnožimo s konstantnimi funkcijami $\gamma_{c_1}, \gamma_{c_2}, \ldots, \gamma_{c_n}$, nato pa dobljene funkcije seštejemo:

$$\gamma_{c_1} f_1 + \gamma_{c_2} f_2 + \ldots + \gamma_{c_n} f_n,$$

dobimo funkcijo, ki ji pravimo *linearna kombinacija funkcij* $f_1, f_2, \ldots, f_n$ s koeficienti $c_1, c_2, \ldots, c_n$.

Linearni kombinaciji potenčih funkcij in konstantne funkcije γ_1 rečemo *polinom*:

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \qquad a_0, a_1, \ldots, a_n \in \mathbb{R}.$$

Z drugimi besedami, polinomi so funkcije, ki jih dobimo iz konstant in identitete z množenjem in seštevanjem.

Ker so konstantne funkcije in identiteta definirane za vsa realna števila, so zato za vsa realna števila definirani tudi njihovi produkti in vsote, torej polinomi. Polinomi (razen izjemoma) niso injektivni.

Če je p polinom, množici $\{x \mid p(x) = 0\}$ rečemo *množica ničel polinoma* p. Iskanje ničel polinoma je načeloma težak postopek, in če nimamo velike sreče, pri $n \geq 5$ celo nerešljiv problem. Približke ničel lahko sicer poiščemo s pomočjo različnih numeričnih prijemov (ki jih tu ne bomo omenjali). Če pa ima polinom kako racionalno ničlo, jo lahko poiščemo s pomočjo naslednje trditve.

Trditev 3.2 *Naj bo* $p(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ *poljuben polinom stiopnje* n *s celimi koeficienti* a_i. *Če je* $\frac{s}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$, *racionalna ničla polinoma* p *(in sta števili* s *in* q *tuji), tedaj* s *deli* a_0, q *pa* a_n.

Ko poiščemo kako racionalno ničlo, denimo $r \in \mathbb{Q}$, $p(r) = 0$, lahko polinom $p(x)$ delimo z linearnim polinomom $x - r$ in dobimo polinom $p_1(x)$ stopnje $n - 1$. Ničle polinoma $p_1(x)$ so hkrati ničle polinoma $p(x)$ in vsaka ničla polinoma $p(x)$ različna od r je hkrati ničla polinoma $p_1(x)$. Iskanje ničel polinoma $p(x)$ lahko torej nadaljujemo z iskanjem ničel polinoma $p_1(x)$.

Preverjanje, ali je dano racionalno število r res ničla polinoma, in deljenje s polinomom $x - r$ lahko opravimo s pomočjo *Hornerjevega algoritma*.

Racionalne funkcije

Če sta p in q dva polinmoma, potem funkciji $\frac{p}{q}$ rečemo *racionalna funkcija*. Naj bo P množica tistih realnih števil x, za katere je $q(x) = 0$. Tedaj je definicijsko območje racionalne funkcije $\frac{p}{q}$ enako $\mathbb{R} \setminus P$. Številom P rečemo poli funkcije $\frac{p}{q}$. Racionalne funkcije v splošnem niso niti injektivne niti surjektivne.

Eksponentna funkcija in logaritemska funkcija

Naj bo $a > 1$ in $a \neq 1$. V razdelku o potenčni funkciji smo definirali potenco a^x za vsako realno število x. Tedaj je *eksponentna funkcija z osnovo* a definirana takole:

$$\exp_a \colon \mathbb{R} \to \mathbb{R}, \qquad \exp_a(x) = a^x.$$

Naravno definicijsko območje ekponentne funkcije so vsa relna števila. Lastnosti:

i) $\mathcal{Z}_{\exp_a} = (0, \infty)$,

ii) $\exp_a$ je naraščajoča za $a > 1$ in padajoča za $a < 1$, (zgled za $a = 1/2$ in $a = 2$)

iii) Eksponentna funkcija je injektivna.

Zadnja lastnost nam omogoča, da definiramo inverz eksponetne funkcije. Inverzni funkciji pravimo *logaritemska funkcija z osnovo* a:

$$\log_a \colon (0, \infty) \to \mathbb{R}\,, \qquad \log_a = \exp_a^{-1}\,.$$

Lastnosti:

i) $\mathcal{Z}_{\log_a} = \mathcal{D}_{\exp_a} = \mathbb{R}$,

ii) $\log_a$ je naraščajoča za $a > 1$ in padajoča za $a < 1$, (zgled za $a = 1/2$ in $a = 2$)

iii) Logaritemska funkcija je bijektivna.

V informatiki igrata med ekponetnimi in logaritemskimi funkcijami najpomembnejšo vlogo tisti z osnovo 2. Zaradi dejstva, da v vsakdanjem življenju običajno uporabljamo desetiški številski sistem, je poleg osnove 2 pogosto uporabljana tudi osnova 10. V tehnični literaturi pogosto z oznako log označujejo ravno logaritem $\log_{10}$. Mi se bomo domenili drugače. V matematiki se namreč izkaže, da je med vsemi osnovami najprikladnejša osnova e, kjer je $e = \lim(1 + 1/n)^n$. Logaritmu z osnovo e rečemo tudi *naravni logaritem*. Za našo rabo bomo zapis osnove pri naravnem logaritmu izpuščali in pisali kar log namesto $\log_e$, desetiški logaritem pa bomo striktno pisali z $\log_{10}$. Omenimo še, da je v tehnični literaturi naravni logaritem navadno označen z ln.

Prehajanje med logaritmi z različnimi osnovami nam omogoča formula

$$\log_a(x) = \frac{\log_b(x)}{\log_b(a)}.$$

Poleg zgornje formule veljajo še naslednja računska pravila:

$$\log_a(xy) = \log_a(x) + \log_a(y)\,, \log_a(\frac{x}{y}) = \log_a(x) - \log_a(y)\,, \log_a(b^x) = x \log_a(b).$$

Kotne funkcije

Kotnih funkcij ne bomo definirali na povsem korekten način, saj se bomo sklicevali na geometrijske pojme, kot so: dolžina krivulje, kot in orientacija.

Naj bo $K = \{(x, y) \mid x^2 + y^2\}$ enotska krožnica v ravnini $\mathbb{R}^2$. Naj bo $x \in \mathbb{R}$ in odmerimo dolžino $|x|$ od točke $(1, 0)$ po krožnici K v nasprotni smeri urinega kazalca (če je $x \geq 0$) oziroma v smeri urinega kazalca (če je $x < 0$). Ordinato točke, do katere prispemo, označimo s $\sin x$ in jo imenujemo *sinus kota* x. Abscisa dobljene točke je tedaj *kosinus* kota x in ga označimo s $\cos x$. Na ta način dobimo *kotni funkciji* sinus in kosinus:

$$\sin\colon \mathbb{R} \to \mathbb{R}\,, \qquad \cos\colon \mathbb{R} \to \mathbb{R}\,.$$

Z definicijskim območjem enakim množici $\mathbb{R}$ in zalogo vrednosti $[-1, 1]$.

Iz geometrijskih razlogov veljajo naslednje zveze med sinusno in cosinusno funkcijo:

- $\cos(x) = \sin(\frac{\pi}{2} - x)$,
- $\sin^2(x) + \cos^2(x) = 1$,
- $\sin(x + y) = \sin(x)\cos(y) + \cos(x)\sin(y)$,
- $\cos(x + y) = \cos(x)\cos(y) - \sin(x)\sin(y)$,
- $\sin(-x) = -\sin(x)$,
- $\cos(-x) = \cos(x)$,
- $|\cos(\frac{x}{2})| = \sqrt{\frac{1}{2}(1 + \cos(x)}$,
- $|\sin(\frac{x}{2})| = \sqrt{\frac{1}{2}(1 - \cos(x)}$,
- $\sin(x) + \sin(y) = 2\sin(\frac{x+y}{2})\cos(\frac{x-y}{2})$,
- $\cos(x) + \cos(y) = 2\cos(\frac{x+y}{2})\cos(\frac{x-y}{2})$,
- $\cos(x) - \cos(y) = -2\sin(\frac{x+y}{2})\sin(\frac{x-y}{2})$,

Poleg funkcij sin in cos med kotne funkcije prištevamo tudi funkciji

$$\tan = \frac{\sin}{\cos} \qquad \text{in } \operatorname{ctg} = \frac{\cos}{\sin}.$$

Pri tem velja:

i) $\mathcal{D}_{\tan} = \mathbb{R} \setminus \{\pi/2 + k\pi \mid k \in \mathbb{Z}\}$, $\mathcal{D}_{\mathrm{ctg}} = \mathbb{R} \setminus \{k\pi \mid k \in \mathbb{Z}\}$;

ii) $\mathcal{Z}_{\tan} = \mathcal{Z}_{\mathrm{ctg}} = \mathbb{R}$;

iii) $\tan(x+y) = (\tan(x) + \tan(y))/(1 - \tan(x)\tan(y))$;

iv) $\tan(-x) = -\tan(x)$, $\mathrm{ctg}(-x) = -\mathrm{ctg}(x)$;

Nekaj nalog:

1. Izračunaj $\cos(\frac{x}{2})$, če veš, da je $\sin(x) = -\frac{1}{4}$ in $\frac{3\pi}{4} \leq x \leq 2\pi$;
2. Reši enačbe:
   (a) $2\sin^2(x) + \sin(x) = \cos(x) + \sin(2x)$;
   (b) $4\sin(x) + 3\cos^2(x) = 3$;
   (c) $\sin(2x) = \sin(2x + \frac{\pi}{3})$.

Kotne funkcije so periodične.

DEFINICIJA 3.3 Funkcija $f\colon \mathbb{R} \to \mathbb{R}$ je periodična s periodo ω, če za vsak $x \in \mathbb{R}$ velja $f(x+\omega) = f(x-\omega) = f(x)$. Perioda ω je osnovna, če ni naraven večkranik kake druge periode.

TRDITEV 3.4 *Funkciji* sin *in* cos *sta periodični z osnovno periodo* 2π*, funkciji* tan *in* ctg *pa z osnovno periodo* π*.*

Ker so kotne funkcije periodične, seveda niso injektivne. Če želimo doseči injektivnost kotnih funkcij, moramo skrčiti njihovo definicijsko območje. Na ta način pridemo do inverznih funkcij, ki jim pravimo *krožne funkcije*.

Krožne funkcije

Skrčimo definicijsko območje funkcije sin na interval $[-\pi/2, \pi/2]$. Skrčena funkcija $\sin|_{[-\pi/2,\pi/2]}$ je naraščajoča in zato injektivna. Njen inverz označimo

$$\arcsin\colon [-1,1] \to \mathbb{R}\,, \qquad \arcsin = (\sin|_{[-\pi/2,\pi/2]})^{-1}.$$

Podobno dobimo funkcije arccos, arctan in arcctg kot inverze skrčitev funkcij cos, tan in ctg:

$$\arccos\colon [-1,1] \to \mathbb{R}\,, \qquad \arccos = (\cos|_{[0,\pi]})^{-1}\,,$$

$$\arctan\colon \mathbb{R} \to \mathbb{R}\,, \qquad \arctan = (\tan|_{[-\pi/2,\pi/2]})^{-1}\,,$$

$$\mathrm{arcctg}\colon \mathbb{R} \to \mathbb{R}\,, \qquad \mathrm{arcctg} = (\mathrm{ctg}|_{[0,\pi]})^{-1}\,.$$

4 Teorija števil

Teorija števil se ukvarja s *celimi števili*. Množico celih števil zapišemo kot

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$$

in jo razdelimo na množico naravnih števil

$$\mathbb{N} = \{1, 2, 3, \ldots, \},$$

množico negativnih celih števil

$$\mathbb{N}^- = \{-1, -2, -3, \ldots\}$$

in množico, ki vsebuje le število 0.

4.1 Delitelji in večkratniki

Med najosnovnejše pojme teorije števil sodi pojem deljivosti.

Definicija 4.1 Celo število m deli celo število n, če in samo če obstaja takšno celo število k, da je $n = km$. V tem primeru pišemo $m \mid n$ in rečemo, da je m delitelj števila n, da je n deljiv s številom m in da je n večkratnik števila m.

Opazimo, da je 0 večkratnik vsakega celega števila (saj je $0 = 0 \cdot m$ za vsak $m \in \mathbb{Z}$) in da je edino število, ki ga 0 deli, število 0 (saj je $k \cdot 0 = 0$ za vsak $k \in \mathbb{Z}$). Po drugi stran pa števili 1 in -1 delita prav vsa cela števila (saj je $n = n \cdot 1$ in $n = (-n) \cdot (-1)$ za vsak $n \in \mathbb{Z}$) in poleg števil 1 in -1 nimata prav nobenih drugih deliteljev.

Naj bosta m in n poljubni števili. Tedaj največje naravno število, ki deli tako m kot n označimo z $\gcd(m, n)$ in ga imenujemo *največji skupni delitelj* števil m in n. (Oznaka gcd izvira iz angleškega poimenovanja *greatest common divisor*). Najmanjše naravno število, ki je deljivo tako z m kot z n, pa imenujemo *najmanjši skupni večkratnik* števil m in n in ga označimo z $\mathrm{lcm}(m, n)$ (angl. *least common multiple*). Celi števili m in n sta *tuji*, če velja $\gcd(m, n) = 1$.

Omenimo še, da je relacija deljivosti tranzitivna relacije. Natančneje, velja naslednje:

Trditev 4.2 *Če $r \mid m$ in $m \mid n$, tedaj $r \mid n$.*

Dokaz: Iz definicije deljivosti sledi, da obstajata celi števili k in ℓ, za kateri je $m = kr$ in $n = \ell m$. Tedaj pa je $n = \ell kr$, od koder sledi, da je n deljiv z r. ∎

Funkciji div in mod

Naj bo n poljubno celo število in m poljubno neničelno celo število. Kot smo že opazili, kvocient n/m tedaj ni nujno celo število, kar pomeni, da v množici celih števil običajna operacija deljenje ni dobro definirana. Namesto običajnega deljenja zato vpeljemo operacijo celoštevilskega deljenja, ki številoma n in m priredi *celoštevilski količnik* $k = n \operatorname{div} m$ ter *ostanek* $r = n \bmod m$. Celoštevilski količnik k in ostanek r sta natanko določena s pogojem:

$$n = km + r; \quad k, r \in \mathbb{Z},\ 0 \leq r \leq |m| - 1.$$

4.2 Praštevila

DEFINICIJA 4.3 Od 1 različno naravno število je praštevilo, če poleg samega sebe in 1 ne premore nobenega drugega naravnega delitelja.

TRDITEV 4.4 *Vsako od* 1 *različno naravno število je deljivo z vsaj enim praštevilom.*

DOKAZ: Dokaz bo potekal z indukcijo na naravno število n. Za $n = 1$ trditev ne trdi ničesar, za $n = 2$ pa je pravilna, saj je 2 res deljiv s praštevilom, namreč kar z 2. Privzemimo torej, da je $n \geq 3$ in da je vsako naravno število, ki je manjše od n, deljivo s kakim praštevilom. Dokazati moramo, da tedaj isto velja tudi za število n.

Če je n praštevilo, tedaj je deljivo s praštevilom n. Če n ni praštevilo, tedaj je deljivo s kakim naravnim številom m, $2 \leq m \leq n-1$. Po indukcijski predpostavki je m deljiv z nekim praštevilom p. Tedaj pa iz Trditve 4.2 sledi, da p deli n. ∎

TRDITEV 4.5 *Praštevil je neskončno mnogo.*

DOKAZ: Pa recimo, da jih je le končno mnogo; označimo jih s p_1, $p_2, \ldots, p_n$. Oglejmo si število $m = p_1 p_2 \ldots p_m + 1$. Očitno je m večji od vsakega od praštevil p_i, zato ni praštevilo. Iz Trditve 4.4 tedaj sledi, da je p deljiv s kakim praštevilom; denimo s p_i. Tedaj je

$$m = p_1 \ldots p_{i-1} p_i p_{i+1} \ldots p_m + 1 = k p_i$$

za kak $k \in \mathbb{Z}$, in zato $1 = p_i(k - p_1 \ldots p_{i-1} p_{i+1} \ldots p_m)$. To pa je nemogoče, saj 1 ni deljiv z nobenim praštevilom, torej tudi ne s p_i. ∎

DEFINICIJA 4.6 Naj bodo $p_1, p_2, \ldots, p_k$ poljubna, paroma različna praštevila in $\alpha_1, \ldots, \alpha_k$ poljubna naravna števila. Tedaj zapisu

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

pravimo razcep števila n na prafaktorje.

TRDITEV 4.7 *Vsako od* 1 *različno naravno število premore razcep na prafaktorje. Razcep je do vrstnega reda faktorjev en sam.*

Včasih je priročno v razcep naravnega števila n vrini še kako praštevilo, s katerim n ni deljiv; tako praštevilo mora seveda v razcepu nastopati z eksponentom 0. Na ta način omogočimo, da poljubni dve naravni števili $a, b \in \mathbb{N}$ zapišemo z naborom istih praštevil: $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, $\alpha_i, \beta_i \geq 0$. S pomočjo razcepa na prafaktorje lahko dokažemo več zanimivih trditev:

TRDITEV 4.8 *Naravno število m deli naravno število n, če in samo če za njuna razcepa na prafaktorje velja naslednje:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ b_i \leq a_i \text{ za vsak } i \in \{1, \ldots, k\}.$$

TRDITEV 4.9 *Naj bodo a, b in c poljubna cela števila. Če sta a in b tuji števili in če a deli bc, tedaj a deli c.*

TRDITEV 4.10 *Naj bosta a in b poljubni celi števili in c njun skupni delitelj. Tedaj je* $\gcd(\frac{a}{c}, \frac{b}{c}) = \frac{\gcd(a,b)}{c}$.

Iz zgornje trditeve neposredno sledi, da sta za poljubni celi števili a in b števili $\frac{a}{\gcd(a,b)}$ in $\frac{b}{\gcd(a,b)}$ tuji.

Računanje gcd **in** lcm **s pomočjo razcepa na prafaktorje**

Vzemimo naravni števili m in n. Če je katero od njih enako 1 (denimo $n = 1$), potem je očitno

$$\gcd(m, 1) = 1 \quad \text{in} \quad \operatorname{lcm}(m, 1) = m.$$

Predpostavimo sedaj, da je $m, n \geq 2$. Naj bodo $p_1, \ldots, p_n$ tista praštevila, ki delijo tako m kot n. Tedaj imata razcepa števili m in n na prafaktorje obliko

$$\begin{aligned} m &= p_1^{\alpha_1} \cdots p_n^{\alpha_n} \cdot q_1^{\delta_1} \cdots q_k^{\delta_k}, \\ n &= p_1^{\beta_1} \cdots p_n^{\beta_n} \cdot r_1^{\gamma_1} \cdots r_\ell^{\gamma_\ell}, \end{aligned}$$

pri čemer je $q_i \neq r_j$ za vsak par indeksov i, j. V tem primeru velja:

$$\begin{aligned} \gcd(m,n) &= p_1^{\min\{\alpha_1,\beta_1\}} \cdots p_n^{\min\{\alpha_n,\beta_n\}} \\ \operatorname{lcm}(m,n) &= p_1^{\max\{\alpha_1,\beta_1\}} \cdots p_n^{\max\{\alpha_n,\beta_n\}} \cdot q_1^{\delta_1} \cdots q_k^{\delta_k} \cdot r_1^{\gamma_1} \cdots r_\ell^{\gamma_\ell} \end{aligned}$$

Od tod neposredno sledi naslednje:

TRDITEV 4.11 *Za poljubni naravni števili m in n velja enakost*

$$\gcd(m,n) \cdot \operatorname{lcm}(m,n) = mn.$$

4.3 Diofantske enačbe

Enačbe, pri katerih iščemo zgolj celoštevilske rešitve, se imenujejo *diofantske enačbe*. Oglejmo si nekoliko podrobneje linearne diofantske enačbe, torej enačbe oblike

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c, \qquad (*)$$

kjer so a_i, $i = 1, \ldots, n$, in c poljubna cela števila, x_i, $i = 1, \ldots, n$, pa neznanke. Rešitev enačbe $(*)$ je vsaka n-terica $(x_1, \ldots, x_n)$ celih števil, ki zadošča $(*)$.

Oglejmo si najprej primer, ko imamo eno samo neznanko:

$$ax = c, \;\; a \neq 0. \qquad (+)$$

Če bi dopuščali tudi racionalne rešitve, bi zgornja enačba imela natanko eno rešitev, namreč $x = c/a$. Ker pa nas pri diofantskih enačbah zanimajo le celoštevilske rešitve, bo imela diofantska enačba $(+)$ rešitev tedaj in le tedaj, ko bo a delil c (in bo zato c/a celo število).

Nekoliko bolj zanimiva je linearna diofantska enačba z dvema neznankama:

$$ax + by = c, \;\; a, b \neq 0. \qquad (\times).$$

Premislimo najprej, kako je z racionalnimi rešitvami. Ker je $a \neq 0$, lahko zgornjo enakost preoblikujemo v $x = (c - by)/a$. To pomeni, da lahko za poljuben y najdemo ustrezen x, tako da bo par (x, y) rešil enačbo $(\times)$. Racionalnih rešitev enačbe $(\times)$ je torej neskončno mnogo pri poljubnih koeficientih a, b in c.

Če pa zahtevamo, da so rešitve celoštevilske, pa se pojavi težava, saj število $x = (c - by)/a$ niti pri celoštevilskih y ni nujno celo. Velja pa naslednje:

IZREK 4.12 *Diofantska enačba*

$$ax + by = c, \;\; a, b \neq 0, \qquad (\times)$$

je rešljiva, če in samo če je število c deljivo z največjim skupnim deliteljem števil a in b. V tem primeru je rešitev neskončno mnogo. Če je (x_0, y_0) neka rešitev enačbe $(\times)$, so ostale rešitve enačbe $(\times)$ oblike

$$x = x_0 - kb', \;\; y = y_0 + ka', \qquad k \in \mathbb{Z},$$

kjer je $a' = a/\gcd(a, b)$ in $b' = b/\gcd(a, b)$.

DOKAZ: Obstoj rešitve, v primeru, da $\gcd(a, b)$ deli c, bomo pokazali v nadaljevanju, ko bomo predstavili postopek za iskanje rešitve. Osredotočimo se torej na preostale trditve iz izreka.

Denimo, da je enačba $(\times)$ rešljiva. Tedaj obstajata takšni števili $x_0, y_0 \in \mathbb{Z}$, da je $ax_0 + bx_0 = c$. Če je m poljuben skupni delitelj števil a in b, tedaj je $a = rm$ in $b = tm$ za neki celi števili r in t, in zato

$$c \;=\; ax_0 + by_0 \;=\; rmx_0 + tmy_0 \;=\; (rx_0 + ty_0)m.$$

Od tod sledi, da vsak skupni delitelj števil a in b (tudi $\gcd(a, b)$) deli c.

Naj bo (x_0, y_0) poljubna rešitev enačbe $(\times)$ in $x = x_0 - kb'$, $y = y_0 + ka'$ za neko celo število k. Tedaj je

$$ax + by = a(x_0 - kb') + b(y_0 + ka') = ax_0 + by_0 = c,$$

kar dokazuje, da je tudi (x, y) rešitev enačbe.

Dokazati moramo le še, da je res vsaka rešitev enačbe $(\times)$ oblike $x = x_0 + kb'$, $y = y_0 - ka'$. Pa naj bo (x_1, y_1) še neka rešitev enačbe $(\times)$. Tedaj je $(ax_0 + by_0) - (ax_1 + by_1) = 0$, in zato $a(x_0 - x_1) = b(y_1 - y_0)$. Če iz slednje enakosti pokrajšamo največji skupni večkratnik števil a in b, dobimo

$$a'(x_0 - x_1) = b'(y_1 - y_0).$$

Iz trditve 4.10 sledi, da sta števili a' in b' tuji. Tedaj pa iz trditve 4.9 sledi, da je $k = (y_1 - y_0)/a'$ celo število. Pri tem velja

$$x_0 - kb' = x_0 - \frac{(y_1 - y_0)b'}{a'} = x_0 - (x_0 - x_1) = x_1, \quad y_0 + ka' = y_0 + (y_1 - y_0) = y_1,$$

in rešitev (x_1, y_1) je res zahtevane oblike. ∎

4.4 Razširjeni Evklidov algoritem

Razširjeni Evklidov algoritem uporabljamo za računanje največjege skupnega delitelja danih celih števil in za reševanje linearnih diofanstskih enačb z dvema neznankama. Sam postopek lahko opišemo takole:

VHODNI PODATEK: Par (a, b) neničelnih celih števil.

$(r_0, x_0, y_0) := (a, 1, 0)$;
$(r_1, x_1, y_1) := (b, 0, 1)$;
$i := 1$;
dokler $r_i \neq 0$ izvajaj
    $i := i + 1$;
    $k_i := r_{i-2}$ div r_{i-1};
    $(r_i, x_i, y_i) := (r_{i-2}, x_{i-2}, y_{i-2}) - k_i(r_{i-1}, x_{i-1}, y_{i-1})$;
konec zanke

VRNI: $(r_{i-1}, x_{i-1}, y_{i-i})$.

TRDITEV 4.13 *Naj bosta a in b neničelni celi števili. Tedaj trojica (d, x, y), ki jo vrne razširjeni Evklidov algoritem z vhodnim podatkom (a, b), zadošča pogoju*

$$ax + by = d, \quad d = \gcd(a, b).$$

DOKAZ: Za števila r_i, a_i in b_i iz opisa razširjenega evklidovega algoritma za vsak $i \geq 0$ z indukcijo dokažimo enakost

$$ax_i + by_i = r_i. \tag{$*$}$$

Ta enakost očitno velja za $i = 0$ in $i = 1$, saj je $ax_0+by_0 = a\cdot 1+b\cdot 0 = a = r_0$ in $ax_1+by_1 = a\cdot 0+b\cdot 1 = b = r_1$. Denimo sedaj, da je $i \geq 2$, in privzemimo, da enakost $(*)$ velja za vse indekse manjše od izbranega i. Tedaj

$$ax_i+by_i = a(x_{i-2}-k_ix_{i-1})+b(y_{i-2}-k_iy_{i-1}) = ax_{i-2}+by_{i-2}-k(ax_{i-1}+by_{i-1}).$$

Po indukcijski predpostavki je slednje enako $r_{i-2} - kr_{i-1} = r_i$. S tem smo dokazali enakost $(*)$, in zato tudi $ax + by = d$.

Dokazati moramo še, da je $\gcd(a, b) = d$. V izreku 4.12 smo že dokazali, da iz enakosti $ax + by = d$ sledi, da $\gcd(a, b)$ deli d. Dokazati moramo še, da d deli tako a kot b (in zato tudi $\gcd(a, b)$).

Razširjeni Evklidov algoritem se ustavi takrat, ko vrednost ostanka r_i pade na nič, število d, ki ga algoritem vrne, pa je zadnji neničelni ostanek

(označimo njegov indeks z n). Ker je $0 = r_{n+1} = r_{n-1} - kr_n = r_{n-1} - kd$, vidimo, da d deli r_{n-1}. Dokažimo, da d deli r_i za vsak $i \in \{0, \ldots, n\}$. Pa denimo, da temu ni tako, in vzemimo največji indeks j, za katerega r_n ne deli r_j (seveda $j \leq n-2$). Ker je $r_{j+2} = r_j - kr_{j+1}$, je $r_j = r_{j+2} + kr_{j+1}$. Iz definicije indeksa j sledi, da sta števili r_{j+1} in r_{j+2} deljivi z d, in zato tudi število r_j. To pa je v protislovju z našo predpostavko. S tem smo dokazali, da d res deli r_i za vsak $i \geq 0$, torej tudi $r_0 = a$ in $r_1 = b$. S tem je izrek dokazan. ■

Trditev 4.13 nam pove, kako poiskati rešitev diofantske enačbe $ax + by = c$ kadar je $c = \gcd(a, b)$. Kaj pa, če je c nek pravi večkratnik števila $\gcd(a, b)$, na primer $c = t \gcd(a, b)$. Tedaj najprej z razširjenim Evklidovim algoritmom poiščemo rešitev (x', y') enačbe $ax' + by' = \gcd(a, b)$. Če to enakost pomnožimo s številom t, vidimo, da je $x_0 = tx'$, $y_0 = ty'$ res rešitev prvotne diofantske enačbe.

Zgled. *Poišči vse rešitve diofantske enačbe*

$$4333x + 623y = 21. \qquad (*)$$

Izvedimo razširjeni Evklidov algoritem z vhodnim podatkom $(a, b) = (4333, 623)$.

i	r_i	x_i	y_i	k_i
0	4333	1	0	
1	623	0	1	
2	595	1	−6	6
3	28	−1	7	1
4	7	22	−153	21
5	0	−89	619	4

Algoritem torej vrne trojico $(7, 22, -153)$. Trditev 4.13 tedaj pravi, da je $\gcd(4333, 623) = 7$ in

$$4333 \cdot 22 + 623 \cdot (-153) = 7.$$

Enakost pomnožimo s 3 in dobimo:

$$4333 \cdot 66 + 623 \cdot (-459) = 21.$$

Od tod razberemo, da je $x_0 = 66$ in $y_0 = -459$ rešitev enačbe $(*)$. Iz Izreka 4.12 sledi, da je poljubna rešitev enačbe $(*)$ enaka $x_k = 66 - \frac{623}{7}k = 66 + 89k$, $y_k = -459 + \frac{4333}{7}k = -459 + 619k$, za kak $k \in \mathbb{Z}$. ■

4.5 Modularna aritmetika

DEFINICIJA 4.14 Naj bo m poljubno naravno število. Pravimo, da sta celi števili x in y *kongruentni po modulu* m, če in samo če m deli $y - x$. Pri tem pišemo

$$x \equiv y \pmod{m} \text{ ali tudi } x \equiv_m y.$$

Relacija kongruence je v tesni zvezi z operacijo celoštevilskega ostanka mod . Velja namreč naslednje:

TRDITEV 4.15 *Za poljubna števila* $x, y \in \mathbb{Z}$ *in* $m \in \mathbb{N}$ *velja*

$$x \equiv y \pmod{m} \;\Leftrightarrow\; x \bmod m = y \bmod m.$$

DOKAZ: Zapišimo $x = km + r$ in $y = \ell m + s$, kjer je $r = x \bmod m$ in $s = y \bmod m$. Če je $r = s$, tedaj očitno m deli število $y - x = m(\ell - k)$.

Denimo sedaj, da je $x \equiv y \pmod{m}$. Dokazati moramo, da od tod sledi $r = s$. Ker m deli število $y - x = (\ell - k)m + s - r$, je $(\ell - k) + s - r = tm$ za neki $t \in \mathbb{Z}$, in zato $s - r = m(t + k - \ell)$. Vendar števili s in r obe ležita na intervalu med 0 in $m - 1$, zato tudi njuna razlika po absolutni vrednosti ne presega števila $m - 1$. Iz zgornje enakosti tedaj sledi, da je $t + k - \ell = 0$, in zato $s = r$, kot je bilo potrebno dokazati. ∎

Kot kaže naslednji izrek, je relacija kongruence lepo uglašena z operacijama seštevanja in množenja.

IZREK 4.16 *Naj velja* $x_1 \equiv y_1 \pmod{m}$ *in* $x_2 \equiv y_2 \pmod{m}$. *Tedaj velja tudi*

$$x_1 + x_2 \equiv y_1 + y_2 \pmod{m} \;\text{ in }\; x_1 x_2 \equiv y_1 y_2 \pmod{m}.$$

DOKAZ: Pišimo $y_1 - x_1 = k_1 m$ in $y_2 - x_2 = k_2 m$. Tedaj je $(y_1 + y_2) - (x_1 + x_2) = (k_1 + k_2)m$, in zato $x_1 + x_2 \equiv y_1 + y_2 \pmod{m}$.

Pri dokazu druge kongruence moramo biti nekoli zviti. Računajmo:

$$y_1 y_2 - x_1 x_2 = y_1(y_2 - x_2) + (y_1 - x_1)x_2 = (y_1 k_2 + k_1 x_2)m.$$

Torej m deli in razliko $y_1 y_2 - x_1 x_2$, in zato $x_1 x_2 \equiv y_1 y_2 \pmod{m}$. ∎

Od tod lahko z uporabo indukcije izpeljemo naslednji sklep.

TRDITEV 4.17 *Če je* $x \equiv y \pmod{m}$ *in* $r \in \mathbb{N}$, *tedaj je tudi* $x^r \equiv y^r \pmod{m}$.

Naslednji izrek pa nam pove, na kakšen način lahko iz kongruence krajšamo multiplikativne faktorje.

IZREK 4.18 *Naj bodo a, x, y poljubna cela števili in m poljubno naravno število. Tedaj velja sklep*

$$ax \equiv ay \pmod{m} \;\Rightarrow\; x \equiv y \pmod{\frac{m}{\gcd(a,m)}}.$$

DOKAZ: Naj bo velja $ax \equiv ay \pmod{m}$. Tedaj obstaja $k \in \mathbb{Z}$, tako da je $ay - ax = km$. Na levi izpostavimo a in enakost lahko delimo z $\gcd(a, m)$. Dobimo

$$\frac{a}{\gcd(a,m)}(y-x) = k\frac{m}{\gcd(a,m)}.$$

Iz trditve 4.9 sledi, da sta števili $\frac{a}{\gcd(a,m)}$ in $\frac{m}{\gcd(a,m)}$ tuji. Trditev 4.10 pa tedaj pravi, da $\frac{m}{\gcd(a,m)}$ deli $y - x$, kot smo želeli pokazati. ∎

Zgornjo trditev največkrat uporabimo v dveh skrajnih primerih: ko je a tuj m in ko a deli m. Sklepa, ki ju dobimo v teh dveh primerih, zapišimo posebej:

POSLEDICA 4.19 *Naj velja $ax \equiv ay \pmod{m}$.*

(i) *Če je $\gcd(a, m) = 1$, tedaj je $x \equiv y \pmod{m}$.*

(ii) *Če a deli m, tedaj $x \equiv y \pmod{\frac{m}{a}}$.*

4.6 Kolobar ostankov

Skozi ves razdelek naj m predstavlja poljubno fiksno naravno število, večje ali enako 2. Množico vseh možnih ostankov pri deljenju s številom m označimo takole:

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}.$$

Na množici ostankov $\mathbb{Z}_m$ definirajmo operaciji, ki ju bomo imenovali *seštevanje in množenje po modulu m* in označevali z $\oplus$ in $\odot$. Za $a, b \in \mathbb{Z}_m$ naj bo

$$a \oplus b = (a+b) \bmod m \;\text{ in }\; a \odot b = (ab) \bmod m.$$

Ti dve operaciji se v mnogočem obnašata podobno kot navadno seštevanje in množenje, zato bomo, kadar ne bo nevarnosti za pomoto, krožec okoli znakov $+$ in $\cdot$ izpuščali. Ni se težko prepričati, da $\mathbb{Z}_n$ skupaj s tema dvema operacijama tvori kolobar.

V kolobarju $\mathbb{Z}_n$ pa se lahko nekateri elementi obnašajo nekoliko nenavadno. Oglejmo si na primer elementa 6 in 4 v $\mathbb{Z}_8$. Njun običajni produkt je enak 24, kar je deljivo z 8. Zato v $\mathbb{Z}_8$ velja enakost $6 \odot 4 = 0$. V kolobarju ostankov je torej produkt dveh neničelni Števil lahko enak 0. Takšna števila si zaslužijo ime: imenujemo jih *delitelji niča*. Ni težko razmisliti, da je neničelni element x kolobarja $\mathbb{Z}_n$ delitelj niča, če in samo če x ni tuj n.

4.7 Obrnljivi elementi v $\mathbb{Z}_n$

Naj bo n poljubno naravno število, večje ali enako 2. Zaradi enostavnejšega zapisa bomo v tem razdelku operaciji $\oplus$ in $\odot$ v kolobarju $\mathbb{Z}_n$ pisali kar kot običajna "plus" in "krat". Kadar bo obstajala nevarnosti za nesporazum, bomo posebej poudarili, ali imamo v mislih običajne operacije v $\mathbb{Z}$ ali pa gre za operacije v $\mathbb{Z}_n$.

DEFINICIJA 4.20 Naj bo x poljuben element kolobarja ostankov $\mathbb{Z}_n$. Če v $\mathbb{Z}_n$ obstaja element $\bar{x}$, za katerega v kolobarju $\mathbb{Z}_n$ velja $x\bar{x} = 1$, rečemo, da je element x obrnljiv v $\mathbb{Z}_n$, element $\bar{x}$ pa imenujemo *inverz* elementa x in ga označimo z x^{-1}.

Za zgled si oglejmo element 2 v $\mathbb{Z}_7$. Ker je $2 \cdot 4 = 8 \equiv 1 \pmod 7$, je 2 obrnljiv element v $\mathbb{Z}_7$ in $2^{-1} = 4$. Če si ogledamo spodnjo tabelico množenja v kolobarju $\mathbb{Z}_7$, se hitro prepričamo, da je v $\mathbb{Z}_7$ obrnljiv prav vsak neničelni element.

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Inverze lahko prečitamo iz spodnje tabele.

x	1	2	3	4	5	6
x^{-1}	1	4	5	2	3	6

Precej drugačna je situacija v kolobarju $\mathbb{Z}_6$. Oglejmo si tabelico množenja.

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Vidimo, da imata sta edina obrnljiva elementa kolobarja $\mathbb{Z}_6$ števili 1 in 5. Pri tem, kot vedno, velja $1^{-1} = 1$. Nekoliko nenavadna pa je enakost $5^{-1} = 5$.

Vprašajmo se torej, ali znamo za dano naravno število n ugotoviti, kateri elementi kolobarja $\mathbb{Z}_n$ so obrnljivi, ne da bi izračunali celotno tabelico množenja. Odgovor se skriva v naslednjem izreku.

Izrek 4.21 *Neničelni element a kolobrja $\mathbb{Z}_n$ je obrnljiv, če in samo če je tuj proti številu n.*

Dokaz: Problem prevedimo na običajne operacije med celimi števili. Element $a \in \mathbb{Z}_n$ je obrnljiv v $\mathbb{Z}_n$, če in samo če obstaja število x, za katerega je $ax \equiv 1 \,(\mathrm{mod}\, n)$, oziroma, če in samo če obstajata celi števili x in y, za kateri je $ax - 1 = ny$. Takšni števili pa obstajata, če in samo če je rešljiva naslednja diofantska enačba

$$ax - ny = 1. \qquad (*)$$

Kot vemo pa ima zgornja enačba rešitev, če in samo če sta števili a in n tuji. S tem je izrek dokazan. ∎

Dokaz pa nam je povedal tudi, kako inverz danega elementa dejansko izračunati. Potrebno je rešiti diofantsko enačbo $(*)$ in po potrebi poiskati tisto rešitev, za katero je x na intervalu med 0 in $n - 1$. (Premisli, da lahko takšno rešitev vedno najdemo.)

Zgled. *Izračunaj* 31^{-1} *v* $\mathbb{Z}_{365}$

Rešiti moramo diofantsko enačbo $31x + 365y = 1$. To lahko storimo z razširjenim Evklidovim algoritmom. ∎

Koliko obrnljivih elementov pa premore kolobar $\mathbb{Z}_n$? Kot pravi izrek 4.21, natanko toliko, kot je naravnih števil med 1 in $n - 1$, ki so tuja številu n. Število takšnih števil je tako pomembno, da nosi svoje ime.

4.8 Eulerjeva funkcija

DEFINICIJA 4.22 Naj bo n poljubno naravno število, večje ali enako 2. Število tujih naravnih števil med 1 in $n-1$ označimo z $\varphi(n)$. Dodatno definiramo še $\varphi(1) = 1$. Tako definirani funkciji $\varphi\colon \mathbb{N} \to \mathbb{N}$ rečemo *Eulerjeva funkcija.*

TRDITEV 4.23 *Če je p praštevilo in r poljubno naravno število, je*

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1) = p^r(1 - \frac{1}{p}).$$

Če sta a in b tuji naravni števili, je

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Zgornja trditev nam omogoča, da izračunamo Eulerjevo funkcijo $\varphi(n)$ za vsako naravno število n, če ga le znamo razcepiti na prafaktorje. Namreč, če je

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

razcep števila n na prafaktorje, tedaj je

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1}(1 - \frac{1}{p_1})p_2^{\alpha_2}(1 - \frac{1}{p_2}) \cdots p_k^{\alpha_k}(1 - \frac{1}{p_k}) =$$

$$= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

4.9 Mali Fermatov izrek in Eulerjev izrek

IZREK 4.24 (**Fermat**) *Naj bo p praštevilo in a naravno število, tuje p. Tedaj je $a^{p-1} \equiv 1 \bmod p$.*

Opomba. Zgornji izrek lahko povemo tudi v jeziku kolobarjev ostankov. Izrek namreč pravi, da za vsako praštevilo p in element $a \in \mathbb{Z}_p \setminus \{0\}$ velja $a^{p-1} = 1$.

DOKAZ: Oglejmo si elemente $a, 2a, 3a, \ldots, (p-1)a$ of $\mathbb{Z}_p$. Če sta dva izmed njih enaka, denimo $ia = ja$, potem z množenjem z a^{-1} v $\mathbb{Z}_p$ dobimo $i = j$ (spomni se, da je element a v $\mathbb{Z}_p$ obrnljiv, da je tuj proti p. S tem smo dokazali, da so zgoraj našteti elementi paroma različni, in ker jih je ravno $p-1$, tvorijo množico vseh neničelnih elementov v $\mathbb{Z}_p$:

$$\{a, 2a, 3a, \ldots, (p-1)a\} = \{1, 2, 3, \ldots, p-1\}.$$

Če zmnožimo vse elemente množic na levi in desni strani enakosti, dobimo naslednjo enakost v $\mathbb{Z}_p$:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) = a \cdot 2a \cdot 3a \cdots (p-1)a = (p-1)!a^{p-1}.$$

Vendar $(p-1)!$ je tuj proti p, zato ga smemo iz leve in desne strani enakosti v $\mathbb{Z}_p$ pokrajšati. Od to dobimo enakost $a^{p-1} = 1$ v $\mathbb{Z}_p$. ∎

Zgornji izrek pa lahko nekoliko posplošimo. Najprej opazimo, da je $\varphi(p) = p-1$ za vsako praštevilo p. Zato lahko izraz a^{p-1} interpretiramo tudi kot $a^{\varphi(p)}$. Ob tej interpretaciji se izkaže, da lahko pogoj, da je p praštevilo, izpustimo. Velja namreč naslednji izrek.

Izrek 4.25 (**Euler**) *Naj bo n poljubno naravno število in a število, ki je tuje n. Tedaj je $a^{\varphi(n)} \equiv 1 \bmod n$.*

Dokaz Eulerjevega izreka je na las podoben dokazu malega Fermatovega izreka, le da namesto s števili $a, 2a, \ldots, (p-1)a$ pričnemo z elementi za, kjer z preteče vse obrnljive elemente iz $\mathbb{Z}_n^*$. Podrobnosti dokaza lahko izdela bralec sam.

Zgled. *S pomočjo Eulerjevega izreka izračunaj* $1840^{1995} \bmod 26$

Najprej izračunamo $1840 \bmod 26 = 20$. Zato $1840^{1995} \equiv 20^{1995} \bmod 26$. Ker 20 ni tuje 26, Eulerjevega izreka ne moremo uporabiti takoj. Zato 20^{1995} pišemo kot $4^{1995} \cdot 5^{1995}$. Za razcep $20 = 4 \cdot 5$ smo se odložili zato, ker je 5 med delitelji števila 20 največji, ki je tuj 26.

Ker je $\gcd(5, 26) = 1$, lahko število $5^{1995} \bmod 26$ izračunamo neposredno s pomočjo Eulerjevega izreka. Ker je $\varphi(26) = 12$, najprej zapišemo $1995 = 12 \cdot 166 + 3$ in od tod dobimo

$$5^{1995} \equiv (5^{12})^{166} \cdot 5^3 \equiv 5^3 \equiv 21 \,(\bmod 26).$$

Pri računanju ostanka $4^{1995} \bmod 26$ moramo biti nekoliko iznajdljivejši. Najprej zapišemo $4^{1995} = 2^{3990}$ in označimo $x = 2^{3990} \bmod 26$. Tedaj je $x = 2^{3990} - 26q$, kjer $q = 2^{3990} \operatorname{div} 26$, in zato $x = 2y$ za neko naravno število y. Od tod dobimo $2y \equiv 2^{3990} \,(\bmod 26)$, od koder sledi $y \equiv 2^{3989} \,(\bmod 13)$, in zato $y = 2^{3989} \bmod 13$. Slednji ostanek pa lahko izračunamo s pomočjo Eulerjevega izreka (oziroma celo s pomočjo Femratovega malega izreka). Ker je $\varphi(13) = 12$ in $3989 = 332 \cdot 12 + 5$, je

$$2^{3989} \equiv 2^5 \equiv 6 \bmod 13,$$

in torej $y = 6$ in $x = 12$. S tem smo dokazali kongruenco

$$4^{1995} \equiv 12 \,(\mathrm{mod}\, 26).$$

Račun zaključimo takole:

$$1840^{1995} \equiv 20^{1995} \equiv 4^{1995} \cdot 5^{1995} \equiv 12 \cdot 5^3 \equiv 60 \cdot 25 \equiv 8 \cdot (-1) \equiv 18 \,(\mathrm{mod}\, 26).$$

■

4.10 Kriptografski sistem RSA

Za zgled uporabe modularne aritmetike si oglejmo kriptografsko metodo, imenovano RSA, ki omogoča pošiljanje tajnih sporočil med več udeleženci, pri čemer vsebino tajnega sporočila lahko razbere le tisti, ki mu je bilo sporočilo poslano.

Sistem RSA sodi med kriptografke sisteme z javnim ključem. Posebnost teh sistemov je, da vsak udeleženec komunikacije, ki želi prejemati tajna sporočila od ostalih udeležencev, javno objavi svoj *javni ključ* (geslo), ki ga ostali uporabijo za šifriranje njemu namenjenih sporočil, v tajnosti pa ohrani svoj *privatni ključ*, ki je potreben za dešifriranje sporočil, ki so bila zašifrirana z njegovim javnim ključem. Varnost metode sledi na dejstvu, da je iz posameznikovega javnega ključa zelo težko (praktično neizvedljivo) izračunati njegov privatni ključ.

Opišimo na kratko, kaj mora storiti oseba A, ki bi od osebe B želela prejeti tajno sporočilo.

- Najprej naključno izbere dve praštevili, p in q, ter izračuna

  $$n = pq, \quad \varphi = \varphi(n) = (p-1)(q-1).$$

  Za varnost sistema je zelo pomembno, da sta praštevili p in q tako veliki, da števila n nihče, razen osebe A, ne zna razcepiti na produkt praštevil. Danes se v praksi uporabljajo vsaj 100 mestna praštevila, kjer pa je potrebna večja varnost, pa še večja praštevila.

- Izbere poljubno število $e \in \mathbb{Z}_\varphi^*$ (število med 1 in $\varphi - 1$, ki je tuje φ) in s pomočjo razširjenega Evklidovega algoritma izračuna inverz

  $$d = e^{-1} \in \mathbb{Z}_\varphi^*.$$

V praksi število e izbremo tako, da naključno izberemo število med 1 in $\varphi - 1$, nato pa z razširjenim Evklidovim algoritmom testiramo, ali je število e res tuje številu φ; če ni, postopek izbire števila e ponovimo. Kot bomo videli kasneje, nekatere vrednosti števila e niso najbojše (na primer, $e = 1$), zato zavrnemo tudi morebitne takšne naključne izbire.

- Javno objavi števili n in e (javni ključ), sam pa varno shrani število d (privatni ključ). Ostale podatke "pozabi".

Zdaj pa si oglejmo, kaj mora storiti oseba B, ki želi osebi A poslati tajno sporočilo.

- Svoje tekstovno sporočilo najprej pretvori v število $m \in \mathbb{Z}_n$. To stori na javno znan način in tako, da bo vsak, ki bo poznal število m, brez težav rekonstruiral začetno tekstovno sporočilo. Če je tekstovno sporočilo predolgo, ga najprej razbije na manjše dele, jih pretvori v zaporedje števil v $\mathbb{Z}_n$, in izvede spodaj opisani postopek za vsak člen tega zaporedja.
- Prebere javni ključ (n, e) osebe A, izračuna število

$$c = m^e \bmod n$$

in ga pošlje osebi A.

Ko oseba A prejme število c, uporabi svoj privatni ključ d in izračuna število

$$m' = c^d \bmod n.$$

Izkaže se, da je število m' kar enako originalnemu številu m. Nazadnje oseba A iz števila $m' = m$ rekonstruira tekstovno sporočilo osebe B.

Vidimo, da celotna metoda temelji na naslednji trditvi.

TRDITEV 4.26 *Naj bosta p in q različni praštevili in naj bo $n = pq$ ter $\varphi = (p-1)(q-1)$. Nadalje, naj bo e poljuben obrnljiv element kolobarja $\mathbb{Z}_\varphi$ in $d = e^{-1} \in \mathbb{Z}_\varphi^*$ njegov inverz. Tedaj za vsako celo število m, $1 \leq m \leq n-1$, iz enakosti $c = m^e \bmod n$ sledi enakost $c^d \bmod n = m$.*

DOKAZ: Ker je d inverz elementa e v $\mathbb{Z}_\varphi$, obstaja celo število x, za katerega je $ed - x\varphi = 1$. Tedaj

$$c^d \equiv m^{ed} = m^{1+x\varphi} = m \cdot (m^\varphi)^x \bmod n.$$

Če je $\gcd(m, n) = 1$, potem iz Eulerjevega izreka sledi $m^{\varphi} \equiv 1 \bmod n$, in zato $c^d \equiv m \bmod n$.

Predpostavimo torej lahko, da m ni tuj n. To se zgodi le, če bodisi p bodisi q deli število m. Brez izgube splošnoti lahko predpostavimo, da je m večkratnik števila p. Tedaj je tudi število $c^d = m^{ed}$ deljivo s p, in zato

$$c^d \equiv m \equiv 0 \bmod p.$$

Ker m ni hkrati deljiv tudi s q (saj bi sicer ne bil manjši od n), smemo uporabiti Fermatov izrek in ugotoviti, da je $m^{q-1} \equiv 1 \bmod q$. Zato velja

$$c^d = m^{ed} = m^{1+x\varphi} = m \cdot \left(m^{(q-1)}\right)^{(p-1)x} \equiv m \bmod q.$$

Od tod sledi, da imata števili $c^d \bmod n$ in m enaka ostanka pri deljenju s p kot tudi pri deljenju s q. Ni težko videti, da imata tedaj enaka ostanka tudi pri deljenju z $n = pq$. Ker sta obe števili manjši ali enaki n, sta zato enaki. ∎

5 Relacije

V matematiki (in tudi zunaj nje) imamo velikokrat opravka s pojmom *relacija*. Na primer, v množici števil lahko vpeljemo relacijo $\leq$, ali pa relacijo $\neq$, ali denimo $\equiv (\bmod 3)$, itd. V geometriji lahko vpeljemo relacije *vzporednosti*, *skladnosti* in podobno. Tudi v vsakdanjem življenju si lahko mislimo relacije kot so: "x je oče y", "x ima rad y", "x je starejši od y", itd. Kako ta intuitiven pojem vpeljati na korekten način?

Denimo, da imamo neko relacijo R med objekti množice A. Ta relacija določa množico

$$\{(x, y) \mid x \text{ je v relaciji } R \text{ z } y\} \subseteq A \times A.$$

Očitno je zgornja množica z relacijo R natanko določena. Velja pa tudi obratno. Vsaka podmnožica $R \subseteq A \times A$ določa neko relacijo, namreč tisto, za katero velja:

$$x \text{ je v relaciji z } y \text{ natanko tedaj, ko je } (x, y) \in R.$$

V tem smislu lahko pojem relacije in podmnožice množice $A \times A$ kar enačimo. V resnici na ta način dobimo tako imenovane dvomestne relacije. Seveda pa poznamo relacije, ki povezujejo več kot dva objekta, na primer, v geometriji lahko vpeljemo "premica x je v relaciji s premicama y in z, če seka y in z pod istim kotom", ali pa v teoriji števil, "x, y in z so v relaciji, če je $x+y = z$", itd. Takšne *trimestne relacije* lahko predstavimo s podmnožicami karteţicnega produkta $A \times A \times A$.

DEFINICIJA 5.1 Naj bo n naravno število. Podmnožici R množice $A^n = A \times A \times \ldots \times A$ pravimo n-mestna relacija na množici A. Če je $(x_1, x_2, \ldots, x_n) \in R$. rečemo, da so elementi $x_1, x_2, \ldots, x_n$ v relaciji R. Če je $n = 2$, dejstvo $(x_1, x_2) \in R$ zapišemo tudi kot $x_1 R x_2$.

Od sedaj dalje se bomo ukvarjali le z dvomestnimi relacijami. Če je množica A, na kateri je relacija definirana, končna (in ne prevelika), si lahko dvomestno relacijo predstavimo tudi s pomočjo *grafa relacije*, ki ga dobimo takole:

Vsak element množice A predstavimo kot točko v ravnini, za vsak par elementov $a, b \in A$, za katera velja aRb, pa narišemo usmerjeno daljico od a do b. Če je $a = b$ (in torej aRa), potem namesto usmerjene daljice narišemo zanko skozi a (ukrivljeno črto, ki se prične in konča v a).

ZGLED. *Nariši graf relacije R na množici $\{2,3,4,5,6,7,8,9\}$ definirani s predpisom $xRy \equiv x$ deli y.*

Narišemo osem točk v ravnini (denimo enakomerno razporejenih na obodu kroga), jih označimo s števili $2, 3, \ldots, 9$, narišemo usmerjene daljice $\overrightarrow{24}$, $\overrightarrow{26}$, $\overrightarrow{28}$, $\overrightarrow{36}$, $\overrightarrow{39}$, $\overrightarrow{48}$ in dodamo še zanko na vsako od osmih točk. ∎

Naj bo R dvomestna relacija na množici A. Tedaj množici

$$\mathcal{D}_R = \{x \mid \exists y(xRy)\}$$

rečemo *domena realcije* R, množici

$$\mathcal{Z}_R = \{y \mid \exists x(xRy)\}$$

pa *zaloga vrednosti realcije* R. Očitno velja $R \subseteq \mathcal{D}_R \times \mathcal{Z}_R$. Unija $\mathcal{D}_R \cup \mathcal{Z}_R$ se imenuje *polje relacije* R. Na grafu domeno relacije prepoznamo kot množico točk, iz katerih kaže vsaj ena usmerjena daljica (ali zanka), zalogo vrednosti pa kot mnozčio točk, v katero kaže vsaj ena usmerjena daljica (ali zanka).

5.1 Operacije na relacijah

Iz danih relacij R in T na množici A lahko tvorimo nove relacije na množici A. Oglejmo si nekaj načinov:

Komplementarna relacija: Elementa $x, y \in A$ sta v *komplementarni relaciji* $\bar{R}$ natanko tedaj, ko nista v relaciji R:

$$x \,\bar{R}\, y \Leftrightarrow \neg(x \,R\, y).$$

Graf komplementarne relacije narišemo tako, da narišemo usmerjene daljice povsod, kjer jih prej ni bilo, stare pa zbrišemo.

ZGLEDI: Če je R relacija "biti večji ali enak" na množici naravnih števil, je komplementarna relacija $\bar{R}$ relacija "ne biti večji ali enak", kar je na množici naravnih števil isto kot "biti strogo manjši". Komplementarna relacija relacije "biti sin od" je "ne biti sin od". Podobno, če je R relacija "biti vzporeden" na množici vseh premic v ravnini, potem sta dve premici v komplementarni relaciji $\bar{R}$, če in samo če nista vzporedni.

Inverzna relacija: Elementa $x, y \in A$ sta v inverzni relaciji R^{-1}, natanko tedaj, ko sta v obratnem vrstnem redu, y, x, v relaciji R:

$$x \,R^{-1}\, y \Leftrightarrow y \,R\, x.$$

Velja: $\mathcal{D}_{R^{-1}} = \mathcal{Z}_R$ in $\mathcal{Z}_{R^{-1}} = \mathcal{D}_R$. Očitno tudi: $(R^{-1})^{-1} = R$. Graf inverzne relacije dobimo tako, da spremenimo usmeritev vsem usmerjenim daljicam.

Zgledi: Inverz relacije $\leq$ na množici $\mathbb{R}$ je relacija $\geq$. Inverz relacije "mož" na množici držaljanov RS je "žena". Inverz relacije "je sosed ali soseda" pa je kar relacija "je sosed ali soseda".

Kompozitum relacij: Elementa x in z sta v sestavljeni relaciji $T \circ R$, če lahko najdemo kak element (recimo y), za katerega velja xRy in yTz. S simboli:

$$x\,(T \circ R)\,z \Leftrightarrow \exists y(x\,R\,y \wedge y\,T\,z).$$

Graf kompozita $T \circ R$ dobimo tako, da na isto sliko narišemo grafa relacij T in R, prvega z modro barvo, drugega z rdečo, nato pa vsak zaporedni par rdeče in modre usmerjene daljice (v tem vrstnem redu) nadomestimo z novo (črno) usmerjeno daljico. Stare (rdeče in modre) daljice seveda zbrišemo.

Zgled. *Kakšne relacije na množici ljudi predstavljajo naslednji kompoziti: "je brat" ∘ "je sin"; "je sin" ∘ "je brat"; "je sin" ∘ "je oče"; "je oče" ∘ "je sin". Pri tem zaradi enostavnosti predpostavimo, da ima vsaka oseba otroke z največ eno drugo osebo, le-ta pa je nasprotnega spola.*

- x ("je brat" ∘ "je sin") $y \Leftrightarrow x$ "je nečak (po očetovi strani)" y;
- x ("je sin" ∘ "je brat") $y \Leftrightarrow x$ "je sin" $y \wedge x$ ima brata;
- x ("je sin" ∘ "je oče") $y \Leftrightarrow (x = y \wedge x$ ima sina) $\vee$(x je moški in ima sina z y);
- x ("je oče" ∘ "je sin") $y \Leftrightarrow x = y \vee x$ je brat ali sestra y.

■

Zgornji zgledi kažejo, da v splošnem ne velja komutativnostni zakon $R \circ T = T \circ R$. Velja pa asociativnostni zakon, $R \circ (T \circ S) = (R \circ T) \circ S$, in običajno pravilo za računanje inverza sestavljene relacije, $(R \circ T)^{-1} = T^{-1} \circ R^{-1}$.

Na vsaki množici A z vsaj dvema elementoma imamo vedno vsaj tri relacije: *univerzalno relacijo* $U = A \times A$, prazno relacijo $\emptyset$ in identiteto $I = \{(x, x) \mid x \in A\}$. Očitno za poljubno relacijo R velja:

- $R \circ I = I \circ R = R$,
- $R \circ \emptyset = \emptyset \circ R = \emptyset$,

- $x\, R \circ U\, y \Leftrightarrow (\exists u)(uRy)$,
- $x\, U \circ R\, y \Leftrightarrow (\exists v)(xRv)$.

5.2 Lastnosti relacij

Naj bo R dvomestna relacija na množici A. Tedaj pravimo:

- R je *refleksivna* $\Leftrightarrow (\forall x \in A)(xRx)$;
- R je *irefleksivna* $\Leftrightarrow (\forall x \in A)(x\bar{R}x)$;
- R je *simetrična* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x\, R\, y \Rightarrow y\, R\, x)$;
- R je *asimetrična* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x\, R\, y \Rightarrow y\, \bar{R}\, x)$;
- R je *antisimetrična* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x\, R\, y \wedge y\, R\, x \Rightarrow x = y)$;
- R je *tranzitivna* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(\forall z \in A)(x\, R\, y \wedge y\, R\, z \Rightarrow x\, Rz)$;
- R je *sovisna* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x \neq y \Rightarrow (x\, R\, y \vee y\, R\, x))$;
- R je *strogo sovisna* $\Leftrightarrow (\forall x \in A)(\forall y \in A)(x\, R\, y \vee y\, R\, x)$.

Zgornje lastnosti relacij se seveda odražajo tudi na grafu relacije. Tako je, na primer, relacija *refleksivna*, če skozi vsako točko poteka zanka, *simetrična*, če graf z vsako usmerjeno daljico vsebuje tudi njej nasprotno usmerjeno daljico (v tem primeru takšen par navadno nadomestimo z eno samo, neusmerjeno daljico), *tranzitivna*, če z vsakim parom zaporednih usmerjenih daljic graf premore tudi usmerjeno daljico od prve do tretje točke v takšnem zaporedju itd.

Za vajo premisli, katere od zgoraj naštetih lastnosti imajo naslednje relacije:

- $<$ na množici $\mathbb{R}$,
- $\leq$ na množici $\mathbb{R}$,
- "kongruenten modulo 5" na $\mathbb{Z}$,
- $\subseteq$ na $\mathcal{P}(\mathbb{N})$.

5.3 Ekvivalenčna relacija in relacije urejenosti

Relacija je *ekvivalenčna*, če je hkrati refleksivna, simetrična in tranzitivna. Najpreprostejši zgled je kar identiteta I. Nadaljni zgledi so kongruenca po modulu m v množici $\mathbb{Z}$, vzporednost v množici premic v ravnini, "biti enako star" na množici ljudi itd.

Lastnost "biti ekvivalenčna relacija" lahko izrazimo tudi v jeziku inverza in kompozita relacij.

Trditev 5.2 *Relacija R je ekvivalenčna relacija na množici A natanko tedaj, ko je $\mathcal{D}_R = A$ in velja $R^{-1} \circ R = R$.*

Graf ekvivalenčne relacije razpade na nekaj med seboj nepovezanih grozdov, pri čemer znotraj posameznega grozda najdemo vse možne usmerjene daljico (vključno z vsemi zankami). Tem grozdom pravimo tudi *ekvivalenčni razredi* relacije. Ekvivalenčne razrede natančneje definiramo takole:

Definicija 5.3 Naj bo R ekvivalenčna relacija na množici A in $a \in A$. Tedaj množici

$$R(a) = \{x \in A \mid aRx\}$$

rečemo ekvivalenčni razred elementa a. Množici

$$A/R = \{R(a) \mid a \in A\}$$

vseh ekvivalenčnih razredov rečemo *faktorska množica* glede na R.

Množici $\mathcal{R} = \{A_1, \ldots, A_n\}$ nepraznih, paroma disjunktnih množic A_i, katerih unija je enaka A, rečemo *razbitje* množice A. Ni se težko prepričati v naslednje:

Trditev 5.4 *Faktorska množica A/R ekvivalenčne relacije $R \subseteq A \times A$ tvori razbitje množice A.*

Velja pa tudi obrat zgornje trditve: Denimo, da je $\mathcal{R}$ razbitje množice A. Definirajmo relacijo R na A takole: $xRy \Leftrightarrow$ "x in y ležita v isti množici razbitja $\mathcal{R}$". Ni težko videti, da je tako definirana relacija R ekvivalenčna, faktorska množica A/R pa kar enaka $\mathcal{R}$.

Relacijam, ki so tranzitivne, rečemo tudi *relacije urejenosti*. Relacije urejenosti razvrstimo v različne skupine (in podskupine), glede na to, katere dodatne lastnosti še imajo:

DEFINICIJA 5.5 Naj bo R tranzitivna relacija na množici A. Če je še:

- refleksivna in antisimetrična, ji rečemo *delna urejenost*;
- antisimetrična in strogo sovisna ji rečemo *linearna urejenost*;
- asimetrična, ji rečemo *stroga delna urejenost*;
- asimetrična in sovisna, ji rečemo *stroga linearna urejenost*.

TRDITEV 5.6 *Vsaka strogo sovisna relacija je refleksivna.*

DOKAZ: Naj bo R strogo sovisna relacija na množici S. Tedaj za poljuben par elementov $x, y \in S$ velja xRy ali yRx. Če za y vzamemo kar x, dobimo: xRx ali xRx, kar je isto kot xRx. ∎

Neposredno iz definicije skupin urejenosti in zgornje trditve tedaj sledi:

- R je linearna urejenost $\Rightarrow$ R je delna urejenost;
- R je stroga linearna urejenost $\Rightarrow$ R je stroga delna urejenost.

6 Kompleksna števila

V prejšnjem razdelku smo videli, da ima znotraj množice relanih števil vsaka linearna enačba, to je enačba oblike $ax + c = b$, kjer je $a \neq 0$, natanko eno rešitev. Videli smo tudi, da imajo nekatere kvadratne enačbe eno ali več rešitev. Žal pa ni res, da bi imela vsaka kvadratna enačba oblike

$$ax^2 + bx + c = 0,\ a \neq 0, \tag{1}$$

kakšno rešitev znotraj množice $\mathbb{R}$. Vemo, da ima enačba (1) realne rešitve le, če je $b^2 - 4ac \geq 0$. V posebnem primeru enačba

$$x^2 = -1 \tag{2}$$

znotraj $\mathbb{R}$ nima rešitve.

Če se želimo tej težavi izogniti, moramo številsko množico razširiti in vpeljati *množico kompleksnih števil* $\mathbb{C}$.

Definicija 6.1 Množica kompleksnih števil je definirana kot množica vseh urejenih parov realnih števil:

$$\mathbb{C} := \mathbb{R} \times \mathbb{R}.$$

Pri tem za kompleksno število $z = (x, y)$ definiramo

$$\mathrm{Re}(z) = x \quad \text{in} \quad \mathrm{Im}(z) = y.$$

Množica $\mathbb{C}$ je torej definirana enako kot dvorazsežni vektorski prostor nad obsegom $\mathbb{R}$. Zato si jo večkrat predstvljamo kot običajno ravnino in ji rečemo tudi *kompleksna ravnina*. Operacija seštevanja je v množici $\mathbb{C}$ definirana enako kot v vektorskih prostorih:

Definicija 6.2 Za poljubni kompleksni števili $z_1 = (x_1, y_1)$ in $z_2 = (x_2, y_2)$ definiramo: $z_1 + z_2 = (x_1 + x_2, y_1 + y_2)$.

Kot vemo, v splošnih vektorskih prostorov množenja dveh vektorjev ne moremo vpeljati tako, da bi veljala običajna računska pravila: komutativnost, asociativnost, in distributivnost proti vsoti. Dvorazsežni primer pa je izjema. V množici $\mathbb{C}$ lahko vpeljemo množenje na takšen način, da bodo zanj veljala vsa običjna pravila, ki jih poznamo že iz množice realnih števil. To storimo takole:

DEFINICIJA 6.3 Za poljubni kompleksni števili $z_1 = (x_1, y_1)$ in $z_2 = (x_2, y_2)$ definiramo: $z_1 z_2 = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$.

Za zgled preverimo, da za tako definiranem množenje velja asociativnostni zakon. Naj bodo $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$ in $z_3 = (x_3, y_3)$ poljubna kompleksna števila. Tedaj je

$$(z_1 z_2) z_3 = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)(x_3, y_3) =$$

$$((x_1 x_2 - y_1 y_2) x_3 - (x_1 y_2 + x_2 y_1) y_3,\ (x_1 x_2 - y_1 y_2) y_3 + (x_1 y_2 + x_2 y_1) x_3) =$$

$$(x_1 x_2 x_3 - x_3 y_1 y_2 - x_1 y_2 y_3 - x_2 y_1 y_3,\ x_1 x_2 y_3 - y_1 y_2 y_3 + x_1 x_3 y_2 + x_2 x_3 y_1)$$

Po drugi strani pa je

$$z_1 (z_2 z_3) = (x_1, y_1)(x_2 x_3 - y_2 y_3, x_2 y_3 + x_3 y_2) =$$

$$x_1 (x_2 x_3 - y_2 y_3) - y_1 (x_2 y_3 + x_3 y_2),\ x_1 (x_2 y_3 + x_3 y_2) + y_1 (x_2 x_3 - y_2 y_3) =$$

$$(x_1 x_2 x_3 - x_1 y_2 y_3 - x_2 y_1 y_3 - x_3 y_1 y_2,\ x_1 x_2 y_3 + x_1 x_3 y_2 + x_2 x_3 y_1 - y_1 y_2 y_3).$$

Obakrat smo dobili enak rezultat, zato je množenje kompleksnih števil res asociativno.

Strogo gledano realna števila niso podmnožica kompleksnih števil. Kljub temu pa lahko množico $\mathbb{R}$ na smiseln način vložimo v množico $\mathbb{C}$. Vsakemu realnemu številu $a \in \mathbb{R}$ priredimo v množici $\mathbb{C}$ predstavnika $(a, 0) \in \mathbb{C}$. Hitro se vidi, da je predstavnik produkta dveh realnih števil $(ab, 0)$ enak produktu ustreznih predstavnikov $(a, 0)(b, 0)$. Podobno velja tudi za vsoto. To nam pove, da je množica $\mathbb{R}$ vložena v množico $\mathbb{C}$ skladno z operacijami množenja in seštevanja.

Označimo posebej še kompleksno število

$$i := (0, 1),$$

za katerega očitno velja

$$i^2 = (-1, 0) = -1 \in \mathbb{R}$$

Pri zgoraj vpeljanih oznakah se poljubno kompleksno število $(x, y) \in \mathbb{C}$ enolično zapiše kot vsota

$$x + iy,\ x, y \in \mathbb{R}.$$

6.1 Absolutna vrednost kompleksnega števila

DEFINICIJA 6.4 Absolutna vrednost kompleksnega števila $z = x + iy$, $x, y \in \mathbb{R}$, je definirana s formulo:

$$|z| = \sqrt{x^2 + y^2}.$$

Če si kompleksno število predstavljamo kot točko v kompleksni ravnini, je njegova absolutna vrednost ravno oddaljenost števila od izhodišča kompleksne ravnine. Če pa si kompleksno število predstavljamo kot vektor v ravnini, je njegova absolutna vrednost kar njegova dolžina.

Podobno, absolutna vredsnot razlike

$$|z - w|$$

je ravno razdalja med točkama z in w v kompleksni ravnini. Iz geometrijske interpretacije absolutne vrednosti sledi *trikotniška neenakost za kompleksna števila*:

TRDITEV 6.5 *Za poljubni kompleksni števili z in w velja neenakost*

$$|z + w| \leq |z| + |w|.$$

DOKAZ: V zgornjo trditev se najlažje prepričamo, če si ogledamo trikotnik, ki ga v kompleksni ravnini tvorijo točke 0, z in $z+w$. Stranice trikotnika nosijo vektorji z, w in $z + w$. Če verjamemo, da je dolžina vsake stranice manjša od (ali največ enaka, če je trikotnik izrojen) vsoti dolžin drugih dveh stranic, dobimo iskano neenakost.

Seveda takšen razmislek ni strog dokaz trditve. Pravi dokaz trditve lahko naslonimo zgolj na definicijo absolutne vrednosti kompleksnega števila. ■

TRDITEV 6.6 *Za poljubni kompleksni števili z in w velja:*

$$|zw| = |z|\,|w|.$$

6.2 Konjugirana vrednost

Kompleksnemu številu $z = x + iy$, $x, y \in \mathbb{R}$, priredimo število

$$\bar{z} := x - iy,$$

ki mu pravimo *konjugirana vrednost kompleksnega števila* z.

TRDITEV 6.7 *Za poljubni števili* $z, w \in \mathbb{C}$ *velja:*

i) $\bar{\bar{z}} = z$,

ii) $\overline{z + w} = \bar{z} + \bar{w}$ *in* $\overline{zw} = \bar{z}\bar{w}$,

iii) $\mathrm{Re}(z) = \frac{1}{2}(z + \bar{z})$ *in* $Im(z) = \frac{1}{2i}(z - \bar{z})$,

iv) $|z| = \sqrt{z\bar{z}}$.

POSLEDICA 6.8 *Bodi* $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ *polinomska enačba z realnimi koeficienti. Če je kompleksno število* z *njena rešitev, potem je njena rešitev tudi število* $\bar{z}$.

DOKAZ: Iz točke ii) trditve 6.7 sledi, da pri poljubnem polinomu $p(x)$ in pri poljubnem kompleksnem številu z velja $p(\bar{z}) = \overline{p(z)}$. Če je torej $p(z) = 0$, je tudi $p(\bar{z}) = \overline{p(z)} = \bar{0} = 0$. ∎

6.3 Polarni zapis kompleksnega števila

Tako kot lahko vsaki točki v ravnini poiščemo bodisi njeni *pravokotni koordinati* bodisi njeni *polarni koordinati*, lahko tudi kompleksnemu številu v kompleksni ravnini poleg *pravokotnega zapisa* $x + iy$, $x, y \in \mathbb{R}$, najdemo tudi *polarni zapis*.

Bodi $z = x + iy$, $x, y \in \mathbb{R}$, poljubno kompleksno število. Tedaj je

$$z = |z|(\cos\phi + i\sin\phi), \qquad (*)$$

kjer je ϕ kot med realno osjo kompleksne ravnine in poltrakom iz izhodišča ravnine skozi točko z. Takšnemu kotu ϕ rečemu tudi *argument kompleksnega števila* z in ga označimo z

$$\arg z.$$

Po definicji leži število $\arg z$ vedno na intervalu $[0, 2\pi)$.

Ker sta cos in sin periodični funkciji s periodo 2π, je lahko namesto kota $\phi = \arg z \in [0, 2\pi)$ v formulo $(*)$ vstavimo tudi katerikoli kot oblike $\phi + 2k\pi$, kjer je k poljubno celo število. Na ta način dobimo poleg osnovnega polarnega zapisa še neskončno mnogo dugih (enakovrednih) polarnih zapisov.

Polarni zapis nam omogoča preprostejše množenje, potenciranje in korenjenje kompleksnih števil.

Bodita z in w poljubni kompleksni števili, ki ju zapišemo v polarni obliki:

$$z = |z|(\cos\phi + i\sin\phi) \text{ in } w = |w|(\cos\psi + i\sin\psi).$$

Tedaj je

$$zw = |z||w|(\cos\phi\cos\psi - \sin\phi\sin\psi + i(\cos\phi\sin\psi + \cos\psi\sin\phi)) =$$

$$|zw|(\cos(\phi+\psi) + i\sin(\phi+\psi)).$$

Iz tega je razvidno, da se kompleksna števila množijo tako, da se absolutne vrednosti zmnožijo, argumenti pa seštejejo.

Iz zgornjega med drugim sledi, da se kompleksna števila potencirajo tako, da se potencirajo njihove absolutne vrednosti, argumenti pa množijo z eksponentom:

$$z^n = |z|^n(\cos n\phi + i\sin n\phi). \qquad (+)$$

Zgornja formula nam omogoča za dano kompleksno število w in dano narabno število n poiskati vsa števila $z \in \mathbb{C}$, ki zadoščajo enakosti $z^n = w$.

Zgled. *Poišči vsa kompleksna števila z, ki zadoščajo enakosti $z^8 = 1$.*

Kompleksno število 1 lahko v polarni obliki zapišemo natanko na naslednje načine:

$$1 = \cos 2k\pi + i\sin 2k\pi,\ k \in \mathbb{Z}.$$

Iskano število z naj ima polarni zapis enak

$$z = |z|(\cos\phi + i\sin\phi).$$

Iz formule $(+)$ sledi, da je

$$|z|^8 = 1 \text{ in } 8\phi = 2k\pi, \text{ kjer je } k \text{ poljubno celo število.}$$

Sledi, da je $|z| = 1$ in $\phi = k\frac{\pi}{4}$, $k \in \mathbb{Z}$. Če to razpišemo, dobimo osem različnih rešitev:

$$
\begin{aligned}
z_0 &= \cos 0 + i \sin 0 = 1, \\
z_1 &= \cos \frac{\pi}{4} + i \sin \frac{\pi}{4} = \frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}, \\
z_2 &= \cos \frac{\pi}{2} + i \sin \frac{\pi}{2} = i, \\
z_3 &= \cos 3\frac{\pi}{4} + i \sin 3\frac{\pi}{4} = -\frac{\sqrt{2}}{2} + i \frac{\sqrt{2}}{2}, \\
z_4 &= \cos \pi + i \sin \pi = -1, \\
z_5 &= \cos 5\frac{\pi}{4} + i \sin 5\frac{\pi}{4} = -\frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2}, \\
z_6 &= \cos 3\frac{\pi}{2} + i \sin 2\frac{\pi}{2} = -i \text{ in} \\
z_7 &= \cos 7\frac{\pi}{4} + i \sin 7\frac{\pi}{4} = \frac{\sqrt{2}}{2} - i \frac{\sqrt{2}}{2}.
\end{aligned}
$$

■