UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO
LABORATORIJ ZA MATEMATIČNE METODE
V RAČUNALNIŠTVU IN INFORMATIKI

Aljaž Zalar

REŠENE NALOGE IZ DISKRETNIH STRUKTUR

Študijsko gradivo

Ljubljana, 2022

Uvod

Naloge na naslednjih straneh so se pojavljale na teoretičnih izpitih pri predmetu Diskretne strukture za študente visokošolskega študija računalništva in informatike na FRI v študijskih letih 2019/20–2021/22.

Naloge so urejene po poglavjih, ki se obravnavajo pri predmetu, tako da jih lahko poskušate rešiti že sproti, ko obdelate posamezno poglavje.

To študijsko gradivo ni recenzirano in gotovo se v rešitvah pojavi kakšna napaka. Če opazite kakšno napako, jo prosim sporočite na elektronski naslov aljaz.zalar@fri.uni-lj.si.

Za lažjo navigacijo po dokumentu so na voljo bližnjice. Če kliknete na simbol ⇩ ob nalogi, boste skočili do rešitve. Če kliknete na simbol ⇧ ob rešitvi, se boste vrnili k besedilu naloge. Za TeX predlogo dokumenta se zahvaljujem dr. Aleksandri Franc.

Naloge računsko niso zahtevne, pomembno je predvsem razumevanje ideje v ozadju. Zato priporočam, da o nalogi nekaj časa razmišljate, pobrskate po zapiskih oz. literaturi, v kolikor ideje ne dobite, potem pa tudi v celoti napišete rešitev. Šele nato svojo rešitev primerjate z rešitvami v zbirki. Poleg razumevanja bistva nalog je namreč cilj predmeta tudi to, da se naučite svoje ideje pravilno matematično zapisati, pri čemer se osredotočite predvsem na bistven sklep in ne navajate več možnih sklepov, ki bi lahko vodili k pravi rešitvi.

Kazalo

Del 1

Naloge

POGLAVJE 1

Izjavni račun

NALOGA 1.
Naj bodo p, q, r izjavne spremenljivke. V vsakega od spodnjih okvirčkov $\boxed{}$ vpišite:

a. Eno od izjavnih spremenljivk p, q, r ali njenih negacij, da dobite enega od osnovnih pravilnih sklepov.

$$p,\ p \Rightarrow \boxed{} \models q, \qquad\qquad p \vee q,\ \boxed{} \models p.$$

b. Enega od izjavnih veznikov $\wedge, \vee, \underline{\vee}, \Rightarrow, \Leftrightarrow$, da dobite pravilni sklep.

$$p \Rightarrow q,\ \neg q,\ \neg p \boxed{}\, r \models \neg r$$

c. Enega od izjavnih veznikov $\wedge, \vee, \underline{\vee}, \Rightarrow, \Leftrightarrow$, da dobite **nepravilni** sklep.

$$p \Rightarrow q,\ \neg q,\ \neg p \boxed{}\, r \models \neg r$$

Pojasnite, zakaj je dopolnjen sklep nepravilen.

NALOGA 2.
Naj bosta p in r izjavni spremenljivki. Odgovorite na naslednja vprašanja. Vse odgovore dobro utemeljite.

a. Ali je izjavni izraz $p \Rightarrow r$ tavtologija?
b. Ali je izjavni izraz $(p \Rightarrow r) \Rightarrow p$ tavtologija?
c. Ali je izjavni izraz $((p \Rightarrow r) \Rightarrow p) \Rightarrow p$ tavtologija?
d. Samo z uporabo izjavnega izraza $((p \Rightarrow r) \Rightarrow p) \Rightarrow p$, veznika $\Rightarrow$ in konstante 0 zapišite izjavni izraz, ki je protislovje.

NALOGA 3.

a. Navedite nabor izjavnih veznikov z vsaj 2 veznikoma, ki ni poln. Odgovor utemeljite.
b. Utemeljite, da je nabor izjavnih veznikov $\{\neg, \wedge, \vee\}$ poln.
(Namig: pomagate si lahko z obstojem konjuktivne ali disjunktivne normalne oblike.)

c. Naj bosta I in J izjavna izraza. Pri sklepu s protislovjem pravilnost sklepa $I \models J$ preverimo s pravilnostjo sklepa $I, \neg J \models 0$. Razložite, zakaj to lahko naredimo.

NALOGA 4.

a. Razvrstite izjavne veznike $\wedge, \vee, \Leftrightarrow$ glede na število 1 v resničnostni tabeli. Začnite s tistim, ki ima največ 1.

b. Naj bodo A, B, C izjavni izrazi. Obkrožite črke pred tistimi pari izjavnih izrazov, ki niso enakovredni za vse trojice A, B, C.

(i) $(A \wedge \neg B) \vee A,\ \neg B$ (ii) $\neg(\neg A \wedge B),\ A \vee \neg B$ (iii) $(A \vee B) \wedge C,\ (A \wedge C) \vee (B \wedge C)$

c. Naj bo $\{\triangle, \bigcirc, \otimes\}$ nek poln nabor izjavnih veznikov, $\{\bigcirc, \sqcup, *\}$ pa nabor, ki ni poln. Pod vsakega od naslednjih nabor napiši P, če je poln, N, če ni poln, in ?, če iz podatkov ni moč določiti, ali je poln.

$$\{\triangle, \bigcirc\}, \qquad \{\bigcirc, \sqcup\}, \qquad \{\bigcirc, \sqcup, *, \otimes\}, \qquad \{\bigcirc, \sqcup, \otimes, \triangle\}.$$

Naloga 5.

a. Kdaj pravimo, da sta dva izjavna izraza enakovredna?

b. Napišite disjunktivno normalno obliko izraza $I(p, q)$, ki ima naslednjo resničnostno tabelo:

p	q	$I(p,q)$
1	1	1
1	0	0
0	1	1
0	0	0

.

c. Napišite pravilo sklepanja modus ponens in dokažite, da velja.

Naloga 6.

a. Navedite oba de Morganova zakona iz izjavnega računa.

b. Konjunktivna normalna oblika izjavnega izraza $I(p, q, r)$ je naslednja:

$$(\neg p \vee \neg q \vee r) \wedge (\neg p \vee q \vee \neg r) \wedge (p \vee \neg q \vee \neg r) \wedge (p \vee \neg q \vee r).$$

Izpolnite manjkajoč stolpec v resničnostni tabeli izraza $I(p, q, r)$:

p	q	r	$I(p,q,r)$
1	1	1	
1	1	0	
1	0	1	
1	0	0	
0	1	1	
0	1	0	
0	0	1	
0	0	0	

.

c. Napišite pravilo sklepanja modus tollens in dokažite, da velja.

Naloga 7.

a. Naj bosta A, B izjavna izraza. Pravilo sklepanja Modus ponens s simboli zapišemo kot

$$A \Rightarrow B,\ A\ \models\ B.$$

Z besedami na kratko razložite pomen tega zapisa.
(Opomba: Iz $A \Rightarrow B$ in A sledi B ni zadostna utemeljitev.)

b. Predpis za negacijo $\neg$ lahko podamo s preslikavo $f : \{0,1\} \to \{0,1\}$, $f(p) = 1 - p$. Kateri dvomestni izjavni veznik predstavlja preslikava $g : \{0,1\} \times \{0,1\} \to \{0,1\}$, $g(p,q) = pq$?

c. Naj bosta f, g kot v (b). Kateri dvomestni izjavni izraz, zapisan z veznikoma $\neg, \vee$, predstavlja preslikava $f \circ g$?

Naloga 8.

a. Naj bosta A, B izjavna izraza. Pravilo sklepanja Modus tollens s simboli zapišemo kot

$$A \Rightarrow B,\ \neg B\ \models\ \neg A.$$

Z besedami na kratko razložite pomen tega zapisa.
(Opomba: Iz $A \Rightarrow B$ in $\neg B$ sledi $\neg A$ ni zadostna utemeljitev.)

b. Predpis za negacijo $\neg$ lahko podamo s preslikavo $f : \{0,1\} \to \{0,1\}$, $f(p) = 1 - p$. Kateri dvomestni izjavni veznik predstavlja preslikava $g : \{0,1\} \times \{0,1\} \to \{0,1\}$, $g(p,q) = |p - q|$?

c. Naj bosta f, g kot v (b). Kateri dvomestni izjavni veznik predstavlja preslikava $f \circ g$?

Naloga 9.

a. Za vsakega od izjavnih izrazov $p \Leftrightarrow p$ in $p \Leftrightarrow p \Leftrightarrow p$ navedite, ali je tavtologija. Odgovora utemeljite.

b. Naj bosta p in r izjavni spremenljivki. Ali obstaja izjavni izraz $I(p)$, tako da je izjavni izraz

$$I(p) \vee r$$

tavtologija? Če je odgovor da, navedite primer takega izjavnega izraza, sicer pa utemeljite, zakaj je odgovor ne.

Naloga 10.

a. Ali je izjavni izraz $p \Rightarrow p \vee p$ tavtologija? Odgovor utemeljite.

b. Naj bosta p in r izjavni spremenljivki. Ali obstaja izjavni izraz $I(p)$, tako da je izjavni izraz
$$I(p) \Rightarrow r$$
tavtologija? Če je odgovor da, navedite primer takega izjavnega izraza, sicer pa utemeljite, zakaj je odgovor ne.

Naloga 11.

V celi nalogi sta p, q izjavni spremenljivki in $\oplus$ izjavni veznik, za katerega velja
$$\neg p = p \oplus p \quad \text{in} \quad p \vee q = (p \oplus p) \oplus (q \oplus q).$$

a. Ali je nabor $\{\oplus\}$ poln? Odgovor utemeljite.

b. Samo z uporabo $\oplus$ izrazite $p \Rightarrow q$.

POGLAVJE 2

Predikatni račun

NALOGA 12.

Dana je izjavna formula

(1) $$(\forall x : \neg P(x)) \Rightarrow (\neg \exists x : P(x))\,.$$

a. Izberite si področje pogovora $\mathcal{D}$ in pomen predikata $P(x)$. Napišite interpretacijo izjavne formule (1) pri tej izbiri $\mathcal{D}$ in $P(x)$.

b. Izjavno formulo (1) preoblikujte v preneksno normalno obliko.

c. Ali je izjavna formula (1) splošno veljavna? Če je odgovor da, to utemeljite, sicer pa poiščite protiprimer.

NALOGA 13.

a. Navedite induktivno definicijo izjavne formule. (Definicije atoma vam ni potrebno razlagati.)

b. Dane so tri izjavne formule

$$\forall x \exists y : (P(y,x) \vee Q(x)),$$
$$\forall x \exists y : (P(y,x) \vee R(z)),$$
$$\neg \forall x \exists y : P(y,x) \vee R(z).$$

V spodnji interpretaciji s področjem pogovora D z besedami zapišite pomen vsake od njih!

področje pogovora D :	množica nalog na prvem izpitu iz DS.
$R(x)$:	x je naloga iz poglavja permutacij.
$Q(x)$:	x je najzahtevnejša naloga.
$P(x,y)$:	x je zahtevnejša naloga od naloge y.
z :	naloga 6 na prvem izpitu iz DS.

c. Tisto izjavno formulo iz prejšnje točke, ki ni v preneksni normalni formi, preoblikujte vanjo.

NALOGA 14.

a. Navedite oba distributivnostna zakona iz predikatnega računa.

b. Prepišite naslednjo izjavno formulo in dodajte oklepaje tako, da nakažete po kakšen vrstnem redu se računa njeno vrednost:

$$\forall x \exists y : P(x,y) \vee R(y) \wedge \neg Q(z) \vee \exists y \forall w : (T(w) \vee Z(x,y,w))$$

c. Naj bo dano področje pogovora

$\mathcal{D}$: predmeti v prvem letniku visokošolskega študija računalništva in informatike na FRI

in predikata

$$P(x) : x \text{ se izvaja v zimskem semestru,}$$
$$Q(x, y) : x \text{ in } y \text{ se izvajata v istem semestru.}$$

Napišite izjavno formulo W v preneksni obliki, ki zadošča naslednjim pogojem:

- Vsebuje spremenljivki x in y, ki sta vezani.
- Vsebuje konstanto z.
- Vsebuje predikata $P(x)$ in $Q(x, y)$.
- Ni resnična, če za konstanto z izberemo predmet *Diskretne strukture*.
- Je resnična, če za konstanto z izberemo predmet *Osnove verjetnosti in statistike*.

Naloga 15.

a. Prepišite izjavno formulo

$$\forall x Q(x) \wedge \neg R(y) \Rightarrow P(x, y)$$

in dodajte oklepaje, ki nakazujejo prednostni red računanja.

b. Naj bo $\mathcal{D} = \{\text{rdeča, modra, oranžna}\}$ področje pogovora in $P, Q : \mathcal{D} \to \{0, 1\}$ predikata, podana z naslednjo tabelo:

x	$P(x)$	$Q(x)$
rdeča	1	1
modra	0	0
oranžna	0	1

Ali je formula

$$\exists x \forall y : (P(x) \vee Q(y))$$

v zgornji interpretaciji resnična? Odgovor utemeljite.

Naloga 16.

a. Prepišite izjavno formulo

$$\exists x P(x, y) \Rightarrow \neg Q(x) \wedge R(y)$$

in dodajte oklepaje, ki nakazujejo prednostni red računanja.

b. Naj bo $\mathcal{D} = \{\text{rdeča, modra, oranžna}\}$ področje pogovora in $P, Q : \mathcal{D} \to \{0, 1\}$ predikata, podana z naslednjo tabelo:

x	$P(x)$	$Q(x)$
rdeča	1	1
modra	1	0
oranžna	0	0

Ali je formula

$$\forall x \exists y : (P(x) \wedge Q(y))$$

v zgornji interpretaciji resnična? Odgovor utemeljite.

Naloga 17.

Napišite preneksne normalne oblike naslednjih izjavnih formul:

a. $\neg \forall x \exists y : (P(x) \wedge Q(y))$.

b. $\forall x \neg \forall y : (\neg P(x) \vee Q(y))$.

c. $\exists x \neg \forall y : (P(x) \Rightarrow Q(y))$.

Naloga 18.

Naj bosta p, q izjavni spremenljivki in $\oplus$ izjavni veznik, za katerega velja

$$\neg p = p \oplus p \quad \text{in} \quad p \vee q = (p \oplus p) \oplus (q \oplus q).$$

Napišite preneksno normalno obliko izjavne formule $I \oplus I$, kjer je I izjavna formula

$$\forall x \exists y : ((P(x) \oplus P(x)) \oplus (Q(y) \oplus Q(y))).$$

POGLAVJE 3

Množice

NALOGA 19.
Naj bodo A, B, C množice.

a. Navedite enega od zakonov distributivnosti iz teorije množic.

b. Zakona absorpcije sta $A \cap (A \cup B) = A$ in $A \cup (A \cap B) = A$. Dokažite veljavnost enega od njiju.

c. Z uporabo zakonov distributivnosti in absorpcije preverite naslednjo enakost množic:
$$(A \cap B) \cup (A \cap B^c) = A.$$

NALOGA 20.
Naj bo U univerzalna množica, A, B, C pa njene podmnožice. V jeziku predikatnega računa vsebovanost $A \subseteq B$ izrazimo z izjavno formulo
$$\forall x \in U : (x \in A \Rightarrow x \in B).$$
V jeziku predikatnega računa izrazite še naslednje trditve, pri čemer lahko poleg izjavnih veznikov in kvantifikatorjev uporabljate še $\in$ (ne pa tudi $=$, $\subseteq$, $\subset$, $\supseteq$, $\supset$).

a. $A = B$.

b. $A \cap B = \emptyset$.

c. Če sta množici A in B disjunktni, potem množici B in C nista disjunktni.

NALOGA 21.

a. Navedite de Morganov zakon iz teorije množic.

b. Definirajte potenčno množico $\mathcal{P}A$ množice A.

c. Za vsako od naslednjih množic ugotovite, ali je potenčna množica neke množice. Če je odgovor da, navedite to množico, sicer pa utemeljite, zakaj je odgovor ne.
   (a) $\{\emptyset, 1, 2, \{1, 2\}\}$.
   (b) $\{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.
   (c) $\{\emptyset, \{1\}, \{\{2, 7\}\}, \{1, \{2, 7\}\}\}$.

NALOGA 22.

a. Ena izmed lastnosti kartezičnega produkta množic A, B, C, D je
$$(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D).$$
Ali lahko od tod sklepamo tudi $(A \cap B) \times (C \cap D) = (A \times D) \cap (B \times C)$?
Če je odgovor da, to utemeljite, sicer pa poiščite protiprimer.

b. Napišite primer množice A, katere potenčna množica ima 64 elementov.

c. Naj bo M množica refleksivnih relacij na vaši množici A iz (b). Koliko je $|M|$?

NALOGA 23.

a. Ena izmed lastnosti kartezičnega produkta množic A, B, C, D je
$$(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D).$$
Ali lahko od tod sklepamo tudi $(A \cap B) \times (C \cap D) = (B \times C) \cap (A \times D)$? Če je odgovor da, to utemeljite, sicer pa poiščite protiprimer.

b. Napišite primer množice A, katere potenčna množica ima 32 elementov.

c. Naj bo M množica simetričnih relacij na vaši množici A iz (b). Koliko je $|M|$?

NALOGA 24.

a. Določite množico A tako, da bo imela množica $\mathbb{N} \times A$ končno mnogo elementov. Napišite še, kaj je množica $\mathbb{N} \times A$.

b. Naj bo B množica dvomestnih izjavnih veznikov. Napišite tri elemente iz množice $\mathcal{P}(\mathbb{N} \times B)$.

c. Naj bo C množica tromestnih izjavnih veznikov in $f : \mathbb{N} \to C$ preslikava. Ali je f lahko injektivna? Če je odgovor da, napišite primer, sicer pa utemeljite, zakaj je odgovor ne.

NALOGA 25.

a. Določite množico A tako, da bo imela množica $\{1, 2, 3\} \times A$ neskončno mnogo elementov.

b. Naj bo B množica dvomestnih izjavnih veznikov. Napišite tri elemente iz množice $\mathcal{P}(B \times \mathbb{N})$.

c. Naj bo C množica tromestnih izjavnih veznikov in $f : C \to \mathbb{N}$ preslikava. Ali je f lahko surjektivna? Če je odgovor da, napišite primer, sicer pa utemeljite, zakaj je odgovor ne.

POGLAVJE 4

Relacije in preslikave

NALOGA 26.

Naj bo $f : \mathbb{N} \to \{1,2,3,4,5\}$ **surjektivna** preslikava, $A, B \subseteq \mathbb{N}$ množici in $g : A \to B$ taka preslikava, da je kompozitum $g \circ f : \mathbb{N} \to B$ dobro definirana preslikava. Odgovorite na naslednja vprašanja.

a. Napišite primer preslikave f z zgornjimi lastnostmi.

b. Kaj lahko iz dobre definiranosti $g \circ f$ sklepamo o množici A?

c. Ali obstaja taka množica A in preslikava $g : A \to \mathbb{N}$, da je $g \circ f$ surjektiven? Odgovor utemeljite.

d. Izberite taki množici A, B in preslikavo $g : A \to B$, da bo $g \circ f$ surjektiven.

NALOGA 27.

Naj bo $A = \{1,2,3,4,5\}$ množica.

a. Napišite primer relacije $R \subseteq A \times A$ z natanko tremi elementi.

b. Najmanj koliko elementov ima refleksivna relacija $R \subseteq A \times A$? Odgovor utemeljite.

c. Največ koliko elementov ima lahko relacija $R \subseteq A \times A$? Odgovor utemeljite.

d. Koliko različnih dvomestnih relacij na množici A obstaja? Odgovor utemeljite.

NALOGA 28.

Naj bosta $A = \{1,2,3,4\}$ in $B = \{b_1, b_2, b_3, b_4, b_5, b_6\}$ množici.

a. Napišite injektivno preslikavo $f : A \to B$.

b. Koliko preslikav iz množice A v B obstaja?

c. Koliko injektivnih preslikav iz množice A v B obstaja?

d. Naj bo $g : A \to B$ preslikava, definirana z $g(1) = g(2) = b_1$, $g(3) = b_2$, $g(4) = b_6$. Poiščite neko preslikavo $h : B \to B$, da velja $g = h \circ f$, kjer je f vaša preslikava iz (a).

NALOGA 29.

Naj bo A množica vseh obveznih predmetov na prvi stopnji Visokošolskega strokovnega študija FRI, B pa množica vseh obveznih predmetov na prvi stopnji Univerzitetnega študija FRI. Velja $A \cap B = \emptyset$. Naj bo R relacija na množici A, definirana s predpisom

$$xRy \quad \text{natanko tedaj, ko se } x \text{ in } y \text{ izvajata v istem letniku študija.}$$

Na isti način definiramo relacijo S na množici B.

a. Navedite definicijo ekvivalenčne relacije. Ali je R ekvivalenčna?

b. Kaj so ekvivalenčni razredi za S?

c. Če A in B vložimo v $A \cup B$, potem R in S postaneta relaciji na $A \cup B$. Določite $R * S$ in R^{-2020} na množici $A \cup B$.

NALOGA 30.

a. Kdaj je relacija $f \subseteq A \times A$ preslikava na množici A?

b. Poiščite množico A in preslikavo $f : A \to A$, ki je injektivna, a ni surjektivna.

c. Napišite in dokažite natančen pogoj za injektivnost kompozituma $f \circ f$, kjer je $f : A \to A$ preslikava.

NALOGA 31.

a. Kaj je dvomestna relacija R v množici A?

b. Naj bosta R in S dvomestni relaciji v množici A. Kaj je produkt relacij $R * S$?

c. Naj bo $A = \{x, y, z, u, v\}$ in $R = \{(x, y), (y, z), (z, u), (u, v)\}$. Določite tranzitivno ovojnico relacije R.

NALOGA 32.
Na množici študentov, ki so se udeležili izpita iz Diskretnih struktur, definiramo relaciji R in S:

$$\begin{aligned} xRy &\quad\Leftrightarrow\quad x \text{ in } y \text{ sta dobila enako oceno,} \\ xSy &\quad\Leftrightarrow\quad \text{Rezultat } x \text{ in } y \text{ se razlikuje za največ 1 točko.} \end{aligned}$$

a. Določite ekvivalenčne razrede tiste izmed relacij R in S, ki je ekvivalenčna.
Opomba. Ni vam potrebno utemeljevati, da je relacija res ekvivalenčna.

b. Utemeljite, zakaj druga izmed relacij R in S ni ekvivalenčna.

c. Študent x je dosegel na izpitu 94, študent z pa 96 točk. Ali lahko z gotovostjo trdimo, da sta študenta x in z v relaciji S^2? Odgovor utemeljite.

NALOGA 33.
Dana je množica $C = \{1, 2, 3, 4, 5\}$. Preslikava $f : C \to C$ zadošča pogojem $f(1) = 2$, $f(4) = 5$ in $f \circ f = \mathrm{id}_C$. Določite $f(2), f(3), f(5)$.

NALOGA 34.
V celi nalogi so dane množice $X = \{a, b, c, d\}$, $Y = \{1, 2, 3\}$ in $Z = \{F, G\}$. Naj bodo $f : X \to Y$, $g : Y \to Z$ in $h : Z \to X$ neke preslikave. V nalogi nas bodo zanimali še kompozitumi:

$$(*) \qquad g \circ f, \quad f \circ h, \quad h \circ g \circ f \quad \text{in} \quad g \circ h \circ f.$$

a. Navedite primer preslikave g, ki je surjektivna.

b. Enega od kompozitumov iz $(*)$ ne bomo mogli izračunati za nobeno trojico f, g, h. Navedite, kateri je to in kje je težava.

c. Samo eden od kompozitumov iz (∗) je lahko injektivna preslikava za neko trojico f, g, h. Navedite, kateri je to in napišite primer preslikav f, g, h, za katere je ta kompozitum res injektivna preslikava.

Naloga 35.

Relacija $R \subseteq \mathbb{Z}^2 \times \mathbb{Z}^2$ je podana s predpisom

$$(x_1, y_1)R(x_2, y_2) \quad \Leftrightarrow \quad (x_1, y_1) \text{ in } (x_2, y_2) \text{ sta rešitvi diofantske enačbe } 2x + 3y = 5.$$

Napišite vsaj 2 elementa iz definicijskega območja relacije R.

POGLAVJE 5

Teorija grafov

NALOGA 36.

O enostavnem grafu G (nima večkratnih povezav med dvema vozliščema in nima zank) imamo naslednje informacije:

- G vsebuje Hamiltonov cikel, ki je lihe dolžine.
- Največja stopnja vozlišča v grafu je 5.
- G ni poln graf.

Za vsako od naslednjih trditev napišite, ali je pravilna ali ne. Vsak odgovor utemeljite.

a. Graf G ni dvodelen.
b. Graf G je Eulerjev.
c. Za kromatično število $\chi(G)$ velja $3 \leq \chi(G) \leq 5$.
d. Graf G ima natanko 7 vozlišč.

NALOGA 37.

a. Narišite primer dvodelnega grafa, ki je Eulerjev.
b. Pojasnite, zakaj dvodelni graf na 12 točkah s 5 belimi in 7 črnimi točkami, ni Hamiltonov.
c. Koliko različnih Hamiltonovih ciklov ima poln graf na 5 točkah? Pri tem cikla štejemo za različna, če se razlikujeta vsaj v eni uporabljeni povezavi.

NALOGA 38.

V tej nalogi so vsi grafi enostavni, tj. nimajo večkratnih povezav med dvema vozliščema in nimajo zank.

a. Narišite dva neizomorfna grafa, ki imata stopnje vozlišč $2, 2, 2, 1, 1$.
b. Naj bo $2k_1, 2k_2, \ldots, 2k_m$, $k_i \in \mathbb{N}$, zaporedje sodih števil, ki je grafično. Ali je vsak graf, ki pripada temu zaporedju, Eulerjev? Če je odgovor da, to utemeljite, sicer pa napišite protiprimer (tj. izberete m in $k_1, \ldots, k_m$ ter narišete pripadajoč graf, ki ni Eulerjev).
c. Naj bo $n_1, n_2, \ldots, n_m$, $n_i \in \mathbb{N}$, zaporedje naravnih števil, ki je grafično. Denimo, da je nek graf, ki pripada temu zaporedju, dvodelen. Ali je tudi vsak drug graf, ki pripada temu zaporedju, dvodelen? Če je odgovor da, to utemeljite, sicer pa napišite protiprimer (tj. izberete m in $n_1, \ldots, n_m$ ter narišete dva grafa s temi parametri, pri čemer je en dvodelen, drugi pa ne).

NALOGA 39.

a. Naj bo G graf z n točkami in m povezavami. Napišite zvezo med stopnjami točk in številom povezav, ki jo podaja lema o rokovanju.

b. Kaj pomeni, da je končno zaporedje naravnih števil grafično?

c. Obkrožite črke pred tistimi zaporedji, ki so grafična:

(i) $5, 2, 1, 0$ (ii) $3, 3, 2, 1$ (iii) $3, 3, 3, 3$ (iv) $3, 3, 1, 1$.

d. Naj bo dano neko *padajoče* grafično zaporedje naravnih števil $n_1, n_2, n_3, \ldots, n_k$, kjer je $k \in \mathbb{N}$, in G eden izmed pripadajočih grafov.

(a) Kaj mora veljati za števila n_i, da bo G Eulerjev?

(b) Največ koliko je kromatično število $\chi(G)$? Odgovor utemeljite.

NALOGA 40.

a. Naj bo K_9 poln graf na 9 točkah, $H = (V, E)$ pa njemu izomorfen graf. Izpolnite:

(i) $|V| =$ (ii) $|E| =$ (iii) $\chi(H) =$ (iv) $H^c =$

b. Naj bo $G = (V, E)$ graf, kjer je V množica vozlišč, E pa množica povezav. Kaj pomeni, da je množica $S \subseteq V$ prerezna za graf G?

c. Naj bo G Hamiltonov graf in S prerezna množica moči k. Največ koliko komponent za povezanost ima $G - S$? Odgovor utemeljite.

NALOGA 41.
Za vsako od naslednjih trditev napišite, ali drži ali ne in odgovor pojasnite.

a. Poln graf na 5 točkah ima 20 povezav.

b. Komplement dvodelnega grafa s 5 točkami ni nikoli dvodelen.

c. Hamiltonov graf ima lahko dve komponenti za povezanost.

d. Obstaja graf z n vozlišči in m povezavami, $m > 2$, ki ima kromatično število $n \cdot m$.

e. Če Eulerjevemu grafu dodamo eno povezavo, potem novi graf ni Eulerjev.

NALOGA 42.
Vsi grafi v tej nalogi naj imajo neusmerjene povezave, nimajo zank in nimajo večkratnih povezav.

a. Narišite dva neizomorfna grafa s 4 vozlišči, ki sta Hamiltonova, a nista Eulerjeva.

b. Razložite, kaj v Brooksovem izreku ne velja v primeru, ko je G lih cikel.

c. Naj bo G graf s 27 vozlišči in kromatičnim številom $\chi(G) = 2$. Ali je G lahko Hamiltonov? Če je odgovor da, napišite primer, sicer pa utemeljite, zakaj je odgovor ne.

Naloga 43.

Relacija $\mathcal{R}$ na množici grafov (neusmerjeni, brez zank in brez večkratnih povezav) je podana s predpisom

$$G \,\mathcal{R}\, H \qquad \Leftrightarrow \qquad |V(G)| = |V(H)| \quad \text{in} \quad ||E(G)| - |E(H)|| = 2.$$

Narišite 2 neizomorfna grafa, ki sta v relaciji $\mathcal{R}$ z grafom P_4 (pot na 4 točkah).

Naloga 44.

Ali obstaja povezan graf G, ki zadošča $\chi(G) = 2022$ in $\Delta(G) = 2020$? Kaj pa povezan graf H, ki zadošča $\chi(H) = 2022$ in $\Delta(H) = 2021$?

Kot ponavadi nas zanimajo samo neusmerjeni grafi, ki nimajo zank ali večkratnih povezav. Če je odgovor da, navedite primer takega grafa, sicer pa utemeljite, zakaj je odgovor ne.

Naloga 45.

Grafu G z 2022 vozlišči odstranimo 5 povezav in dobimo graf z 2016 povezavami. Ali je G lahko Hamiltonov? Če je odgovor da, navedite primer takega grafa, sicer pa utemeljite, zakaj je odgovor ne.

POGLAVJE 6

Linearne diofantske enačbe in permutacije

NALOGA 46.

a. Z razširjenim Evklidovim algoritmom poiščite največji skupni delitelj števil 65 in 26.

b. Obkrožite črke pred tistimi linearnimi diofantskimi enačbami, ki nimajo nobene celoštevilske rešitve:

$$\text{(i)}\quad 65x + 26y = 16, \qquad \text{(ii)}\quad 65x + 26y = 130,$$
$$\text{(iii)}\quad 65x + 26y = -39, \qquad \text{(iv)}\quad 65x + 26y = 27.$$

c. Izberite eno od linearnih diofantskih enačb iz prejšnje točke, ki ima celoštevilske rešitve, in napišite formulo, ki opiše vse njene celoštevilske rešitve.

NALOGA 47.

a. Dana je enačba $84x + 63y = c$, kjer sta x, y celoštevilski spremenljivki, c pa celoštevilski parameter. Za katere parametre c ima enačba vsaj eno celoštevilsko rešitev?

b. Za najmanjši pozitiven celoštevilski c, pri katerem ima zgornja enačba celoštevilsko rešitev, napišite formulo, ki opiše vse celoštevilske rešitve.

NALOGA 48.

a. Dana je enačba $ax + by = c$, kjer sta x, y celoštevilski spremenljivki, a, b, c pa celoštevilski parametri.

   (a) Napišite potreben in zadosten pogoj na parametre a, b, c, da bo imela enačba vsaj eno celoštevilsko rešitev (x_0, y_0).

   (b) V primeru $a = 35$, $c = 21$ ugotovite, ali obstaja parameter b, za katerega ima enačba vsaj eno celoštevilsko rešitev. Odgovor utemeljite.

NALOGA 49.
Naj bosta

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 6 & 2 & 1 \end{pmatrix} \quad \text{in} \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 6 & 5 & 2 & 3 \end{pmatrix}$$

permutaciji.

a. Določite definicijsko območje in zalogo vrednosti permutacije π?

b. Zapišite permutacijo π v obliki produkta disjunktnih ciklov in določite njen red.

c. Zapišite permutacijo π v obliki produkta transpozicij in določite njeno parnost.

d. Izračunajte produkt $\pi * \psi$.

Naloga 50.

a. Naj bodo a, b, c pozitivna cela števila. Če a deli $b \cdot c$ in sta si a, b tuja, koliko je navečji skupni delitelj števil a in c? Odgovor utemeljite.

b. Naj bosta a, b pozitivni celi števili, ki sta si tuji. Ali obstajata pozitivni celi števili k, ℓ, da velja $ka + \ell b = 1$?

c. Napišite permutacijo α množice $\{1, 2, \ldots, 9\}$ s ciklično strukturo $[4, 4, 1]$.

d. Rešite enačbo $\pi^2 = \alpha$, kjer je α vaša rešitev točke (c).

Naloga 51.

a. Naj bodo b, c, d pozitivna cela števila. Če b deli $c \cdot d$ in sta si b, d tuja, koliko je navečji skupni delitelj števil b in c? Odgovor utemeljite.

b. Naj bosta a, b pozitivni celi števili, ki sta si tuji. Ali obstajata negativni celi števili k, ℓ, da velja $ka + \ell b = -1$?

c. Napišite permutacijo α množice $\{1, 2, \ldots, 7\}$ s ciklično strukturo $[3, 3, 1]$.

d. Rešite enačbo $\pi^2 = \alpha$, kjer je α vaša rešitev točke (c), π pa nima ciklične strukuture $[3, 3, 1]$.

Naloga 52.

a. Napišite primer naravnih števil a, b, za kateri velja $\gcd(a, b) = 2$ in $\mathrm{lcm}(a, b) = 20$.

b. Napišite permutacijo α reda 6 na množici 5 točk.

Naloga 53.

a. Napišite primer naravnih števil a, b, za kateri velja $\gcd(a, b) = 2$ in $\mathrm{lcm}(a, b) = 12$.

b. Napišite permutacijo α reda 6 na množici 6 točk, ki nima ciklične struktrure $\mathcal{C}(\alpha) = [6]$.

Naloga 54.

a. Naj bosta a in b števili, za kateri velja $\gcd(a,b)=2$. Koliko celoštevilskih rešitev $(x,y\in\mathbb{Z})$ ima enačba

$$ax+by=2022?$$

Odgovor utemeljite.

b. Ali obstajata naravni števili a in b, za kateri velja $\gcd(a,b)=2^5$ in $\operatorname{lcm}(a,b)=3^7$? Če je odgovor da, ju poiščite, sicer pa utemeljite, zakaj je odgovor ne.

c. Rešite permutacijsko enačbo

$$\varphi^2=\begin{pmatrix}1&2&3&4&5&6&7\\2&3&1&6&7&4&5\end{pmatrix}.$$

Naloga 55.
Poiščite celo število b, za katerega enačba $4x+by=20$ ima celoštevilske rešitve $(x,y\in\mathbb{Z})$, enačba $4x+20y=b$ pa jih nima.

Naloga 56.
Naj bo

$$\varphi=\begin{pmatrix}1&2&3&4&5&6&7\\3&x&y&2&z&w&5\end{pmatrix}$$

delno določena permutacija. Določite x,y,z tako, da bo φ^2 identična permutacija.

Del 2

Rešitve

Izjavni račun

Rešitev naloge 1.

a. $p,\ p \Rightarrow \boxed{q} \models q, \qquad p \vee q,\ \boxed{\neg q} \models p.$

b. $p \Rightarrow q,\ \neg q,\ \neg p \boxed{\veebar} r \models \neg r$

c. Pravilni so vezniki $\wedge, \vee, \Rightarrow, \Leftrightarrow$. Protiprimer za pravilnost sklepa so vrednosti izjavnih spremenljivk $p = 0$, $q = 0$, $r = 1$, saj je v tem primeru

$$p \Rightarrow q \sim 1, \quad \neg q \sim 1, \quad \neg p \boxed{\{\wedge, \vee, \Rightarrow, \Leftrightarrow\}} r \sim 1, \quad \neg r \sim 0.$$

Rešitev naloge 2.

a. Izjavni izraz ni tavtologija. Za $p = 1$ in $r = 0$ vrednost izraza ni 1: $1 \Rightarrow 0 \sim 0$.

b. Izjavni izraz ni tavtologija. Za $p = 0$ in $r = 0$ vrednost izraza ni 1:

$$(0 \Rightarrow 0) \Rightarrow 0 \sim 1 \Rightarrow 0 \sim 0.$$

c. Izjavni izraz je tavtologija. Preveriti moramo, da ima pri vseh naborih vrednosti izjavnih spremenljivk p in r izjavni izraz vrednost 1, tj.

$$\begin{aligned}
p = 1, r = 1: &\quad ((1 \Rightarrow 1) \Rightarrow 1) \Rightarrow 1 \sim 1 \Rightarrow 1 \sim 1,\\
p = 1, r = 0: &\quad ((1 \Rightarrow 0) \Rightarrow 1) \Rightarrow 1 \sim 1 \Rightarrow 1 \sim 1,\\
p = 0, r = 1: &\quad ((0 \Rightarrow 1) \Rightarrow 0) \Rightarrow 0 \sim (1 \Rightarrow 0) \Rightarrow 0 \sim 0 \Rightarrow 0 \sim 1,\\
p = 0, r = 0: &\quad ((0 \Rightarrow 0) \Rightarrow 0) \Rightarrow 0 \sim (1 \Rightarrow 0) \Rightarrow 0 \sim 0 \Rightarrow 0 \sim 1.
\end{aligned}$$

d. $(((p \Rightarrow r) \Rightarrow p) \Rightarrow p) \Rightarrow 0$.

Rešitev naloge 3.

a. Nabor $\{\vee, \wedge\}$ ni poln, saj ohranja logično vrednost 1, tj. $1 \vee 1 \sim 1$ in $1 \wedge 1 \sim 1$.

b. Za vsak izjavni izraz I obstaja izjavni izraz I', v katerem nastopajo samo vezniki $\neg, \wedge, \vee$, pri čemer imata I in I' isto resničnostno tabelo. Primera takega izjavnega izraza I' sta konjunktivna in disjunktivna normalna oblika izraza I.

c.
- Sklep $I \models J$ je pravilen natanko tedaj, ko iz $I \sim 1$ sledi $J \sim 1$.
- Sklep $I, \neg J \models 0$ pa je pravilen, ko iz $I \sim 1$ in $\neg J \sim 1$, sledi $0 \sim 1$. To pa je ekvivalentno temu, da iz $I \sim 1$ in $J \sim 0$, sledi $0 \sim 1$. Ker je $0 \not\sim 1$, je $I, \neg J \models 0$ pravilen natanko tedaj, ko predpostavki $I \sim 1$ in $J \sim 0$ nista nikoli izpolnjeni. To pa je res natanko tedaj, ko iz $I \sim 1$ sledi $J \sim 1$.
- Torej sta sklepa $I \models J$ in $I, \neg J \models 0$ enakovredna.

Rešitev naloge 4.

a. Največ 1 ima $\vee$, najmanj pa $\wedge$.

b. Izraza v (i) nista enakovredna. Za $A \sim 1$ in $B \sim 1$ je $(A \wedge \neg B) \vee A \sim 1$ in $\neg B \sim 0$.

Izraza v (ii) sta enakovredna, saj velja

$$\neg(\neg A \wedge B) \sim \neg\neg A \vee \neg B \sim A \vee \neg B.$$

Izraza v (iii) sta enakovredna, saj velja

$$(A \vee B) \wedge C \sim (A \wedge C) \vee (B \wedge C).$$

c.
- $\{\triangle, \bigcirc\}$: ?. Če od polnega nabora odvzamemo nek veznik, nov nabor ni nujno več poln.
- $\{\bigcirc, \sqcup\}$: N. Če od nepolnega nabora odvzamemo nek veznik, nov nabor ni poln.
- $\{\bigcirc, \sqcup, *, \otimes\}$: ?. Ta nabor ne vsebuje polnega nabora, niti ni podmnožica nepolnega nabora. Torej ne moremo nič sklepati o njegovi polnosti.
- $\{\bigcirc, \sqcup, \otimes, \triangle\}$: P. Ta nabor vsebuje poln nabora, torej je poln.

Rešitev naloge 5.

a. Izjavna izraza sta enakovredna, kadar imata za vsak nabor vrednosti izjavnih spremenljivk enaki logični vrednosti.

b. $(p \wedge q) \vee (\neg p \wedge q)$.

c. Modus ponens: $A \Rightarrow B, A \models B$.

A	B	$A \Rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

Predpostavki $A \Rightarrow B$ in A sta resnični samo v prvi vrstici zgornje tabele, kjer je resničen tudi zaključek B. Torej je sklep pravilen.

Rešitev naloge 6.

a. $\neg(A \wedge B) \sim \neg A \vee \neg B$ in $\neg(A \vee B) \sim \neg A \wedge \neg B$.

b.

p	q	r	$I(p,q,r)$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	1

.

c. Modus tollens: $A \Rightarrow B, \neg B \models \neg A$

Iz resničnostne tabele

A	B	$A \Rightarrow B$	$\neg B$	$\neg A$
1	1	1	0	0
1	0	0	1	0
0	1	1	0	1
0	0	1	1	1

opazimo, da imata obe predpostavki $A \Rightarrow B$ in $\neg B$ hkrati vrednost 1 samo za $A \sim B \sim 0$. Takrat pa ima tudi zaključek $\neg A$ vrednost 1.

Rešitev naloge 7.

a. Pri vseh naborih vrednosti A, B, za katere sta izraza $A \Rightarrow B$ in A resnična, je resničen tudi izraz B.

b. Ker je $g(1,1) = 1$ in $g(1,0) = g(0,1) = g(0,0) = 0$, g predstavlja $\wedge$.

c. 1. možnost: Ker je $(f \circ g)(1,1) = f(g(1,1)) = f(1) = 0$ in podobno $(f \circ g)(0,0) = (f \circ g)(1,0) = (f \circ g)(0,1) = 1$, g predstavlja $\neg p \vee \neg q$.

2. možnost: $(f \circ g)(p,q) = f(g(p,q)) = f(p \wedge q) = \neg(p \wedge q) = \neg p \vee \neg q$.

Rešitev naloge 8.

a. Pri vseh naborih vrednosti A, B, za katere sta izraza $A \Rightarrow B$ in $\neg B$ resnična, je resničen tudi izraz $\neg A$.

b. Ker je $g(1,1) = g(0,0) = 0$ in $g(1,0) = g(0,1) = 1$, g predstavlja $\veebar$.

c. 1. možnost: Ker je $(f \circ g)(1,1) = f(g(1,1)) = f(0) = 1$ in podobno $(f \circ g)(0,0) = 1$, $(f \circ g)(1,0) = (f \circ g)(0,1) = 0$, g predstavlja $\Leftrightarrow$.

2. možnost: $(f \circ g)(p,q) = f(g(p,q)) = f(p \veebar q) = \neg(p \veebar q) = p \Leftrightarrow q$.

Rešitev naloge 9.

a. Ker je $1 \Leftrightarrow 1 \sim 1$ in $0 \Leftrightarrow 0 \sim 1$, je izraz $p \Leftrightarrow p$ tavtologija. Ker je
$$(0 \Leftrightarrow 0) \Leftrightarrow 0 \sim 1 \Leftrightarrow 0 \sim 0,$$
izraz $p \Leftrightarrow p \Leftrightarrow p$ ni tavtologija.

b. Če za $I(p)$ vzamemo katerokoli tavtologijo, bo izraz $I(p) \vee r$ tavtologija. $I(p)$ je npr. 1, $p \vee \neg p$, $p \Leftrightarrow p$, $\ldots$

Rešitev naloge 10.

a. Ker je $1 \Rightarrow (1 \vee 1) \sim 1 \Rightarrow 1 \sim 1$ in $0 \Rightarrow (0 \vee 0) \sim 0 \Rightarrow 0 \sim 1$, je izraz $p \Rightarrow p \vee p$ tavtologija.

b. Če za $I(p)$ vzamemo katerokoli protislovje, bo izraz $I(p) \Rightarrow r$ tavtologija. $I(p)$ je npr. 0, $p \wedge \neg p$, $p \Leftrightarrow \neg p$, $\ldots$

Rešitev naloge 11.

a. Nabor $\{\oplus\}$ je poln, saj se da z njim izraziti oba veznika iz polnega nabora $\{\neg, \vee\}$.

b.
$$p \Rightarrow q \ \sim\ \neg p \vee q \ \sim\ (p \oplus p) \vee q \ \sim\ ((p \oplus p) \oplus (p \oplus p)) \oplus (q \oplus q).$$

Predikatni račun

Rešitev naloge 12.

a. Pri izbiri $\mathcal{D} = \mathbb{N}$ in $P(x)$: 'x je sodo število.' je interpretacija formule (1): Če za vsako naravno število velja, da ni sodo, potem ne obstaja naravno število, ki bi bilo sodo.

b.
$$\begin{aligned}
&(\forall x : \neg P(x)) \Rightarrow (\neg \exists x : P(x)) \\
&\sim (\forall x : \neg P(x)) \Rightarrow (\neg \exists y : P(y)) \\
&\sim \neg (\forall x : \neg P(x)) \vee (\neg \exists y : P(y)) \\
&\sim (\exists x : P(x)) \vee (\forall y : \neg P(y)) \\
&\sim \exists x : (P(x) \vee \forall y : \neg P(y)) \\
&\sim \exists x \forall y : (P(x) \vee \neg P(y)) \,.
\end{aligned}$$

c. Formula je splošno veljavna. V interpretaciji s področjem pogovora $\mathcal{D}$ mora obstajati $d \in \mathcal{D}$, tako da za vsak $d' \in \mathcal{D}$ velja $P(d) \vee \neg P(d') \sim 1$. Če obstaja d_0, da velja $P(d_0) \sim 1$, potem je $d = d_0$ dober za vse d'. Če pa tak d_0 ne obstaja, potem za vsak d' velja $\neg P(d') \sim 1$ in za d lahko vzamemo katerikoli element iz $\mathcal{D}$.

Rešitev naloge 13. ⇧

a. Izjavne formule so definirane induktivno:
   - Atomi so izjavne formule.
   - Če sta W in V izjavni formuli in je x spremenljivka, potem so tudi

$$(\neg W), (W \wedge V), (W \vee V), (W \Rightarrow V), (W \iff V), \ldots$$
$$(\exists x\, W) \quad \text{in} \quad (\forall x\, W)$$

   izjavne formule.

b.
   - Na prvem izpitu iz DS za vsako nalogo velja naslednja trditev: Naloga je najzahtevnejša ali pa obstaja naloga, ki je zahtevnejša od nje.
   - Na prvem izpitu iz DS za vsako nalogo velja naslednje trditev: Obstaja naloga, ki je zahtevnejša od nje ali pa je naloga z iz področja permutacij.
   - Na prvem izpitu iz DS velja naslednja trditev: Ni res, da za vsako nalogo obstaja naloga, ki je zahtevnejša od nje ali pa je naloga z iz področja permutacij.

c. $\exists x \forall y : (\neg P(y, x) \wedge \neg R(z))$.

Rešitev naloge 14. ⇧

a. $\forall x : (W \wedge V) \sim \forall x : W \wedge \forall x : V$ in $\exists x : (W \vee V) \sim \exists x : W \vee \exists x : V$.

b.

$$((\forall x \exists y : P(x, y)) \vee (R(y) \wedge (\neg Q(z)))) \vee (\exists y \forall w : (T(w) \vee Z(x, y, w)))$$

c. Primer izjavne formule W:

$$\exists x \exists y : (P(x) \wedge Q(x, y) \wedge \neg P(z)).$$

Rešitev naloge 15. ⇧

a. $((\forall x Q(x)) \wedge (\neg R(y))) \Rightarrow P(x, y)$.

b. Da, formula je resnična. Ko ima x vrednost 'rdeča', je za vsak y izjava $P(\text{rdeča}) \vee Q(y)$ resnična.

Rešitev naloge 16. ⇧

a. $(\exists x P(x, y)) \Rightarrow ((\neg Q(x)) \wedge R(y))$.

b. Ne, formula ni resnična. Ko ima x vrednost 'oranžna', ne obstaja y, da bi bila izjava $P(\text{oranžna}) \wedge Q(y)$ resnična.

Rešitev naloge 17.

a. $\exists x \forall y : (\neg P(x) \vee \neg Q(y))$.

b. $\forall x \exists y : (P(x) \wedge \neg Q(y))$.

c. $\exists x \exists y : (P(x) \wedge \neg Q(y))$.

Rešitev naloge 18.

$$
\begin{aligned}
I \oplus I &\sim \neg \forall x \exists y : ((P(x) \oplus P(x)) \oplus (Q(y) \oplus Q(y))) \\
&\sim \neg \forall x \exists y : (P(x) \vee Q(y)) \\
&\sim \exists x \forall y : (\neg P(x) \wedge \neg Q(y))
\end{aligned}
$$

Množice

Rešitev naloge 19.

a. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ ali $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

b. $A \cap (A \cup B) = A :$
Vsebovanost $\subseteq$: Naj bo $x \in A \cap (A \cup B)$. Posebej velja $x \in A$. Torej je $A \cap (A \cup B) \subseteq A$.
Vsebovanost $\supseteq$: Velja $A \subseteq A$ in $A \subseteq A \cup B$. Torej je $A \subseteq A \cap (A \cup B)$.

$A \cup (A \cap B) = A :$
Vsebovanost $\subseteq$: Velja $A \subseteq A$ in $A \cap B \subseteq A$. Torej je $A \cup (A \cap B) \subseteq A$.
Vsebovanost $\supseteq$: Iz $A \subseteq A$ sledi $A \subseteq A \cup (A \cap B)$.

c. Velja:

$$
\begin{aligned}
(A \cap B) \cup (A \cap B^c) &= ((A \cap B) \cup A) \cap ((A \cap B) \cup B^c) \\
&= A \cap ((A \cap B) \cup B^c) \\
&= A \cap ((A \cup B^c) \cap (B \cup B^c)) \\
&= A \cap (A \cup B^c) \\
&= A,
\end{aligned}
$$

kjer smo v prvi in tretji enakosti uporabili zakon distributivnosti, v drugi in peti zakon absorpcije, v četrti pa dejstvo, da je $B \cup B^c$ enako univerzalni množici.

Rešitev naloge 20.

a. Pravilni odgovor je katerikoli od naslednjih:
- $\forall x \in U : ((x \in A \Rightarrow x \in B) \ \wedge \ (x \in B \Rightarrow x \in A))$,
- $\forall x \in U : (x \in A \Rightarrow x \in B) \ \wedge \ \forall x \in U : (x \in B \Rightarrow x \in A)$,

- $\forall x \in U : (x \in A \Rightarrow x \in B) \ \wedge \ \forall y \in U : (y \in B \Rightarrow y \in A)$,
- $\forall x \in U : (x \in A \wedge x \in B \ \vee \ \neg(x \in A) \wedge \neg(x \in B))$.
- $\forall x \in U : (x \in A \wedge x \in B \ \vee \ x \notin A \wedge x \notin B)$.

b. Pravilni odgovor je katerikoli od naslednjih:
- $\forall x \in U : (\neg(x \in A) \vee \neg(x \in B))$,
- $\forall x \in U : (x \notin A \vee x \notin B)$,
- $\forall x \in U : ((x \in A \Rightarrow \neg(x \in B)) \ \wedge \ (x \in B \Rightarrow \neg(x \in A)))$,
- $\forall x \in U : (x \in A \wedge \neg(x \in B) \ \vee \ \neg(x \in A) \wedge x \in B \ \vee \ \neg(x \in A) \wedge \neg(x \in B))$.

c. Pravilni odgovor je

$$\forall x \in U : (\neg(x \in A) \vee \neg(x \in B)) \Rightarrow \exists x \in U : (x \in B \wedge x \in C).$$

Rešitev naloge 21.

a. $(A \cap B)^c = A^c \cup B^c$ in $(A \cup B)^c = A^c \cap B^c$.

b. $\mathcal{P}A = \{X : X \subseteq A\}$.

c.
- Ni potenčna množica, saj elementa 1, 2 nista množici.
- Ni potenčna množica, saj ne vsebuje $\emptyset$.
- Je potenčna možica množice $\{1, \{2, 7\}\}$.

Rešitev naloge 22.

a. Da, saj lahko v $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$ zamenjamo vlogi množic C in D.

b. $A = \{1, 2, 3, 4, 5, 6\}$. V tem primeru ima $\mathcal{P}(A)$ natanko $2^6 = 64$ elementov.

c. Refleksivna relacija R vsebuje vse pare $(1, 1), \ldots, (6, 6)$. Vsi ostali urejeni pari (i, j), $i \neq j$, $i, j \in A$, pa so lahko vsebovani v R ali pa ne. Takih parov je $6 \cdot 5 = 30$. Torej je refleksivnih relacij $2^{30} = |M|$.

Rešitev naloge 23.

a. Da, saj lahko v $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$ zamenjamo vlogi množic A in B.

b. $A = \{1, 2, 3, 4, 5\}$. V tem primeru ima $\mathcal{P}(A)$ natanko $2^5 = 32$ elementov.

c. Vsak par $(1, 1), \ldots, (5, 5)$ je lahko vsebovan v simetrični relaciji R ali pa ne. Za vsak urejen par (i, j), $i \neq j$, $i, j \in A$, ki je v R, pa mora biti v R tudi (j, i). Takih dvojic $(i, j), (j, i)$ je $\binom{5}{2} = \frac{5 \cdot 4}{2} = 10$. Vsaka je vsebovana v R ali pa ni. Torej je simetričnih relacij $2^{5+10} = 2^{15} = |M|$.

Rešitev naloge 24.

a. $A = \emptyset$ in $\mathbb{N} \times A = \emptyset$. Če ima A vsaj en element, je množica $\mathbb{N} \times A$ neskončna.

b. $\mathcal{P}(\mathbb{N} \times B) = \{\emptyset, \mathbb{N} \times B, \{(1, \wedge)\}, \{(1, \wedge), (1, \vee)\}, \dots\}$.

c. f ne more biti injektivna, saj je njena domena neskončna množica $\mathbb{N}$, njena kodomena pa končna množica C.

Rešitev naloge 25.

a. Npr. $A = \mathbb{N}$. Katerakoli neskončna množica je ustrezna. Če ima A končno mnogo elementov, bo imela tudi množica $\{1, 2, 3\} \times A$ končno mnogo elementov.

b. $\mathcal{P}(B \times \mathbb{N}) = \{\emptyset, B \times \mathbb{N}, \{(\wedge, 1)\}, \{(\wedge, 1), (\vee, 1)\}, \dots\}$.

c. f ne more biti surjektivna, saj je njena domena končna množica C, njena kodomena pa neskončna množica $\mathbb{N}$.

Relacije in preslikave

Rešitev naloge 26.

a. Pravilni odgovori so npr.:
   - $f(x) = \begin{cases} x, & \text{za } 1 \leq x \leq 5, \\ 1, & \text{sicer.} \end{cases}$
   - Katerokoli premešanje števil 1 do 5, vsa ostala števila pa preslikana kamorkoli v množico $\{1, 2, 3, 4, 5\}$.
   - $f(x) = (x \mod 5) + 1$.

b. Ker je f surjektivna, je $\mathcal{Z}_f = \{1, 2, 3, 4, 5\}$. Torej moramo poznati $g(i)$ za vsak $i = 1, 2, 3, 4, 5$. Zato je $\{1, 2, 3, 4, 5\} \subseteq A$.

c. Ne obstaja. Ker je zaloga vrednosti $\mathcal{Z}_f$ moči 5, je tudi zaloga vrednosti kompozituma $g \circ f$ največ moči 5. Ker je $g \circ f : \mathbb{N} \to \mathbb{N}$, bi morala biti tudi slika kompozituma enaka $\mathbb{N}$. To pa ne gre.

d. Npr. $A = \{1, 2, 3, 4, 5\}$, $B = \{1\}$ in $g(i) = 1$ za vsak $i \in A$.

Rešitev naloge 27.

a. Primer relacije je $R = \{(a, b), (c, d), (e, f)\}$, kjer so a, b, c, d, e, f katera koli števila (ne nujno različna) iz A.

b. Najmanj 5, tj. $(1,1),(2,2),(3,3),(4,4),(5,5)$. Lahko pa še katerega koli od preostalih.

c. 25, saj je različnih elementov v množici $A \times A$ ravno $25 = 5^2$.

d. Vsak izmed elementov iz $A \times A$ je bodisi element R bodisi ni. Torej je različnih relacij $2^{\text{št. elementov } A \times A} = 2^{25}$.

Rešitev naloge 28.

a. $f(1) = b_1,\ f(2) = b_2,\ f(3) = b_3,\ f(4) = b_4$.

b. 6^4, saj lahko vsak element iz A preslikamo v kateregakoli izmed šestih elementov množice B.

c. $6 \cdot 5 \cdot 4 \cdot 3 = 360$. Element 1 lahko preslikamo v kateregakoli izmed šestih elementov množice B, 2 v kateregakoli izmed petih preostalih, 3 v kateregakoli izmed štirih preostalih in 4 v kateregakoli izmed treh preostalih.

d. Veljati mora

$$\begin{aligned} b_1 &= g(1) = (h \circ f)(1) = h(f(1)) = h(b_1), \\ b_1 &= g(2) = (h \circ f)(2) = h(f(2)) = h(b_2), \\ b_2 &= g(3) = (h \circ f)(3) = h(f(3)) = h(b_3), \\ b_6 &= g(4) = (h \circ f)(4) = h(f(4)) = h(b_4). \end{aligned}$$

Ostala elementa b_5, b_6 pa se lahko slikata kamorkoli v B, npr. $h(b_5) = h(b_6) = b_1$.

Rešitev naloge 29.

a. Ekvivalenčna relacija R je relacija na množici A, ki je refleksivna ($(x,x) \in R$ za vsak $x \in A$), simetrična ($(x,y) \in R \;\Rightarrow\; (y,x) \in R$ za vsaka $x, y \in A$) in tranzitivna (Za vse trojice $x,y,z \in A$ iz $(x,y) \in R$ in $(y,z) \in R$, sledi $(x,z) \in R$.). Relacija R v nalogi je ekvivalenčna.

b. Relacija S ima tri ekvivalenčne razrede. V prvem so obvezni predmeti, ki se izvajajo v prvem letniku prve stopnje uni študija na FRI, v drugem predmeti drugega letnika, v tretjem pa predmeti tretjega letnika.

c. $R * S = \emptyset$. Ker je R ekvivalenčna relacija na A, je $R^{-2020} = (R^{-1})^{2020} = R^{2020} = R$. Torej tudi na $A \cup B$ velja $R^{-2020} = R$.

Rešitev naloge 30.

a. Relacija f je preslikava, če je enolična, je njena domena D_f cela množica A in je njena slika $\mathcal{Z}_f$ podmnožica A.

b. $f : \mathbb{N} \to \mathbb{N}$, $f(x) = x + 1$.

c. Kompozitum $f \circ f$ je injektiven natanko tedaj, ko je preslikava f injektivna.

Dokaz v smer ($\Rightarrow$). Če f ne bi bila injektivna, bi obstajala x in y z $x \neq y$, za katera bi bilo $f(x) = f(y)$ in zato $f(f(x)) = f(f(y))$. Toda to je v nasprotju z injektivnostjo $f \circ f$.

Dokaz v smer ($\Leftarrow$). Dokazati moramo, da iz $(f \circ f)(x) = (f \circ f)(y)$ sledi $x = y$. Po definiciji kompozituma velja $f(f(x)) = f(f(y))$. Ker je f injektivna, sledi od tod $f(x) = f(y)$. Ker je f injektivna, je $x = y$.

Rešitev naloge 31.

a. Dvomestna relacija R v A je množica urejenih parov elementov iz $A \times A$.

b. Pravilen odgovor je katerikoli od naslednjih:
   - $R * S$ je relacija v množici A, katere elementi so urejeni pari $(x, y) \in A \times A$, za katere obstaja nek $z \in A$, tako da velja xRz in zSy.
   - $R * S = \{(x, y) \in A \times A\colon \text{za nek } z \in A \text{ velja } xRz \text{ in } zSy\}$.

c. $R^+ = \{(x, y), (y, z), (z, u), (u, v), (x, z), (x, u), (x, v), (y, u), (y, v), (z, v)\}$.

Rešitev naloge 32.

a. Ekvivalenčna relacija je R. Vsi študentje, ki so na izpitu dobili enako oceno, so v istem ekvivalenčnem razredu. Ekvivalenčni razredi so $R[5] = \{x\colon x \text{ je dobil oceno } 5\}$, ..., $R[10] = \{x\colon x \text{ je dobil oceno } 10\}$.

b. Relacija S ni ekvivalenčna, saj ni tranzitivna. Za študente x, y, z, ki so na izpitu dosegli 63, 64, 65 točk velja, xSy in ySz, ne velja pa xSz.

c. x in z sta v relaciji S^2 natanko tedaj, ko obstaja y, da velja xSy in ySz. Tak y bo obstajal, če se bo njegov rezultat razlikoval največ za 1 točko od 94 in 96. Torej bosta x in z v relaciji S^2 natanko tedaj, ko obstaja študent, ki je na izpitu dosegel 95 točk.

Rešitev naloge 33.
Iz pogoja $f \circ f = \mathrm{id}_C$ sledi $f(2) = 1$ in $f(5) = 4$. Iz bijektivnosti pa sledi še $f(3) = 3$.

Rešitev naloge 34.

a. $g(1) = g(2) = F$, $g(3) = G$.

b. Kompozitum $g \circ h \circ f$ ni smiseln, saj f slika v Y, definicijsko območje h pa je Z.

c. Injektivna preslikava je lahko $f \circ h$. Npr., $h(F) = a$, $h(G) = b$, $f(a) = f(c) = f(d) = 1$, $f(b) = 2$. Preslikave g ne potrebujemo.

Rešitev naloge 35.

V definicijskem območju R so ravno vsi pari (x, y), ki rešijo enačbo $2x + 3y = 5$. Npr. $(1, 1), (4, -1), (7, -3), \ldots$.

Teorija grafov

Rešitev naloge 36.

a. Trditev je pravilna. Graf G vsebuje cikel lihe dolžine, zato ni dvodelen.

b. Trditev ni pravilna. Graf G ni Eulerjev, saj obstaja točka lihe stopnje (tj. 5).

c. Trditev je pravilna. Kromatično število je $\chi(G)$ je več kot 2, saj graf G ni dvodelen. Ker je največja stopnja vozlišča 5, je $\chi(G) \leq 6$. Ker pa graf ni niti lih cikel (saj obstaja točka stopnje več kot 2) niti poln graf, po Brooksovem izreku velja $\chi(G) \leq 5$.

d. Trditev ni pravilna. Graf $G = (V, E)$ z 9 vozlišči, ki ustreza pogojem naloge, je

$$V = \{v_1, v_2, \ldots, v_9\},$$
$$E = \{(v_1, v_2), (v_2, v_3), \ldots, (v_8, v_9), (v_1, v_3), (v_1, v_4), (v_1, v_5), (v_1, v_6)\}$$

Rešitev naloge 37.

a. Npr. cikel na 4 točkah.

b. Če odstranimo vseh 5 belih točk, graf razpade na 7 komponent. Po izreku o razpadu zato prvotni graf ni Hamiltonov.

c. Fiksirajmo neko vozlišče. Cikel lahko začnemo po kateri koli od štirih povezav. V naslednjem vozlišču izbiramo med tremi preostalimi, nato med dvema, zadnja povezava pa je določena. Upoštevati moramo še, da smo vsak cikel dvakrat šteli, saj smo ga lahko prepotovali v eno ali v druge smer, tj. $v_1v_3v_5v_4v_2$ je isti cikel kot $v_1v_2v_4v_5v_3$. Imamo $\frac{4 \cdot 3 \cdot 2}{2} = 12$ ciklov.

Rešitev naloge 38.

a. Prvi graf je pot na pet točkah, drugi pa unija cikla na treh točkah in poti na dveh točkah.

b. Če je graf povezan, potem je odgovor da, saj je graf Eulerjev natanko tedaj, ko so vsa vozlišča sodih stopnj. Če pa graf ni povezan, je odgovor ne.

c. Ne. Za zaporedje $2, 2, 2, 1, 1$ sta grafa iz rešitve točke (a) protiprimera. Prvi je dvodelen, drugi pa ni.

Rešitev naloge 39.

a. Naj bo $G = (V, E)$ graf, kjer je V množica vozlišč, E pa množica povezav. Velja $\sum_{v \in V} \deg(v) = 2|E|$.

b. Zaporedje je grafično, če obstaja graf, katerega stopnje vozlišč so v bijektivni korespondenci z danim zaporedjem.

c.
- Zaporedje $5, 2, 1, 0$ ni grafično, saj bi moralo biti prvo vozlišče povezano s 5 vozlišči, na razpolago pa so le 3.
- Zaporedje $3, 3, 2, 1$ ni grafično, saj vsota števil v zaporedju ni soda.
- Zaporedje $3, 3, 3, 3$ je grafično. Ustreza mu poln graf na 4 točkah.
- Po izreku je zaporedje $3, 3, 1, 1$ grafično natanko tedaj, ko je $2, 2, 0, 0$ grafično. To pa ni grafično, saj bi moralo biti prvo vozlišče povezano z dvema vozliščema, na razpolago pa je le eno.

d.
- Vsa števila n_i bi morala biti soda.
- Kromatično število grafa je največ za 1 večje od stopnje največjega vozlišča, saj požrešna metoda barvanja deluje. Torej je največ $n_1 + 1$.

Rešitev naloge 40.

a. $|V| = 9$, $|E| = \frac{9 \cdot 8}{2} = 36$, $\chi(H) = 9$, $H^c = \emptyset$.

b. Množica $S \subseteq V$ je prerezna, če po odstranitvi vseh vozlišč in povezav, ki imajo vsaj eno krajišče v S, graf razpade na več povezanih komponent, kot jih je imel prvotni graf.

c. Graf $G - S$ ima največ k komponent za povezanost. Če bi jih imel več, bi moral Hamiltonov cikel vsaj $(k + 1)$-krat zamenjati komponento, pri čemer bi moral iti na vsakem koraku prek vozlišča v S. Ker je teh le k, to ne bi šlo.

Rešitev naloge 41.

a. Ne drži, saj ima poln graf na 5 točkah $\frac{5 \cdot 4}{2} = 10$ povezav.

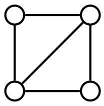
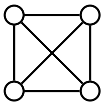
b. Drži, saj ima vsaj ena množica razbitja grafa vsaj 3 vozlišča. V komplementu grafa so vse vozlišča iste množice razbitja povezana, torej dobimo cikel dolžine 3.

c. Ne drži. Če ima graf dve komponenti za povezanost, potem ne obstaja cikel, ki vsebuje vse točke grafa.

d. Ne drži. Kromatično število grafa je navzgor omejeno s številom vozlišč, tj. n.

e. Drži. Če Eulerjevemu grafu dodamo eno povezavo, potem obstajata natanko dve vozlišči lihe stopnje. Graf je namreč Eulerjev natanko tedaj, ko so vsa vozlišča sodih stopenj.

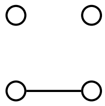
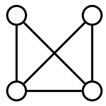
Rešitev naloge 42.

a.  

b. V primeru, ko je G lih cikel, ne velja desna neenakost $\chi(G) \leq \Delta(G)$ v Brooksovem izreku, saj je $\chi(G) = 3$ in $\Delta(G) = 2$.

c. Ker je $\chi(G) = 2$, je G dvodelen. Ker je vozlišč liho mnogo, barvna razreda nista enako velika. Za take grafe pa vemo (npr. z uporabo izreka o razpadu, kjer za prerezno množico vzamemo barvni razred z manjšim številom točk), da niso Hamiltonovi.

Rešitev naloge 43.

Dva primera grafov sta G_1:  G_2: 

Rešitev naloge 44.
Za povezan neusmerjen graf brez zank ali večkratnih povezav velja $\chi(G) \leq \Delta(G)+1$. Ker ne velja $2022 \leq 2021$, tak graf G ne obstaja.

Primer grafa H je poln graf na 2022 točkah.

Rešitev naloge 45.
Graf G ni Hamiltonov, saj bi moral imeti vsaj 2022 povezav (da ima lahko cikel), ima pa jih samo 2021.

Linearne diofantske enačbe in permutacije

Rešitev naloge 46.

a.

$$
\begin{aligned}
(1): \quad & 65 = 1 \cdot 65 + 0 \cdot 26, & & \\
(2): \quad & 26 = 0 \cdot 65 + 1 \cdot 26, & & 65 = 2 \cdot 26 + 13, \\
(3) = (1) - 2(2): \quad & 13 = 1 \cdot 65 - 2 \cdot 26, & & 26 = 2 \cdot 13 + 0, \\
(4) = (2) - 2(3): \quad & 0 = -2 \cdot 65 + 5 \cdot 26. & &
\end{aligned}
$$

Torej je $D(65, 26) = 13$.

b. Veljati mora, da $D(65, 26)$ deli desno stran enačbe. Enačbi z desno stranjo 16 oz. 27 nimata celoštevilskih rešitev, tisti z 130 in -39 pa imata celoštevilske rešitve.

c. Izberimo enačbo $65x + 26y = 130$. Eno od rešitev (x_0, y_0) dobimo tako, da predzadnjo vrstico razširjenega Evklidovega algoritma pomnožimo z $\frac{130}{13} = 10$. Torej $130 = 10 \cdot 65 - 20 \cdot 26$ in zato $(x_0, y_0) = (10, -20)$. Vse rešitve pa so oblike

$$\left(x_0 + k \cdot \frac{26}{13}, y_0 - k \cdot \frac{65}{13}\right) = (10 + 2k, -20 - 5k),$$

kjer je $k \in \mathbb{Z}$.

Rešitev naloge 47.

a.

$$\begin{array}{rll} (1): & 84 = 1 \cdot 84 + 0 \cdot 63, & \\ (2): & 63 = 0 \cdot 84 + 1 \cdot 63, & 84 = 1 \cdot 63 + 21, \\ (3) = (1) - (2): & 21 = 1 \cdot 84 - 1 \cdot 63, & 63 = 3 \cdot 21 + 0, \\ (4) = (2) - 3(3): & 0 = -3 \cdot 84 + 4 \cdot 63. & \end{array}$$

Torej je $D(84, 63) = 21$. Zato mora biti c celoštevilski večkratnik števila 21.

b. Najmanjši tak c je 21. Eno od rešitev (x_0, y_0) dobimo iz predzadnje vrstice razširjenega Evklidovega algoritma. Torej $(x_0, y_0) = (1, -1)$. Vse rešitve pa so oblike

$$\left(x_0 + k \cdot \frac{84}{21}, y_0 - k \cdot \frac{63}{21}\right) = (1 + 4k, -1 - 3k),$$

kjer je $k \in \mathbb{Z}$.

Rešitev naloge 48.

a. Največji skupni delitelj parametrov a in b mora deliti c.

b. Ustrezen je vsak b, za katerega velja, da največji skupen delitelj števil 35 in b deli 21. Npr. $1, 7, 14, 21, \ldots$

Rešitev naloge 49.

a. Definicijsko območje in zaloga vrednosti sta $\{1, 2, 3, 4, 5, 6\}$.

b. $\pi = (1, 4, 6)(2, 5)$. Red je najmanjši skupni večkratnik dolžin ciklov, tj. 6.

c. $\pi = (1, 6)(1, 4)(2, 5)$. Parnost pemutacije π je liha.

d. $\pi * \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 3 & 4 & 1 \end{pmatrix}.$

Rešitev naloge 50.

a. Ker je $a|b \cdot c$ in $D(a,b) = 1$, sledi $a|c$. Torej je $D(a,c) = a$.

b. Ne. Ker so a, b, k, ℓ pozitivna cela števila, je $ka + \ell b \geq 1 \cdot 1 + 1 \cdot 1 = 2 > 1$.

c. $\alpha = (1234)(5678)(9)$.

d. Ciklična struktura π je $[8, 1]$. Torej je $\pi = (15263748)(9)$.

Rešitev naloge 51.

a. Ker je $b|c \cdot d$ in $D(b,d) = 1$, sledi $b|c$. Torej je $D(b,c) = b$.

b. Ne. Ker sta a, b pozitivni celi števili, k, ℓ pa negativni celi števila, je $ka + \ell b \leq (-1) \cdot 1 + (-1) \cdot 1 = -2 < -1$.

c. $\alpha = (123)(456)(7)$.

d. Ciklična struktura π je $[6, 1]$. Torej je $\pi = (142536)(7)$.

Rešitev naloge 52.

a. Primeri so pari $(a, b) \in \{(2, 20), (4, 10), (10, 4), (20, 2)\}$.

b. Primer je npr. $\alpha = (123)(45)$. Edina možna ciklična struktura je $\mathcal{C}(\alpha) = [3, 2]$.

Rešitev naloge 53.

a. Primeri so pari $(a, b) \in \{(2, 12), (4, 6), (6, 4), (12, 2)\}$.

b. Primer je npr. $\alpha = (123)(45)(6)$. Edina možna ciklična struktura je $\mathcal{C}(\alpha) = [3, 2, 1]$.

Rešitev naloge 54.

a. Ker $\gcd(a, b) = 2$ deli 2022, je enačba rešljiva nad $\mathbb{Z}$, rešitev pa je neskončno mnogo.

b. Taki naravni števili a, b ne obstajata, saj bi moral $\gcd(a, b)$ deliti $\operatorname{lcm}(a, b)$.

c. Velja $\varphi^2 = (57)(46)(123)$. Zato je $\mathcal{C}(\varphi^2) = [3, 2, 2]$. Sledi $\mathcal{C}(\varphi) = [4, 3]$. Dve rešitvi sta $\varphi = (5476)(132)$ in $\varphi = (5674)(132)$.

Rešitev naloge 55.
Da bo imela enačba $4x + by = 20$ celoštevilske rešitve, mora $\gcd(4, b)$ deliti 20. Da enačba $4x + 20y = b$ ne bo imela celoštevilskih rešitev, pa $4 = \gcd(4, 20)$ ne sme deliti b. Primeri so $b = 1$, $b = 2$, $b = 6$, ...

Rešitev naloge 56.

Velja $\varphi^2(i) = \varphi(\varphi(i)) = i$. Vstavimo zaporedoma $i = 1, 4, 7$:

$$1 = \varphi^2(1) = \varphi(\varphi(1)) = \varphi(3) = y,$$
$$4 = \varphi^2(4) = \varphi(\varphi(4)) = \varphi(2) = x,$$
$$7 = \varphi^2(7) = \varphi(\varphi(7)) = \varphi(5) = z.$$

Ker je φ permutacija, imamo za $\varphi(6)$ samo eno možnost, tj. $6 = w$.