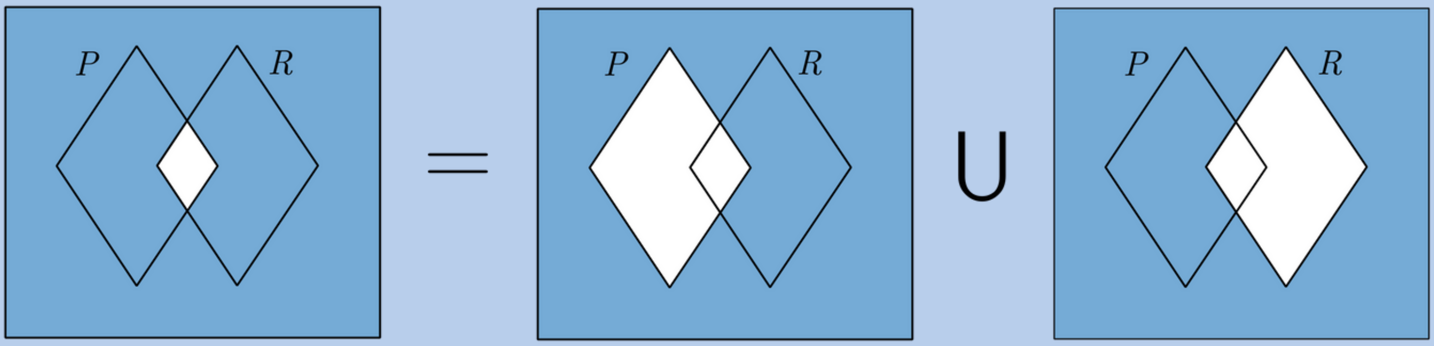
FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA
I INFORMACIJSKIH TEHNOLOGIJA OSIJEK

Sveučilište Josipa Jurja Strossmayera u Osijeku

30+30
Diskretna matematika



$$\neg(P \wedge R) \quad \Leftrightarrow \quad \neg P \quad \vee \quad \neg R$$

TOMISLAV RUDEC ANJA ŠTEKO

Izdavač
Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek

Za izdavača
prof. dr. sc. Tomislav Matić

Autori
doc. dr. sc. Tomislav Rudec
Anja Šteko, asistent

Recenzenti
doc. dr. sc. Anita Katić
Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek
izv. prof. dr. sc. Tomislav Marošević
Sveučilište Josipa Jurja Strossmayera u Osijeku
Odjel za matematiku

Lektor
doc. dr. sc. Dragana Božić Lenard
Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek

Siječanj, 2023. godine

ISBN: 978-953-8184-06-2

Sveučilište Josipa Jurja Strossmayera u Osijeku

Suglasnost za izdavanje ovog sveučilišnog udžbenika donio je Senat Sveučilište Josipa Jurja Strossmayera u Osijeku na 1. sjednici u akademskoj godini 2022./2023. održanoj 27. listopada 2022. godine pod brojem 26/22.

Sveučilište J. J. Strossmayera u Osijeku
Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek

Tomislav Rudec | **Anja Šteko**

30 + 30

Diskretna matematika

Osijek, 2023.

Sadržaj

Uvod **1**

1 Matematička logika **3**

1.1. Uvod u logiku. Tradicionalna logika. Kategorički silogizam. 3

1.2. Logika sudova. Tablice istinitosti. Modeliranje formulama logike sudova. . 14

1.3. Konjunktivna i disjunktivna normalna forma. Odnosi među veznicima . . . 38

1.4. Sudovne jednadžbe 46

1.5. Prirodna dedukcija 52

1.6. Logika prvog reda 61

2 Teorija skupova **75**

2.1. Skupovi i operacije sa skupovima 75

2.2. Vennovi dijagrami. Jednakost skupova. 83

2.3. Relacije 96

2.4. Kardinalni brojevi 115

3 Teorija brojeva **127**

3.1. Djeljivost. Prosti brojevi. 127

3.2. Djeljivost u zadacima s matematičkih natjecanja 148

3.3. Kongruencije 157

3.4. Eulerov teorem i mali Fermatov teorem 168

3.5. Diofantske jednadžbe 173

4 Logički zadaci kombinatorne i diskretne matematike **187**

4.1. Primirje na šahovskoj ploči 187

4.2. Rekurzivne logičke zagonetke 193

4.3. Rasvjeta 198
4.4. Neboderi 207
4.5. Mostovi 215
4.6. Kakuro 223
4.7. Integram 231
4.8. Sudoku 243
4.9. Što mogu 1, 2, 3, 4 i 5? 252
4.10. Logička ispunjaljka 255

Prilozi **269**

Prilog 1: Prijedlog izvedbe kolegija po nastavnim satima 269

Kazalo **277**

UVOD

Riječ "diskretno" u ovom kontekstu znači odvojeno, s udaljenosti, ili suprotno od neprekidno. Realni brojevi čine neprekidan, gust skup, bez "praznina" na pravcu, a prirodni (ili cijeli brojevi) čine na pravcu diskretan skup, tj. takav da se oko svake njegove točke može opisati okolina koja ne sadrži više niti jednu od ostalih točaka tog skupa.

Riječ matematika dolazi iz starogrčkog jezika i u izvorniku otprilike znači znanost ili "ono što se uči".

Diskretna matematika dio je matematike koji se bavi sljedećim disciplinama: matematička logika, teorija skupova, teorija brojeva, teorija grafova, teorija algoritama i najčešće dijelovi kombinatorike (osnove kombinatorike).

Knjiga je namijenjena studentima "nematematičkih" fakulteta (onima koji nisu na odjelima ili odsjecima za matematiku te nisu u studijskom programu imali matematičku logiku, teoriju skupova i slično). Cilj joj je prikazati način razmišljanja matematike i logike te odmah pokazati upotrebu i važnost takvog načina razmišljanja u rješavanju konkretnih zadataka i u konstrukcijama osnovnih matematičkih objekata.

Prva cjelina *Matematička logika* ima za cilj uvesti studente u područje koje je na granici logike, tj. teorija poimanja (shvaćanja) i razmišljanja s jedne strane i matematike i računalstva s druge. Prva dva potpoglavlja svakako treba temeljito obraditi.

Druga cjelina *Logika sudova* ima za zadatak dati studentima osjećaj što je to skup, kako se prelazi sa skupa na relaciju, pa na funkciju, pa na broj te podučiti studente osnovnim operacijama sa skupovima i relacijama. Na kraju, objašnjeno je na jednostavan način strogo matematičko zasnivanje pojma broja, zbrajanja i množenja.

Treća cjelina nakon proučavanja djeljivosti i ostatka pri dijeljenju te nakon korištenja tih znanja u rješavanju zadataka s matematičkih natjecanja ulazi dublje u strukturu i poimanje odnosa među prirodnim brojevima. Objašnjen je pojam kongruentnosti i na zadacima su primijenjeni Eulerov teorem i mali Fermatov teorem. Na kraju su dani primjeri linearnih i nelinearnih diofanstkih jednadžbi te neke metode rješavanja navedenih jednadžbi.

Cilj je četvrtog poglavlja prezentirati popularnije logičke zadatke u čijem se rješavanju koriste razne metode kombinatorike i diskretne matematike. Čitatelje pozivamo da za navedene zadatke pokušaju kreirati računalni program koji će riješiti zadanu instancu problema.

Zadnje je poglavlje, koje se odnosi na logičke zadatke, navedeno u knjizi jer vjerujemo kako nakon osnovne i srednje škole te nekih, do ovog kolegija već odslušanih fakultetskih matematika (koje su često "tehničke prirode"), student treba upoznati dio matematike koji pripada pod zanimljivu matematiku. Inače bi sve bilo kao u glazbenom odgoju u kojem poučavamo učenike samo notama, a učenici nikada ne zapjevaju. U svakom bi bloku od dva sata vježbi trebalo predstaviti probleme koji su na granici logike, kombinatorike ili teorije grafova. Primjeri takvih problema mogu se naći u zadnjem paragrafu ovog udžbenika. Logički problemi dio su "esencijalnosti" matematike, tj. čisto (apstraktno) razmišljanje koje matematiku čini kraljicom znanosti. Za matematiku, koja je skup formula koje će primijeniti statističar, menadžer ili bankar, ne vjerujemo kako je kraljica znanosti, nego sluškinja navedenih područja.

U knjizi se nalazi više gradiva nego što se može ispredavati i obraditi na dvama predavanjima i vježbama tijekom jednog semestra. Nastavnik će odabrati gradiva koja će obraditi kao i dubinu u koju će ući u pojedinoj cjelini. Svakako treba obraditi cjeline 1.1., 1.2., prvi dio 1.3., 2.1., 2.2., 2.3., 3.1., 3.2., 3.3., 3.4. te gradiva *Što mogu 1, 2, 3, 4 i 5?* i *Sudoku*.

1

Matematička logika

1.1. Uvod u logiku. Tradicionalna logika. Kategorički silogizam.

Uvod

Cilj je potpoglavlja 1.1. dati studentima osnovna znanja iz tradicionalne logike (neki studenti u srednjoj školi nisu slušali taj predmet, a ostali će ponoviti osnovno, a nešto i nadograditi). Osim općeg znanja o elementima tradicionalne logike, studenti bi trebali usvojiti i osjećaj za formalno razmišljanje.

Konkretno, čitatelj bi trebao shvatiti što su pojam, sud, zaključak, induktivni zaključak, deduktivni zaključak, definicija te kategorički silogizam i trebao bi znati koristiti i rješavati kategorički silogizam.

Ovo gradivo šire je opisano u sljedećim udžbenicima za srednje škole:

1. M. Jakić, *Logika*, Školska knjiga, Zagreb, 2007.
2. S. Kovač, *Logika za gimnazije,* HSN, Zagreb, 2010.
3. I. Macan, *Uvod u tradicionalnu logiku*, `https://www.filozofija.org/wp-content/uploads/knjige/Uvod-u-tradicionalnu-logiku-3.pdf` (zadnji pristup travanj 2022.).
4. G. Petrović, *Logika*, Element, Zagreb, 2015.

Nastanak i osnove logike

Perilica posuđa gotova je s radom. Iz perilice vadimo i na njihovo mjesto slažemo duboke tanjure, plitke tanjure, tanjuriće za kolače, noževe, itd. kako bi nam svi bili "pri ruci", kako bismo znali gdje se točno nalaze te, osim praktičnosti, zato što nam onda u kuhinjskim elementima to izgleda lijepo i uredno. Odjeća je također sortirana i raspodijeljena na svoja mjesta na sličan način. Uredno i funkcionalno. Učeći neki fakultetski ili školski predmet pišemo u više stupaca naslove ili pojmove koje učimo kako bi nam cijeli kolegij bio pregledniji. Biljni i životinjski svijet slažemo po rodovima, vrstama itd. Sustavno, pregledno i praktično slažemo stvari, bića i pojave kako bi nam bile što jednostavnije za korištenje (ali i što ljepše jer i kada ih ne koristimo, izgleda nam dobro kada su na takav način posložene).

Logika (grčki logos – govor, riječ) je pokušaj da sve to napravimo za misli, zaključke, riječi i rečenice i ostale misaone procese. Zadatak je logike sve to analizirati, grupirati te uredno složiti na način da što jednostavnije možemo njima rukovati kad nam i na koji nam način trebaju.

Počeci logičkog izražavanja, to jest upotrebe logike, nalaze se u starogrčkim razgovorima i raspravama u kojima jedan govornik pokušava opovrgnuti teze drugoga, ali i posebno strukturiranim rečenicama koje sliče na zaključke i dokaze. Kako bi se dokazi i zaključci, opovrgavanja i pobijanja mogli sustavno provesti, u staroj je Grčkoj uočeno kako treba proučavati i strukturu samog jezika, riječi i rečenica te gramatiku. Aristotel (384. godine pr. Kr. – 322. godine pr. Kr.) se smatra začetnikom logike. Povijesni razvoj logike dobro je opisan u gore navedenim udžbenicima.

Po definiciji, logika je znanost koja se bavi raznim oblicima ispravnog "razmišljanja".

Logiku, dakle, ne zanima sadržaj, nego oblik misli. Logiku ne zanima je li rečenica "Niti jedan student nije prevarant." točna (time se bave etika, psihologija, statistika i tako dalje). Logiku zanima povlače li sudovi: "Svi su studenti mladi." i "Niti jedna mlada osoba nije prevarant." kao zaključak sud "Niti jedan student nije prevarant.". Logika sada (a ne etika) odgovara: da, ovaj je zaključak ispravan ili valjan ili istinosan. Logika formu ovih sudova zapisuje kao matematika, simbolički, u obliku

Svi S su M.
Niti jedan M nije P.
Dakle, iz gore spomenutih dvaju sudova zaključujemo: "Niti jedan S nije P."

Pojam

Elementarni dio rečenice, u logici, jest pojam. Pojmovi su npr. lopta, živa bića, proljeće, pravokutnik čije su stranice duge $3\,cm$ i $5\,cm$, dakle riječ ili više riječi koje se odnose na "jednu stvar".

Pojam neki autori definiraju kao misao o onom o čemu mislimo, a drugi kao skup svih karakteristika onoga o čemu mislimo. U oba je slučaja definicija zanimljiva, i diskutabilne korisnosti, no nedvosmisleno kaže kako je npr. "brod", pojam "broda", misao koju dobijemo kad tu riječ kažemo ili čujemo ili kad o njoj razmišljamo, odnosno ono što tada zamislimo. Svaki od navedenih srednjoškolskih udžbenika (pre)detaljno navodi podjele pojmova, vrste pojmova, odnose pojmova itd. Na primjer, "jednakostranični pravokutnik" i "kvadrat" su identični ili istovjetni jer govore o istom pojmu. Šuma je kolektivan pojam. Pojmovi "ljekovita biljka" i "kamilica" su različiti po sadržaju i po opsegu. Postoje viši i niži pojmovi. Svi pojmovi imaju opseg, doseg, sadržaj itd.

Sud

Sud je rečenica kojom se nešto tvrdi i koja je ili istinita ili neistinita.
Tako rečenica "Koliko je sati?", kao i bilo koja druga upitna rečenica, nije sud. Kod odlučivanja koja je rečenica sud, a koja ne, važna je (i možda prejaka) obavezna karakteristika suda po kojoj on mora biti ili istinit ili ne. Je li rečenica "Danas je lijep dan." sud ili ne? Postoji li tablica u kojoj su nabrojane temperature, klima ili pojave u danu koje će ga deklarirati kao lijepog ili ružnog? Nakon nešto razmišljanja uviđamo kako gotovo niti jednoj rečenici ne možemo lako dati svojstvo: "istinita je" ili "nije istinita". Čak i jednostavna rečenica tipa "Torta ima više kalorija od jednog kolača." ne mora biti istinita, ali i može.

Sudovi se također klasificiraju, analiziraju i dijele na mnoge načine (ove su podjele uglavnom Aristotelove).
Tradicionalna je podjela sudova po:

a) kvantiteti ili kolikoći na sudove koji su
   - opći ili univerzalni (Svi studenti su mladi.);
   - posebni ili partikularni (Neki auti ne troše puno.);
   - pojedinačni ili singularni (Merkur je blizu Sunca.).

b) kvaliteti ili kakvoći na sudove koji su
   - potvrdni ili afirmativni (Svi studenti su mladi.);
   - niječni ili negativni (Neki auti ne troše puno.);
   - beskonačni ili limitativni (Svi nastavnici su neobični.).

c) relaciji na sudove koji su
  - kategorički (1+1=2.);
  - hipotetički (Ako ne ugasiš mobitel, razbit ću ga.);
  - disjunktivni (Ili je danas petak ili je četvrtak.).

d) modalitetu na sudove koji su
  - problematični (govore kako nešto možda jest, a možda i nije) (Sad smo možda zakasnili.);
  - asertoni (govore kako nešto jest) (Podjele sudova su zanimljive.);
  - apodiktički (govore kako nešto mora biti) (Ako je $x < -2$, mora biti $x^2 > 4$.).

Ovo su samo neke od mnogih podjela.

Važan i zanimljiv sud jest definicija. Treba, naime, opisati neki pojam pomoću višeg pojma (čiji je on hiponim) i pomoću vrsne razlike (po čemu se razlikuje od ostalih pojmova koji također spadaju pod isti viši pojam). Primjerice:

Definicija: Čaj je piće koje dobijemo tako što u vruću vodu stavimo (najčešće) osušene biljke.
Definiramo čaj. Čaj spada pod pića (viši rodni pojam). Od svih drugih pića, čaj se razlikuje po tome što se pripravlja tako što u vruću vodu stavimo (najčešće) osušene biljke (vrsna razlika).

Definicija: Pravokutni trokut je raznostraničan trokut koji ima bar jedan pravi kut. (Naravno, mogli smo ga odrediti i kao "trokut koji ima jedan pravi kut.")
Definiramo pravokutni trokut. On spada pod trokute (viši rodni pojam). Od svih drugih trokuta, razlikuje se po tome što ima pravi kut (vrsna razlika).

Evo nekoliko loših definicija:
Definicija (loša) 1. Komarac je kukac koji može piti krv. *(Ne valja jer to su i krpelji itd.)*
Definicija (loša) 2. Limun je voće od kojeg se pravi limunada. Limunada je piće koje se pravi od limuna. *(Ne valja jer stvar A definiramo pomoću stvari B, a onda B pomoću A.)*
Definicija (loša) 3. Pravokutni trokut je geometrijski lik koji ima pravi kut. *(Ne valja jer smo uzeli predalek viši rod. Ovako je i pravokutnik također trokut.)*

Zaključak

Sud koji logički slijedi iz nekih drugih zadanih sudova zovemo zaključak.

Sudovi od kojih polazimo zovu se premise, a konačni sud kojeg dobivamo iz njih, konačni zaključak, zove se još i konkluzija.

Kod zaključivanja nam je važno da od istinitih premisa dobijemo istinit zaključak. Ili: zaključivanje nije valjano samo ako iz istinitih premisa dobijemo lažan zaključak.

Primjer 1.1.1.
Crvena boja je slična ljubičastoj boji.
Ljubičasta boja je slična plavoj boji.
Zaključak: Crvena je boja slična plavoj boji.

Jasno je kako ovaj zaključak nije valjan jer smo od "istinitih" premisa dobili lažnu izjavu (relacija "biti sličan" nije tranzitivna).

Ali sljedeći zaključak jest:

Svi studenti puno sjede.
Svi koji puno sjede su ljenčine.
Zaključak: Svi studenti su ljenčine.

Ovaj je zaključak valjan, bez obzira što (neki) njegovi dijelovi nisu istinite izjave.

I zaključci imaju svoje podjele, odnose, kategorizacije itd., slično kao pojmovi i sudovi. Najpoznatija podjela zaključaka jest podjela na induktivne i deduktivne zaključke.

U induktivnom zaključku (koji često nije točan) polazimo od pojedinačnih primjera iz kojih zaključujemo o cijeloj populaciji.

Primjer 1.1.2. 1 je veći od nula, 2 je veći od nula, 3 je veći od nula. Zaključujemo da je svaki prirodni broj veći od nula. (Točno, premda smo zaključili samo na osnovu triju primjeraka.)

Primjer 1.1.3. Ušavši u neku stranu državu primjećujemo kako je prva osoba plavokosa, druga i treća također, itd. Zaključujemo: "Sve osobe u ovoj zemlji su plavokose." Radi se o klasičnoj grešci kad na osnovu "nekih" zaključimo o "svima". U stvari je induktivno zaključivanje najčešći oblik zaključivanja jer čovjek može o onome što nije vidio zaključiti samo na osnovu onoga što je vidio, a čovjekovo iskustvo je konačno. "Kava mi ne odgovara." kažemo na osnovu dviju ili triju popijenih kava. Daljnji primjeri su: "Svi Škoti su škrti.", "Svi Nijemci su pedantni.", "Svi induktivni zaključci su pogrešni.", "Sve prethodne rečenice su lažne.".

Prema nekim autorima, induktivni zaključak je onaj u kojem na osnovu analize baš svakog pojedinog pripadnika nekog skupa ili klase zaključimo kako neko svojstvo vrijedi za sve pripadnike tog skupa ili klase.

Deduktivni zaključak je zaključak koji je uvijek ispravan jer koristi činjenicu da ako nešto vrijedi za sve pripadnike nekog skupa, onda vrijedi i za nekog određenog, pojedinačnog pripadnika tog istog skupa. Matematika koristi samo deduktivne zaključke, ali ih najčešće ne napominje posebno jer se podrazumijevaju. Ako je zbroj kutova u svakom trokutu 180 stupnjeva, to jednostavno koristimo kao jedan od koraka u rješavanju zadatka ili dokazivanju nekog teorema za zadani, konkretni trokut.

Najpoznatiji zaključak u literaturi o tradicionalnoj logici jest kategorički silogizam. Silogizam je zaključak u kojem na osnovu dviju premisa (ili više njih) donosimo jednu konkluziju.

Sudove u kategoričkom silogizmu najčešće uzimamo kao kombinaciju afirmativnih, negativnih, partikularnih i univerzalnih sudova koji su uz to i kategorički.

Uz oznake:

S a P - svi S su P (S kao subjekt i P kao predikat)

S e P - nijedan S nije P

S i P - neki S su P

S o P - neki S nisu P

pokušavamo iz dvaju sudova, koji su nekog od gore navedenih oblika, dobiti treći koji je također tog oblika. Nekada iz zadanih dvaju sudova možemo dobiti više rješenja, nekada postoji samo jedno rješenje nekog od tih oblika, a nekada niti jedno navedenog oblika.

U prvom su sudu tradicionalno oznake M i P, u drugom M i S, a treći je oblika S x P, gdje je x ili slovo a, e, i ili o.
M je oznaka za medijalni, srednji ili raspodijeljeni pojam.

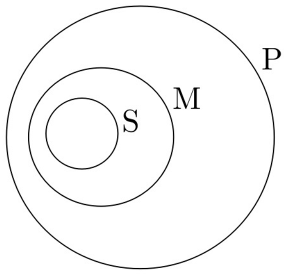
Primjer 1.1.4.

$$\begin{array}{c} \text{M a P} \\ \text{S a M} \\ \hline ? \end{array}$$

M a P znači svi M su P (npr. Svi kukci imaju šest nogu.).
S a M znači svi S su M (npr. Svi komarci su kukci.).

Ovo nije teško. Ako su svi komarci kukci, a svi kukci imaju šest nogu, mora slijediti da svi komarci imaju šest nogu. Svi S su P.
S a P je konačni zaključak.

Pri rješavanju kategoričkih silogizama mogu nam pomoći pomoćni sudovi ili pojmovi, kao gore komarci i kukci. Mogu nam pomoći i slike, pri čemu su sljedeći sudovi označeni pripadnom slikom (Slika 1.1.1)



Slika 1.1.1: Odnos sudova M, P i S.

Primjer 1.1.5. Riješi kategoričke silogizme (ne zaboravimo kako je zaključivanje ispravno ako iz istinitih premisa dobivamo istinit zaključak).

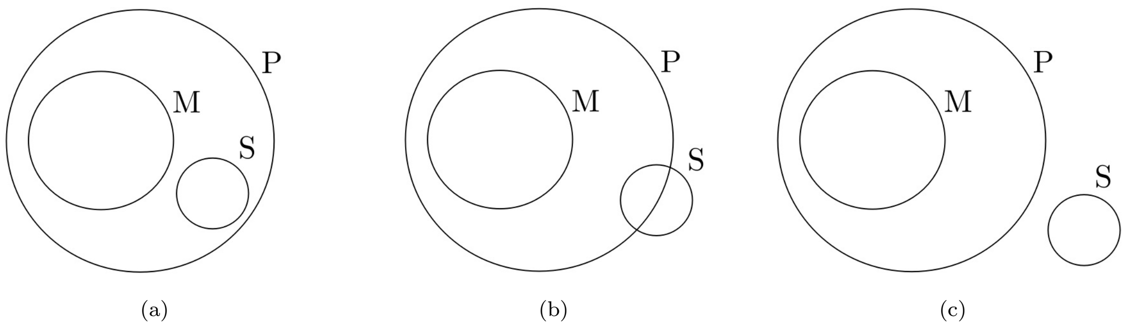
a)

$$\begin{array}{c} \text{M a P} \\ \text{S e M} \\ \hline ? \end{array}$$

Rješenje. Pokušajmo si pomoći konkretnim istinitim rečenicama.

Svi Kinezi su ljudi.
Nijedan indijanac nije Kinez.

Potrebno je zaključiti rečenicu koja se sastoji od “indijanac” i “čovjek”.



Slika 1.1.2: Mogući odnosi sudova M, P i S

Pokušajmo si pomoći i slikom 1.1.2. Na slici smo postavili sve moguće odnose jer ne znamo u kojem su odnosu S i P. Možda imaju presjek, a možda ne. Samo znamo kako su S i M disjunktni (nemaju presjek).

Prođimo u ovom prvom zadatku redom sve mogućnosti.

Je li ovdje sigurno S a P, tj. možemo li sa sigurnošću reći "Svi indijanci su ljudi." ili da je cijeli S na slici u skupu P? Iz slike 1.1.2 b) i 1.1.2 c) vidimo da S a P nije istina. Premda, svi indijanci jesu ljudi. Možda nas zbunjuje činjenica da svi indijanci jesu ljudi jer smo u primjeru uzeli Kineze i indijance koji svi odreda spadaju u ljude. No, ako uzmemo za primjer

Svi Kinezi su ljudi.
Nijedna olovka nije Kinez.

jasno je da S a P ne vrijedi. Dakle, S a P ne vrijedi u svakom slučaju.

Je li ovdje sigurno S e P, tj. možemo li sa sigurnošću reći "Niti jedan indijanac nije čovjek." ili da je cijeli S na slici izvan skupa P? Naravno da ne. I slika i naš primjer dokaz su da S e P ne vrijedi općenito.

Je li ovdje sigurno S i P, tj. možemo li sa sigurnošću reći "Neki indijanci su ljudi" ili da je sigurno bar jedan dio od S na slici u skupu P? Ako nacrtamo S izvan P, vidimo da S i P nije istina. Premda, neki indijanci jesu ljudi. Zbunjuje činjenica da neki indijanci jesu ljudi jer smo u primjeru uzeli Kineze i indijance koji svi odreda spadaju u ljude. Ako uzmemo

Svi Kinezi su ljudi.
Nijedna olovka nije Kinez.

jasno je da S i P ne vrijedi. Dakle, S i P neće vrijediti uvijek.

Je li ovdje sigurno S o P, tj. možemo li sa sigurnošću reći "Nijedan indijanac nije čovjek" ili da je cijeli S na slici izvan skupa P? Naravno da ne. Dakle, ne vrijedi ni S o P.

Zaključak i konačno rješenje: iz M a P i S e M ne može se zaključiti ništa što bi sigurno bilo istina (bez obzira što bili S, M i P) o odnosu suda S i suda P.

b)

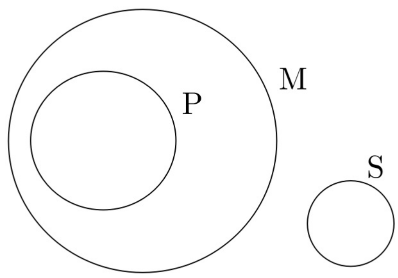
$$\begin{array}{c} \text{P a M} \\ \text{M e S} \\ \hline ? \end{array}$$

Rješenje. Pokušajmo ponovno s konkretnim istinitim rečenicama.

Svi psi su živa bića.
Nijedno živo biće nije četvrtak.

Potrebno je zaključiti rečenicu koja se sastoji od "četvrtak" i "pas".

Predstavimo li situaciju slikom, dobivamo:



Slika 1.1.3: Odnos sudova M, P i S.

Je li ovdje sigurno S a P, tj. možemo li sa sigurnošću reći "Svaki četvrtak je pas." ili može li se reći da je cijeli S na slici u skupu P? Ne, jer tada bi S a P morao biti točan što god bilo S i P, a jasno je da "Svaki četvrtak je pas." ne vrijedi. Dakle, S a P ne vrijedi u svakom slučaju.

Je li ovdje sigurno S e P, tj. možemo li sa sigurnošću reći "Niti jedan četvrtak nije pas." ili da je cijeli S na slici izvan skupa P? Odgovor je da.
Iz slike 1.1.3 vidi se da S i M ne smiju imati zajedničkih točaka, pa onda svakako ne smiju zajedničkih točaka imati niti sud S i sud P jer je P unutar M. S druge strane, ako su svi psi živa bića, onda što god uzeli u drugoj rečenici, što je nevezano uz živa bića, bit će to nevezano i uz pse. Bit će S e P.

Je li ovdje sigurno S i P, tj. možemo li sa sigurnošću reći "Neki četvrtak je pas"? Naravno da ne. S i P neće vrijediti uvijek jer ne vrijede već za naš primjer.

Je li ovdje sigurno S o P, tj. možemo li sa sigurnošću reći "Neki četvrtci nisu psi."? Da, jer niti jedan četvrtak nije pas i na slici se vidi kako niti jedan S nije P pa onda naravno vrijedi da neki S nisu P. Uočavamo: kad god vrijedi S e P, vrijedit će i S o P. (Isto tako, kad god vrijedi S a P, vrijedit će i S i P.) No, S e P je jača tvrdnja od S o P. (Ako netko kaže “Pero ne zna plivati” i netko doda “Nitko iz njegove obitelji ne zna plivati”, jasno je da je druga tvrdnja jača, jer daje puno više informacija nego prva, a i prva odmah slijedi iz druge.)

Zaključak i konačno rješenje: iz P a M i M e S odmah slijedi S e P. (Još jednom, slijedi i S o P, ali bolje je i korisnije imati S e P. Ako nas netko pita koliko je $2+4$, možemo mu odgovoriti “Rezultat je neki paran broj.” i to je istina, ali bolji odgovor je 6.)

$$\begin{array}{c} \text{P a M} \\ \text{M e S} \\ \hline \text{S e P} \end{array}$$

ZADACI ZA VJEŽBU

Zadatak 1.1.1. Riješi kategoričke silogizme:

a)

$$\begin{array}{c} \text{M e P} \\ \text{S i M} \\ \hline \text{S} \quad \text{P} \end{array}$$

b)

$$\begin{array}{c} \text{P a M} \\ \text{S o M} \\ \hline \text{S} \quad \text{P} \end{array}$$

c)

$$\begin{array}{c} \text{M e P} \\ \text{M a S} \\ \hline \text{S} \quad \text{P} \end{array}$$

d)

$$\begin{array}{c} P \ \ i \ \ M \\ M \ \ a \ \ S \\ \hline S \qquad P \end{array}$$

e)

$$\begin{array}{c} P \ \ a \ \ M \\ M \ \ o \ \ S \\ \hline S \qquad P \end{array}$$

Rješenja

1.1.1. a)

$$\begin{array}{c} M \ \ e \ \ P \\ S \ \ i \ \ M \\ \hline S \ \ o \ \ P \end{array}$$

b)

$$\begin{array}{c} P \ \ a \ \ M \\ S \ \ o \ \ M \\ \hline S \ \ o \ \ P \end{array}$$

c)

$$\begin{array}{c} M \ \ e \ \ P \\ M \ \ a \ \ S \\ \hline S \ \ o \ \ P \end{array}$$

d)

$$\begin{array}{c} P \ \ i \ \ M \\ M \ \ a \ \ S \\ \hline S \ \ i \ \ P \end{array}$$

e)

$$\begin{array}{ccc} P & a & M \\ M & o & S \\ \hline S & - & P \end{array}$$

Tj., zadatak e) nema rješenja.

1.2. Logika sudova. Tablice istinitosti. Modeliranje formulama logike sudova.

Uvod

Cilj je potpoglavlja 1.2. predstaviti matematičku logiku preko logike sudova – davanjem njenog alfabeta, formula, interpretacije tih formula te modeliranjem svakodnevnih zaključaka formulama logike sudova.

Nakon usvojenog potpoglavlja 1.2. čitatelj će

- znati što je logika sudova, alfabet logike sudova, što je riječ i formula;
- znati konstruirati riječi i formule,
- razumjeti na što se odnosi sintaksa, a na što semantika formula logike sudova (ili neke druge logike);
- znati interpretirati varijable i odrediti vrijednost formule (tj. interpretirati formulu) u odnosu na vrijednosti (tj. u odnosu na interpretacije) njenih varijabli;
- razumjeti što znači da neka formula logički slijedi iz druge ili da su dvije formule logički ekvivalentne;
- koristeći gore navedena znanja konstruirati logičke modele za rečenice ili zaključivanja iz svakodnevnog života i pomoću tih modela dublje analizirati ili bolje shvatiti značenje tih rečenica ili zaključivanja.

Literatura za 1.2. sljedeće su knjige i skripte:

1. R. Cori, D. Lascar, *Mathematical logic: a course with exercises (Part I)*, Oxford University Press, 2000.

2. M. Vuković, *Matematička logika*, Element, Zagreb, 2009.

3. M. Vuković, *Matematička logika 1*, skripta.
http://www.mathos.unios.hr/logika/Logika_skripta.pdf (zadnji pristup travanj 2022.)

Zadatak je matematičke logike matematici biti sigurna baza za rad s "formalnim" (npr. oblika $\forall x > 0\ \exists y : y = x^2$) izjavama, tj. sudovima te joj pomoći u zadacima odlučivanja kada je što istina ili ne, što iz čega slijedi i slično. Nastala je (krajem 19. stoljeća) kao pomoć matematici, za njeno formalno zasnivanje, a poslije (s počecima u tridesetim i četrdesetim godinama 20. stoljeća) pomogla je u postavljanju formalne baze računarstvu.

Razne logike mogu se pohvaliti karakteristikom vjerodostojnosti jer ne rade s konkretnim, opipljivim svijetom, nego su one potpuno teoretske, formalne teorije. U logici se radi samo sa simbolima, operacijama za koje su postavljena strogo određena pravila. Nema mjesta za polemiziranje (ako je $A = 1$, a $B = 0$, onda je $A \vee B = 1$ i to je dogovor i to je tako što god zamijenili za A i B u pojedinoj situaciji u kojoj će se koristiti ovaj izraz).

Matematička logika daje popis simbola (alfabet), zatim način na koji simboli tvore riječi ili formule i na kraju način na koji se simboli iz formula mogu interpretirati (npr. nulama ili jedinicama). A kada je cijela ta konstrukcija gotova, i kada znamo koja je formula istinita, a koja lažna, matematika ili računalstvo ili neka druga disciplina uočavaju: Varijable ove (vrste) logike bile bi pogodne za interpretaciju simbola naše (konkretne) teorije, gdje bi 0 mogla značiti lažnu izjavu, žicu kroz koju ne prolazi struja ili lažnu rečenicu, a jedinica suprotno. Veznik "ili" propozicionalne logike mogao bi dalje značiti određeni način povezivanja objekata, itd.

Ipak, nije sigurnost i istinitost jedino što logika daje računalstvu, jeziku ili tehnici. Druga dobra karakteristika logike je u tome što je svoje operacije pojedina logika zasnovala ipak na realnom svijetu u koji će se ona kasnije "uroniti", pa su i njene funkcije i relacije odmah dobra vodilja novim realnim, "opipljivijim" odnosima u konkretnoj promatranoj teoriji. (Npr. veznik "ili", tj. $\vee$ logike sudova dogovorno je takav da mu je vrijednost postavljena za "laž" samo ako su njegove obje varijable "laž", kako bi se uklopio u svakodnevno korištenje riječi "ili".)

Više je vrsta logika, a kreirane su najčešće kao alat konkretnim područjima znanosti ili tehnike kojima daju strogost, istinitost i ideje za dalji razvitak (npr. što se još može u teoriji osmisliti na osnovu onoga što logika daje kao svoju tautologiju i slično).

Logika sudova ili propozicionalna logika koristi varijable (velika slova), veznike i zagrade. Logika prvog reda ili predikatna logika sadrži sve što i logika sudova, i nasljeđuje sva njena pravila, ali sadrži i kvantifikatore $\forall$ i $\exists$ te funkcije, konstante i relacije.

Modalna logika ima i operatore oblika "možda" ($\Diamond$) i "sigurno" ($\Box$) .

Fuzzy logika, za razliku od gore navedenih logika, dozvoljava, osim 0 i 1, i bilo koju drugu vrijednost za svoje varijable. Dobar je model za teorije u kojima je vjerojatnost pripadnosti nekom skupu broj iz intervala $[0,1]$ (tu je u neku ruku fuzzy logika u suprotnosti s Booleovim logikama u kojima varijable mogu biti samo 0 ili 1).

Svaka logika razvija odnose među svojim simbolima. Ostalim područjima ljudskog djelovanja zadatak je pronaći pravu vrstu logike i koristiti sve njene zakonitosti i promatrati dvostuku relaciju: kako u određenoj teoriji koja se oslanja na logiku tumačiti pojedinu formulu logike, tj. što logika dodatno donosi teoriji, i drugo, kako pojedini rezultat teorije izgleda u odabranoj logici.

Često nije jasno hoće li odabrana logika biti dobra za neku teoriju. Stoga je najčešća pojava da prvo imamo konkretan "životni" zadatak ili zadani sustav, a onda na osnovu njega kreiramo logiku koja bi tom problemu mogla pomoći.

Logika sudova zove se još i propozicionalna logika ili račun sudova ili logika nultog reda (u stranoj literaturi također je više izraza, npr. *propositional logic*, *statement logic*, *sentential calculus*, *sentential logic*, 0*-th order logic*).

Započnimo sa sintaksom logike sudova.

Alfabet logike sudova je skup

$$\mathcal{A} = \{(,\ ), \land, \lor, \to, \leftrightarrow, \neg, A, B, C, D, E, \ldots\}$$

gdje se A, B, C, ... zovu propozicionalne varijable, $\land$, $\lor$, $\to$, $\leftrightarrow$, $\neg$ su veznici, a "(" i ")" su pomoćni simboli (otvorena i zatvorena zagrada).

Imena veznika $\land$, $\lor$, $\to$, $\leftrightarrow$ i $\neg$ su sljedeća:

$\land$ je konjunkcija (također se ponegdje označava i s & ili && ili $\times$ ili $\cdot$)

$\lor$ je disjunkcija (također se ponegdje označava i s | ili || ili +)

$\to$ je implikacija ili kondicional ili pogodba

$\leftrightarrow$ je ekvivalencija ili bikondicional ili dvopogodba

$\neg$ je negacija (također se ponegdje označava s $-A$ ili $\overline{A}$).

Propozicionalnih varijabli u alfabetu ima beskonačno (označavat ćemo ih velikim slovima A, B, X, P, Q, ..., ili velikim slovima s indeksom A_1, A_2, A_3, ...).

Ponekad, u nekim knjigama ili člancima, alfabet logike sudova sadrži i konstante 0 i 1 (ili $\perp$ i $\top$). Kasnije ćemo vidjeti kako je to praktično za razne zapise, ali remeti urednost i "estetiku" logike sudova pa ih ovdje nećemo smatrati znakovima alfabeta.

Definicija 1.2.1. *Riječ je konačan "niz" znakova alfabeta.*

Primjer 1.2.1. $\vee(($AA, ABBA, RIJEČ, NERIJEČ, $\vee\vee\rightarrow$ su primjeri riječi logike sudova.

Konkatenacija je postupak nastavljanja jedne riječi na drugu, tj. spajanje dviju riječi u jednu. Npr. konkatenacijom riječi ANA i NAS dobivamo riječ ANANAS.

Neće nas zanimati sve riječi, nego samo neke od njih koje ćemo zvati formule.

Definicija 1.2.2.

1. *Svaka propozicionalna varijabla je formula.*
2. *Ako su F_1 i F_2 formule, tada su i riječi $(\neg F_1)$, $(F_1 \wedge F_2)$, $(F_1 \vee F_2)$, $(F_1 \rightarrow F_2)$ i $(F_1 \leftrightarrow F_2)$ također formule.*
3. *Riječ alfabeta logike sudova je formula ako i samo ako je nastala konačnim brojem korištenja koraka 1 i 2.*

Ovakva definicija naziva se induktivna jer "od manjih formula idemo k većima".

Primjer 1.2.2.

a) A, B, $\check{Z}$, ... su formule po 1. pravilu jer su propozicionalne varijable.

b) Budući da su A i B formule, zbog 2. su pravila i $(A \wedge B)$ te $(B \vee A)$ također formule. A onda je opet, po 2. pravilu $\big((A \wedge B) \rightarrow (B \vee A)\big)$ formula. I tako dalje.

Pravila o zagradama, iz definicije formule, nećemo se strogo držati. Ako je jasno "o kojoj se formuli radi", preskočit ćemo zagrade. Tako ćemo $\big((A \wedge B) \rightarrow (B \vee A)\big)$ kraće (i nepravilno) pisati kao $(A \wedge B) \rightarrow (B \vee A)$ ili još kraće $A \wedge B \rightarrow (B \vee A)$.

Dalje, $B \vee A \rightarrow (A \wedge \neg B)$ u stvari je formula $\big((B \vee A) \rightarrow \big(A \wedge (\neg B)\big)\big)$ jer smatrat ćemo kako najveći prioritet ima veznik $\neg$, svi ostali veznici imaju međusobno jednak prioritet i manji od prioriteta veznika "ne".

U nekim knjigama prioriteti su zadani na sljedeći način

Operator	Prednost
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

U nekima $\neg$ ima najveći prioritet, zatim $\wedge$ i $\vee$ koji imaju jednaku važnost pa na kraju $\rightarrow$ i $\leftrightarrow$ koji također imaju međusobno jednaku važnost, itd.

Primjer 1.2.3. Ako su A_1, A_2, A_3, ..., propozicionalne varijable (ima ih beskonačno), onda $A_1 \wedge A_2 \wedge A_3 \wedge \ldots \wedge A_{100}$ jest formula, ali $A_1 \wedge A_2 \wedge A_3 \wedge \ldots$ gdje je u toj riječi navedeno beskonačno puno propozicionalnih varijabli, nije formula zbog 3. pravila.

Po gornjoj definiciji sada imamo razumljiv, razgovorni jezik logike sudova. Jasno je što je riječ, a što ne, što je formula, a što ne.

Što će značiti riječ (formula) $A \rightarrow Z$? To sada moramo odlučiti, a radi se o jednom od najvažnijih zadataka iz same baze logike sudova.

Logika sudova jedna je od najjednostavnijih logika i njene formule ne mogu značiti nešto što vidimo ili možemo uzeti u ruku, ne mogu imati vrijednost 4 ili "najvjerojatnije". Za formule logike sudova dogovoreno je da mogu imati samo dvije vrijednosti, 1 ili 0. Kako se to ne bi miješalo s uobičajenim značenjima simbola 1 (jedan) i 0 (nula), ponegdje se, u nekim knjigama, vrijednosti koje mogu imati ovakve formule označavaju s $\top$ i $\bot$ ili, u nekim knjigama, T i F (po riječima engleskog jezika "true" i "false").

Sintaksa logike sudova rekla nam je što su smislene riječi, formule, a semantika će sada dati tim formulama neko značenje.

Definicija 1.2.3. *Interpretacija je svaka funkcija sa skupa propozicionalnih varijabli na skup* $\{0, 1\}$.

U ovoj ćemo knjizi puno puta koristiti znak "=". Treba primijetiti dvije stvari:

1. Jednakost je najvažnija matematička relacija i najčešće je korišten znak u matematici.
2. Jedan te isti "=" koristimo za potpuno različite stvari u različitim područjima matematike.

Upravo definirani $I(A) = 1$ dao je propozicionalnoj varijabli vrijednost istina.
$I(F) = I(G)$ će dalje u tekstu reći da formule F i G imaju jednaku vrijednost za jednake vrijednosti svojih propozicionalnih varijabli.

Treći "=" koji predstavlja dvomjesnu relaciju logike prvog reda proizvoljno je definirana relacija koja može biti skup parova koji u određenoj prilici odgovaraju teoriji za koju se ovaj "=" definira.

U teoriji skupova, prvi $A = B$ govori da dva skupa imaju jednake elemente, a u teoriji kardinalnih brojeva, $k(A) = k(B)$ kaže da između dvaju skupova, A i B možemo uspostaviti bijekciju.

Najčešći "=", kao kod $2 + 3 = 5$, govori nam da su kardinalni brojevi $2 + 3$ i 5 jednaki itd.

Primjer 1.2.4. Funkcija I, za koju je $I(A) = 0$, $I(B) = 0$, $I(C) = 0$, ..., tj. koja svakoj propozicionalnoj varijabli pridružuje nulu je interpretacija.

Najčešće se interpretacija zadaje samo na propozicionalnim varijablama koje se pojavljuju u promatranoj formuli. Tako ćemo i za funkciju $I : \{X, Y, Z, W\} \to \{0, 1\}$, zadanu pravilom $I(X) = 1$, $I(Y) = 0$, $I(Z) = 0$, $I(W) = 1$, ako je zadana formula $(Y \wedge Y) \vee (Z \wedge W)$, reći da je interpretacija, premda nije definirana na čitavom skupu propozicionalnih varijabli, tj. ne znamo koliko je npr. $I(\check{Z})$ (što nam i ne treba ako se $\check{Z}$ ne pojavljuje kao varijabla u formulama koje će se analizirati). Takvu interpretaciju zovemo parcijalna.

Svaka od varijabli sada može predstavljati neku pojavu iz "stvarnog svijeta" koja može imati dva stanja (0 i 1) – žicu kroz koju prolazi ili ne prolazi struja ili sud koji je istinit ili lažan itd.
Koju će od zadanih vrijednosti imati pojedina formula ako njene propozicionalne varijable imaju unaprijed zadane interpretacije, tj. vrijednosti 0 ili 1?
Kako interpretirati formulu ako znamo interpretaciju njenih propozicionalnih varijabli?

Definicija je induktivna, tj. na isti način kao što gradimo formule, računamo i interpretaciju formule.
Ako je $I(F) = 0$ i $I(G) = 0$ gdje su F i G neke dvije formule (možda i samo propozicionalne varijable), definirat ćemo $I(F \wedge G) = 0$.
Ako je $I(F) = 0$ i $I(G) = 1$, definirat ćemo $I(F \wedge G) = 0$ i tako dalje po sustavu koji je dan u sljedećoj tablici:

Tablica 1.2.1

F	G	$\neg F$	$F \wedge G$	$F \vee G$	$F \to G$	$F \leftrightarrow G$
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Ako je $I(F) = 1$, kažemo da je formula F istinita za interpretaciju I, a ako je $I(F) = 0$, kažemo kako je F lažna (neistinita, laž) za interpretaciju I.

Primjer 1.2.5. Ako je $I(P) = 0$, $I(R) = 1$, $I(S) = 1$, odredimo $I\big(S \to (P \wedge R)\big)$.

Rješenje. $I(P) = 0$, $I(R) = 1$ povlači $I(P \wedge R) = 0$ (gledamo drugi red gornje tablice i četvrti stupac).
$I(S) = 1$ i $I(P \wedge R) = 0$ daje $I\big(S \to (P \wedge R)\big) = I(\text{"}1\text{"} \to \text{"}0\text{"}) = 0$ (gledamo treći red gornje tablice i šesti stupac).
Dakle, za $I(P) = 0$, $I(R) = 1$, $I(S) = 1$ slijedi $I\big(S \to (P \wedge R)\big) = 0$.
Odredimo sada sve moguće interpretacije formule $S \to (P \wedge R)$ s obzirom na sve mogućnosti interpretacija varijabli P, R i S.
Od sada ćemo $I(A) = 0$ kraće (i nepravilno) pisati kao $A = 0$.
Formulu ispitujemo pomoću tablice istinitosti ili semantičke tablice kao dolje.

Tablica 1.2.2

P	R	S	$P \wedge R$	$S \to (P \wedge R)$
0	0	0	0	1
0	0	1	0	0
0	1	0	0	1
0	1	1	0	0
1	0	0	0	1
1	0	1	0	0
1	1	0	1	1
1	1	1	1	1

Iz tablice iščitavamo (prvi red): Ako je $P = 0$, $R = 0$, $S = 0$, onda je $S \to (P \wedge R) = 1$, ako je $P = 0$, $R = 0$, $S = 1$ (drugi red), onda je $S \to (P \wedge R) = 0$, itd.

Vidimo da zadana formula $S \to (P \wedge R)$ ponekad, u nekim redovima, ima vrijednost 1. Takvu formulu zovemo ispunjiva formula. Ona u nekim redovima ima i vrijednost 0. Takvu formulu zovemo oboriva formula. Točnije:

Definicija 1.2.4.

1. *Ako za zadanu formulu F logike sudova postoji interpretacija njenih varijabli za koju ta formula ima vrijednost 1, onda za tu zadanu formulu kažemo da je* ***ispunjiva****.*
2. *Ako za zadanu formulu F logike sudova postoji interpretacija njenih varijabli za koju ta formula ima vrijednost 0, onda za tu zadanu formulu kažemo da je* ***oboriva****.*
3. *Ako zadana formula F logike sudova ima za sve interpretacije svojih varijabli vrijednost 1, zovemo ju* ***valjana formula*** *ili* ***tautologija****.*
4. *Ako zadana formula F logike sudova ima za sve interpretacije svojih varijabli vrijednost 0, zovemo ju* ***antitautologija****.*

Ispitati formulu znači odrediti njene vrijednosti na osnovu svih mogućih vrijednosti varijabli koje se u toj formuli pojavljuju te odrediti je li zadana formula ispunjiva, je li oboriva, je li tautologija i je li antitautologija.

Primjer 1.2.6. Ispitaj formulu $F \equiv (A \wedge C) \to (\neg B \vee \neg C)$.

Rješenje.

Tablica 1.2.3: Ispitivanje formule $F \equiv (A \wedge C) \to (\neg B \vee \neg C)$ tablicom istinitosti ili semantičkom tablicom uz dva pomoćna stupca, $A \wedge C$ i $\neg B \vee \neg C$.

A	B	C	$A \wedge C$	$\neg B \vee \neg C$	$(A \wedge C) \to (\neg B \vee \neg C)$
0	0	0	0	1	1
0	0	1	0	1	1
0	1	0	0	1	1
0	1	1	0	0	1
1	0	0	0	1	1
1	0	1	1	1	1
1	1	0	0	1	1
1	1	1	1	0	0

Zaključujemo kako zadana formula:

a) jest ispunjiva jer je npr. u četvrtom redu tablice, za $I(A) = 0$, $I(B) = 1$, $I(C) = 1$

vrijednost formule F jednaka 1, tj. postoji red u kojem je $I(F) = 1$.

b) jest oboriva jer je npr. u zadnjem redu tablice, za $I(A) = 1$, $I(B) = 1$, $I(C) = 1$ vrijednost formule F jednaka 0, tj. postoji red u kojem je $I(F) = 0$.

c) Nije tautologija jer F nema uvijek vrijednost 1.

d) Nije antitautologija jer F nema uvijek vrijednost 0.

Dalje zaključujemo kako je tablica pregledna analiza formule s obzirom na njene interpretacije, ali pri tome ne smijemo zaboraviti kako prvi red tablice u stvari znači: ako je zadana interpretacija I (koja svakoj propozicionalnoj varijabli pridružuje vrijednost iz skupa $\{0, 1\}$) koja varijabli A pridružuje vrijednost 0, varijabli B vrijednost 0 i varijabli C vrijednost 0, onda je i vrijednost formule F jednaka 0 i tako dalje.

Definicija 1.2.5. *Ako je $S = \{F_1, F_2, \ldots, F_n\}$ skup formula, a F formula za koju vrijedi: za svaku interpretaciju I, za koju je $I(F_i) = 1$, $\forall i = 1, 2, \ldots, n$ je i $I(F) = 1$, onda kažemo da F logički slijedi iz skupa S i pišemo $S \models F$.*

Primjer 1.2.7. Za $S = \{A,\ A \to C\}$ i $F = C$ vrijedi $S \models F$ jer za interpretacije I za koje je $I(A) = 1$ i $I(A \to C) = 1$, slijedi i $I(C) = 1$. To vidimo i iz tablice 1.2.4 (samo interpretacija iz zadnjeg reda tablice to ispunjava). Dakle, $\{A,\ A \to C\} \models C$.

Tablica 1.2.4: Semantičke tablice formula $A \to C$ i C.

A	C	$A \to C$	C
0	0	1	0
0	1	1	1
1	0	0	0
1	1	1	1

Ako je skup S jednočlan, često $S \models F$ pišemo kao $S \Rightarrow F$, ponekad i bez vitičastih zagrada koje označavaju skup.

Primjer 1.2.8. $\{A\} \Rightarrow \neg\neg A$ kratko pišemo $A \Rightarrow \neg\neg A$.

Definicija 1.2.6. *Za formule F i G logike sudova kažemo da su logički ekvivalentne i pišemo $F \Leftrightarrow G$ ako za svaku interpretaciju I vrijedi $I(F) = I(G)$, tj. F i G imaju jednake vrijednosti za sve interpretacije varijabli koje se u F i G pojavljuju, tj. $F \Rightarrow G$ i $G \Rightarrow F$.*

Ako su dvije riječi ili dvije formule potpuno jednake, tj. ako je $F = A \to B$ i $G = A \to B$, pišemo $F \equiv G$.

Primjerice, ako je $F = A \vee B$ i $G = B \vee A$, ne vrijedi $F \equiv G$, tj. $F \not\equiv G$; no, vrijedi da je F logički ekvivalentno s G, tj. $F \Leftrightarrow G$.
Formulu ćemo često zadavati kao "Neka je $F \equiv \ldots$", tj. F je točno ta formula.

Primjer 1.2.9. Neka je $F \equiv A \leftrightarrow B$, $G \equiv B \leftrightarrow A$. Vrijedi $F \Leftrightarrow G$, $F \not\equiv G$.

Ponegdje se $F \Leftrightarrow G$ piše kao $F = G$.

Primjer 1.2.10. Pogledajmo tablice istinitosti formula $A \to B$ i $\neg A \vee B$.

Tablica 1.2.5: Semantičke tablice formula $A \to B$ i $\neg A \vee B$.

A	B	$A \to B$	$\neg A \vee B$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Ove dvije formule imaju iste vrijednosti za iste interpretacije svojih varijabli (imaju "zadnji stupac jednak") pa vrijede svi ovi zapisi:

$$\{A \to B\} \models \neg A \vee B, \qquad \{A \to B\} \Rightarrow \neg A \vee B, \qquad A \to B \Rightarrow \neg A \vee B$$
$$\{\neg A \vee B\} \models A \to B, \qquad \{\neg A \vee B\} \Rightarrow A \to B, \qquad \neg A \vee B \Rightarrow A \to B$$

Ili, najjača tvrdnja, iz koje slijede sve gornje, $A \to B \Leftrightarrow \neg A \vee B$.

Zadaci za vježbu

Zadatak 1.2.1. Semantičkom tablicom ispitajte formule

a) $F \equiv (A \to B) \wedge (B \to A)$

b) $F \equiv (A \leftrightarrow B) \vee (B \leftrightarrow \neg C)$

c) $F \equiv A \to B \to C$

d) $F \equiv A \to (B \to C)$

Zadatak 1.2.2. Dokaži da su sljedeće formule matematičke logike tautologije (i nauči njihova imena). Dalje, osmisli rečenice iz života na koje se mogu primijeniti dolje navedene

formule, gdje je zadana formula složena rečenica, a propozicionalne varijable jednostavne rečenice koje se u njoj pojavljuju.
Npr. $0 \leftrightarrow P \wedge \neg P$ možemo predstaviti rečenicom "Nemoguće je da si i bio na fakultetu i nisi bio na fakultetu." (Uočimo kako smo ovdje znak 0 koristili kao propozicionalnu varijablu.)

a) $F \equiv \neg\neg P \leftrightarrow P$ (dvojna negacija)

b) $F \equiv P \rightarrow P$ (refleksivnost kondicionala)

c) $F \equiv P \leftrightarrow P$ (refleksivnost bikondicionala)

d) $F \equiv P \vee \neg P$ (princip isključenja trećeg)

e) $F \equiv \neg(P \wedge \neg P)$ (neproturječnost)

Zadatak 1.2.3. Dijelove zadanih rečenica zamijeni propozicionalnim varijablama te upotrijebi pravilan veznik kako bi dobivena formula logike sudova dobro prezentirala zadane rečenice. Sastavi tablicu istinitosti dobivene formule i prokomentiraj ju.

a) "Skupim li 50 bodova, položit ću pismeni ispit."

b) "Nos joj je lijep, ali obrazi joj nisu crveni."

c) "Bude li kiša i bude li sunce, izaći će duga, jednaka je informacija kao i ako nema duge, onda nema ni sunca ni kiše."

d) "Bude li jak vjetar, stići ćemo biciklom na predavanje na vrijeme."

e) "Samo nas jak vjetar može dovesti na predavanje na vrijeme."

Zadatak 1.2.4. Dokaži i kao u zadatku 1.2.3. navedi primjer rečenica iz uobičajenog, svakodnevnog govora na koje se mogu primijeniti zadani izrazi.

a) $P \rightarrow R \Leftrightarrow \neg R \rightarrow \neg P$ (formula kontrapozicije)

b) $(P \vee R) \vee S \Leftrightarrow P \vee (R \vee S)$ (disjunkcija je asocijativna)

c) $(P \wedge R) \wedge S \Leftrightarrow P \wedge (R \wedge S)$ (konjunkcija je asocijativna)

d) $(P \wedge R) \vee S \Leftrightarrow (P \vee S) \wedge (R \vee S)$ (konjunkcija je distributivna prema disjunkciji)

e) $(P \vee R) \wedge S \Leftrightarrow (P \wedge S) \vee (R \wedge S)$ (disjunkcija je distributivna prema konjunkciji)

f) $\neg(P \vee R) \Leftrightarrow \neg P \wedge \neg R$ (De Morganov zakon)

g) $\neg(P \wedge R) \Leftrightarrow \neg P \vee \neg R$ (De Morganov zakon)

Zadatak 1.2.5. Većina je matematičkih teorema, iskaza, zaključaka u obliku $P \to R$ (ako P, onda R, iz P slijedi R, P je dovoljan uvjet za R, R je nužan za (ako bude) $P, \ldots$). Suprotna izjava od $P \to R$ je izjava $P \wedge \neg R$. Zadane rečenice zapiši koristeći pojmove "dovoljan", "nedovoljan", "nužan" i "ne nužan" te negiraj zadanu implikaciju.

a) Ako kiša pada, trava raste.

b) $n \in \mathbb{N} \Rightarrow n^2 \in \mathbb{N}$.

c) Ako dva pravca (iste ravnine) nisu paralelna, oni se sijeku.

Zadatak 1.2.6. Formula $\neg B \to \neg A$ zove se kontrapozicija formule $A \to B$.
Pokaži tablicom istinitosti kako su te dvije formule ekvivalentne.
U matematici neku formulu često dokazujemo tako da dokažemo njenu kontrapoziciju. Dokaži zadane tvrdnje direktno, kao $A \to B$, a onda i po kontrapoziciji, tako da počneš od $\neg B$ i onda iz toga dokažeš $\neg A$.

a) $\forall a \in \mathbb{N}$, a^2 je paran $\Rightarrow a$ je paran.

b) $x = 4 \Rightarrow x^2 - 3x - 4 = 0$.

Zadatak 1.2.7. Ana, Barbara i Cvijeta tri su djevojčice koje su ostale same kod kuće dok se roditelji ne vrate iz trgovine. A kad su se roditelji vratili, pronašli su tri djevojčice i razbijen prozor. U istrazi, na pitanje tko je to učinio, odgovorile su:

Ana: Ja nisam, to je neka od njih dviju ili su čak zajedno to učinile.
Barbara: Ako je Cvijeta kriva, onda je i Ana, bile su zajedno.
Cvijeta: Barbara je kriva, a ne Ana.

a) Je li moguća situacija u kojoj sve tri govore istinu? Tko je, dakle, onda kriv?

b) Je li moguće da su sve tri izjave laž (je li to moguća situacija)?

c) Ako niti jedna djevojčica nije kriva, tko je sve lagao?

d) Pretpostavimo li krivicu svh triju djevojčica, tko je sve lagao?

e) Pretpostavimo li lažnu izjavu od krivaca, a istinitu od nevinih, tko je slagao, a tko ne? Tko je u tom slučaju kriv?

Zadatak 1.2.8. Na stolu se nalaze četiri karte na kojima vidimo A, B, 4, 9. Ne znamo o kakvim je kartama riječ. No, netko nam je rekao: "Ako je s jedne strane karte samoglasnik, s druge je parni broj."
Koje sve karte moramo okrenuti kako bismo provjerili tu izjavu?

Zadatak 1.2.9. Sve kao u prethodnom zadatku, s tim da su na stolu A, B, 5, 8, \$. Izjava kojoj treba provjeriti istinitost jest "Ako neka od karata s obje strane ima paran broj, onda postoji karta sa znakom \$ na objema stranama."

Zadatak 1.2.10. Nalazimo se pred dvama kovčezima. Na jednom je natpis: "U ovom kovčegu nije blago.", a na drugom "Točno jedna od ovih dviju rečenica je istinita". Možemo li na osnovu ovih dvaju tekstova saznati u kojem je kovčegu blago?

Zadatak 1.2.11. Neka je $\{A, B, C\}$ skup propozicionalnih varijabli.
Postoji li interpretacija I za koju bi sve formule sastavljene od A, B i C bile tautologije?

Rješenja

1.2.1. a)

A	B	$A \to B$	$B \to A$	F
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

F je ispunjiva, F je oboriva, F nije tautologija i F nije antitautologija.

b)

A	B	C	$A \leftrightarrow B$	$B \leftrightarrow \neg C$	F
0	0	0	1	0	1
0	0	1	1	1	1
0	1	0	0	1	1
0	1	1	0	0	0
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	1	1	1
1	1	1	1	0	1

F je ispunjiva, F je oboriva, F nije tautologija i F nije antitautologija.

c)

A	B	C	$A \to B$	$A \to B \to C$
0	0	0	1	0
0	0	1	1	1
0	1	0	1	0
0	1	1	1	1
1	0	0	0	1
1	0	1	0	1
1	1	0	1	0
1	1	1	1	1

F je ispunjiva, F je oboriva, F nije tautologija i F nije antitautologija.

d)

A	B	C	$B \to C$	$A \to (B \to C)$
0	0	0	1	1
0	0	1	1	1
0	1	0	0	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	0	0
1	1	1	1	1

F je ispunjiva, F je oboriva, F nije tautologija i F nije antitautologija.
Usporedi rezultate s prethodnima. Zaključi o implikaciji i asocijativnosti.

1.2.2. a)

P	$\neg P$	$\neg\neg P$	$\neg\neg P \leftrightarrow P$
0	1	0	1
1	0	1	1

$\neg\neg P \leftrightarrow P$ je ispunjiva, $\neg\neg P \leftrightarrow P$ nije oboriva, $\neg\neg P \leftrightarrow P$ je tautologija i $\neg\neg P \leftrightarrow P$ nije antitautologija.
"Rekao sam da nije istina da on to nije učinio, odnosno učinio je to."

b)

P	$P \to P$
0	1
1	1

$P \to P$ je ispunjiva, $P \to P$ nije oboriva, $P \to P$ je tautologija i $P \to P$ nije antitautologija.
"Ako sam rekao, rekao sam."

c)

P	$P \leftrightarrow P$
0	1
1	1

"Matematika je matematika."

d)

P	$P \vee \neg P$
0	1
1	1

"Ili jesmo ili nismo."

e)

P	$P \wedge \neg P$	$\neg(P \wedge \neg P)$
0	0	1
1	0	1

"Nemoguće je da si položio i da nisi položio ispit.(?)"

1.2.3. a) "Skupim li 50 bodova, položit ću pismeni ispit."
A - skupio sam 50 bodova
B - položio sam ispit
"Skupim li 50 bodova, položit ću pismeni ispit." je rečenica u kojoj je prvi dio uvjet za drugi. Ako bude ispunjen prvi dio rečenice, bit će i drugi. Dakle, rješenje je $A \to B$.

A	B	$A \to B$
0	0	1
0	1	1
1	0	0
1	1	1

Red $I(A) = 0$, $I(B) = 0$ znači: nisam skupio 50 bodova i nisam položio ispit.
Red $I(A) = 0$, $I(B) = 1$ znači: nisam skupio 50 bodova, a položio sam ispit.
Red $I(A) = 1$, $I(B) = 0$ znači: skupio sam 50 bodova i nisam položio ispit.
Red $I(A) = 1$, $I(B) = 1$ znači: skupio sam 50 bodova i položio sam ispit.

Samo treći red u suprotnosti je sa zadanom tvrdnjom jer tvrdnja kaže da student koji ima 50 bodova položit će ispit, a dogodilo se da student ima 50 bodova i "srušili smo ga" na ispitu. Zato je samo treći red formule $A \to B$ jednak 0.
Uočimo ovdje kako slučaj "nisam skupio 50 bodova, a položio sam ispit" ne čini početnu izjavu lažnom. Moguće je možda da student ne skupi 50 bodova, ali da kasnije ispit položi pomoću seminara ili slično.

b) "Nos joj je lijep, ali obrazi joj nisu crveni."
A – nos joj je lijep
B – obrazi su joj crveni
Rješenje: $A \wedge \neg B$

A	B	$A \wedge \neg B$
0	0	0
0	1	0
1	0	1
1	1	0

Red $I(A) = 0$, $I(B) = 0$ znači da osoba nema lijep nos i nema crvene obraze. U toj situaciji izjava o njoj: "Nos joj je lijep, ali obrazi joj nisu crveni." je lažna.
Red $I(A) = 0$, $I(B) = 1$ znači da osoba nema lijep nos i ima crvene obraze. U toj situaciji izjava o njoj: "Nos joj je lijep, ali obrazi joj nisu crveni." je lažna.
Red $I(A) = 1$, $I(B) = 0$ znači da osoba ima lijep nos i nema crvene obraze. U toj situaciji izjava o njoj: "Nos joj je lijep, ali obrazi joj nisu crveni." je

istinita.
Red $I(A) = 1$, $I(B) = 1$ znači da osoba ima lijep nos i ima crvene obraze. U toj situaciji izjava o njoj: "Nos joj je lijep, ali obrazi joj nisu crveni." je lažna.

Uočimo da je moguće i rješenje
A – nos joj je lijep
B – obrazi joj nisu crveni
Rješenje: $A \wedge B$

Očito je veznik hrvatskog jezika "ali" modeliran logičkim veznikom $\wedge$. Podatak "Nos joj je lijep, ali obrazi joj nisu crveni.", naime, znači nam isto što i "Nos joj je lijep i obrazi joj nisu crveni." "Nos joj je lijep, a obrazi joj nisu crveni." "Nos joj je lijep, no obrazi joj nisu crveni." "Nos joj je lijep, obrazi joj nisu crveni.". Dva su podatka nabrojana i nisu niti u kakvoj vezi (premda, stilski, kod veznika "a" ili "ali" kao da želimo reći da djevojci nešto jest, a nešto nije dobro, a kod sastavnih veznika jednostavno čujemo dva podatka bez naznake da je nešto bolje, a nešto lošije) pa treba upotrijebiti $\wedge$.

Zanimljivo je pokušati naći dvije rečenice u kojoj su sve riječi iste, osim što smo u jednoj upotrijebili "a", a u drugoj "ali" i da te dvije rečenice imaju različita tumačenja.

Gledajući rečenice strogo kao informaciju, podatak iz kojeg nešto saznajemo, svi se sastavni i suprotni veznici modeliraju s $\wedge$.
I isključni veznici prezentiraju se s $\wedge$. Npr. "Svi su učenici Osječani osim Perice koji je iz Vinkovaca" modeliramo s $A \wedge B$, gdje je A – svi su učenici Osječani, B – Perica je iz Vinkovaca.

Vremenski veznici također se zamjenjuju s $\wedge$: "Ivan je ustao nakon čega je oprao zube." Također je oblika $A \wedge B$, gdje je A – "Ivan je ustao", B – "Ivan je oprao zube."

Logika sudova ne može iskazati karakteristike kao što su pozitivnost ili negativnost podatka (to je u "jačim" logikama jednomjesni predikat "biti pozitivan", itd.), ili vremenski odnos (pranje zubi je poslije ustajanja) dvije radnje (to je dvomjesni predikat). Prejednostavna je, preslaba, za takve odnose. No, logika prvog reda oba zahtjeva može izmodelirati.

c) "Bude li kiša i bude li sunce izaći će duga, jednaka je informacija kao i ako nema duge, onda nema ni sunca ni kiše."

A – Kiša je.
B – Sunce je.
C – Duga je izašla.

Izjava je sada oblika: $(A \wedge B) \to C \leftrightarrow \neg C \to (\neg A \wedge \neg B)$.

A	B	C	$(A \wedge B) \to C \leftrightarrow \neg C \to (\neg A \wedge \neg B)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Očito izjava nije uvijek istinita. Npr. u situaciji (red $I(A) = 0$, $I(B) = 1$, $I(C) = 0$) kada nema kiše, a sunčano je i nema duge, dio "Bude li kiša i bude li sunce, izaći će duga.", jer $0 \to 0$ je istina, je točan, dok je drugi dio izjave, "Ako nema duge, onda nema ni sunca ni kiše." lažan. Jer zaista, nema duge, pa ne bi trebalo biti ni sunca ni kiše, a sunca ima.

d) "Bude li jak vjetar, stići ćemo biciklom na predavanje na vrijeme."

A – vjetar je
B – stići ćemo na predavanje, biciklom, na vrijeme

Izjava je oblika $A \to B$. Sve je kao u zadatku pod a).

e) "Samo nas jak vjetar može dovesti na predavanje na vrijeme."
Pogledamo li zadatak pod d), uočit ćemo kako je ovdje posrijedi česta matematička igra "ako i samo ako" ili "nužan i dovoljan uvjet". U d) zadatku jak vjetar dovoljan je da stignemo na predavanje. U ovom, e), zadatku, znamo da ako se pojavi jak vjetar, onda jedino imamo šanse stići na vrijeme. Tj. ako se i dogodi da smo stigli na vrijeme, sto posto sigurno dogodilo se to uz pomoć vjetra. Ili, uz oznake

A – vjetar je
B – stići ćemo na predavanje, biciklom, na vrijeme.

izjava je oblika $B \to A$.

U d) zadatku vjetar je dovoljan uvjet za stići na vrijeme. U e) zadatku vjetar je nužan za stići na vrijeme. Pogledajte i zadatak 1.2.5. (Dovoljno i nužno, ako i samo ako, akko (iff na engleski) – nužno je, ali ne i dovoljno razumjeti da bismo rekli da smo razumjeli matematičku logiku.)

1.2.4. a)

P	R	$P \to R$	$\neg R \to \neg P$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Zaista, $P \to R \Leftrightarrow \neg R \to \neg P$ jer za svaku interpretaciju I vrijedi:
$I(P \to R)= I(\neg R \to \neg P)$ tj. $P \to R$ i $\neg R \to \neg P$ imaju jednake vrijednosti za sve interpretacije varijabli P i R.
"Da nije bio u toj državi, ne bi se zarazio.", tj. ako se zarazio, bio je tamo.

b)

P	R	S	$(P \vee R) \vee S$	$P \vee (R \vee S)$
0	0	0	0	0
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	1	1
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

"Odaberi Petru ili Ružicu, ili odaberi Snježanu".
"Odaberi Petru ili odaberi Ružicu ili Snježanu".

c) Gotovo je sve isto kao i u b). Rečenice su npr. "Za položiti ispit morate biti prisutni na 80 % predavanja i riješiti pismeni ispit s bar 50 %, a onda i položiti usmeni ispit." i "Za položiti ispit morate biti prisutni na 80 % predavanja, a zatim i riješiti pismeni ispit s bar 50 % te usmeni ispit."

d) $(P \wedge R) \vee S \Leftrightarrow (P \vee S) \wedge (R \vee S)$ (konjunkcija je distributivna prema disjunkciji)

P	R	S	$(P \wedge R) \vee S$	$(P \vee S) \wedge (R \vee S)$
0	0	0	0	0
0	0	1	1	1
0	1	0	0	0
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

"Ispit ćete riješiti tako da položite pismeni ispit i nakon njega usmeni, ili napišite samo seminar. Dakle, pismeni (ili seminar) i još usmeni (ili već navedeni seminar)."

e) $(P \vee R) \wedge S \Leftrightarrow (P \wedge S) \vee (R \wedge S)$ (disjunkcija je distributivna prema konjunkciji)

P	R	S	$(P \vee R) \wedge S$	$(P \wedge S) \vee (R \wedge S)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	0
1	0	1	1	1
1	1	0	0	0
1	1	1	1	1

"Danas je utorak ili srijeda i zima je. Drugim riječima, danas je utorak i zima je ili je srijeda i zima je."

f) $\neg(P \vee R) \Leftrightarrow \neg P \wedge \neg R$ (De Morganov zakon)

P	R	$\neg(P \vee R)$	$\neg P \wedge \neg R$
0	0	1	1
0	1	0	0
1	0	0	0
1	1	0	0

"Nije istina da su to bili Pero ili Lovro. Nije bio niti Pero niti Lovro."

g) $\neg(P \wedge R) \Leftrightarrow \neg P \vee \neg R$ (De Morganov zakon)

P	R	$\neg(P \wedge R)$	$\neg P \vee \neg R$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

"Nemoguće da su njih dvojica bili u istoj prostoriji. Ili nije bio Pero ili nije bio Lovro."

1.2.5. a) Ako kiša pada, trava raste.
Dovoljno je da kiša pada i trava će rasti.
Nije dovoljno da trava raste da bismo mogli reći da kiša pada.
Da bismo mogli reći da kiša pada, nužno je (između ostalog) da trava raste.
Nužan je rast trave za pad kiše. (Nužno je da trava raste ako kiša pada.)
Nije nužno da kiša pada da bi trava rasla.

Negacija zadane izjave: Kiša pada i trava ne raste.

b) $n \in \mathbb{N} \Rightarrow n^2 \in \mathbb{N}$.
Dovoljno je da broj bude prirodan da bi mu i kvadrat bio prirodan.
Nije dovoljno da kvadrat broja bude prirodan za zaključak da je i sami broj prirodan. (Zaista $(-5)^2 = 25$ i $-5 \notin \mathbb{N}$.)
Nužno je da kvadrat bude prirodan ako želimo da i (promatrani, traženi, odabrani) broj bude prirodan. Nije nužno da broj bude prirodan za činjenicu da mu je kvadrat prirodan.

Negacija zadane izjave: $n \in \mathbb{N}$ i $n^2 \notin \mathbb{N}$.

c) Ako dva pravca (iste ravnine) nisu paralelna, oni se sijeku.
Dovoljno je da pravci nisu paralelni pa će se sigurno sjeći.
Nije dovoljno da se pravci sijeku da bismo zaključili kako nisu paralelni. Ovo je sada lažna izjava, jer u izjavi c) "Ako" je "ako i samo ako", tj. vrijedi i $P \to R$ i $R \to P$, tj. $P \leftrightarrow R$.
Nužno je da se pravci sijeku kako bismo utvrdili da nisu paralelni.
Nije nužno da dva pravca nisu paralelna za zaključak da se sijeku. I ovo je lažna izjava.

Negacija zadane izjave: Postoje dva pravca koja nisu paralelna, a i ne sijeku se.

1.2.6. a) $A \to B$:
a^2 je paran $\Rightarrow$ u rastavu broja a^2 na proste faktore, pojavljuje se broj 2 $\Rightarrow$ u rastavu broja a na proste faktore, pojavljuje se broj 2 $\Rightarrow a = 2k,\ k \in \mathbb{N} \Rightarrow a$ je paran.

$\neg B \to \neg A$:
a je neparan $\Rightarrow a = 2k-1,\ k \in \mathbb{N} \Rightarrow a^2 = (2k-1)^2,\ k \in \mathbb{N} \Rightarrow a^2 = 4k^2-4k+1$, $k \in \mathbb{N} \Rightarrow a^2$ je neparan jer je $4k^2 - 4k$ sigurno paran, a paran broj umanjen za jedan je neparan.

b) $A \to B$:
$x = 4 \Rightarrow x^2 - 3x - 4 = 4^2 - 3 \cdot 4 - 4 = 0$

$\neg B \to \neg A$:
$x^2 - 3x - 4 \neq 0$. Ovaj izraz znači kako je istinit jedan od dvaju uvjeta

I) $x^2 - 3x - 4 > 0$	ili	I) $x^2 - 3x - 4 < 0$
I)		II)
$x \in \langle -\infty, -1\rangle \cup \langle 4, +\infty\rangle$		$x \in \langle -1, 4\rangle$

Kako $x = 4$ nije rješenje niti jedne od nejednadžbi, tj. $x = 4$ nije rješenje nejednadžbe $x^2 - 3x - 4 \neq 0$, iz $x^2 - 3x - 4 \neq 0$, slijedi $x \neq 4$.

1.2.7. Očito izjave i krivice nekako treba zapisati formulama logike sudova i onda ispitati istinitost izjava i krivicu djevojčica.

Označimo, prirodno,
A – Ana je kriva,
B – Barbara je kriva,

C – Cvijeta je kriva.

Sad će $I(A) = 1$ značiti: izjava A je točna, tj. Ana je kriva je točno, a $I(A) = 0$ će značiti: izjava A je netočna, tj. Ana nije kriva.

Anina izjava (AI): Ja nisam, to je neka od njih dviju ili su čak zajedno to učinile. $\neg A \wedge (B \vee C)$
Barbarina izjava (BI): Ako je Cvijeta kriva, onda je i Ana, bile su zajedno. $C \to A$
Cvijetina izjava (CI): Barbara je kriva, a ne Ana. $B \wedge \neg A$

A	B	C	AI	BI	CI
0	0	0	0	1	0
0	0	1	1	0	0
0	1	0	1	1	1
0	1	1	1	0	1
1	0	0	0	1	0
1	0	1	0	1	0
1	1	0	0	1	0
1	1	1	0	1	0

a) Je li moguća situacija u kojoj sve tri govore istinu? Tko je, dakle, onda kriv?
Pitamo se je li moguće da su AI, BI i CI istinite. Odgovor je da. U trećem redu tablice $I(AI) = I(BI) = I(CI) = 1$, dakle, u tom slučaju sve su rekle istinu. S lijeve strane tog reda očitavamo kako je tu $I(A) = 0$, tj. Ana nije kriva za razbijeni prozor, $I(B) = 1$, tj. Barbara je kriva i $I(C) = 0$ tj. Cvijeta nije krivac.

b) Je li moguće da su sve tri izjave laž (je li to moguća situacija)?
Ne, jer ne postoji red u kojem bi bilo $I(AI) = I(BI) = I(CI) = 0$.

c) Ako niti jedna djevojčica nije kriva, tko je sve lagao?
U prvom je redu tablice $I(A) = I(B) = I(C) = 0$ (sve tri su nevine), a u tom redu je $I(AI) = 0$, $I(BI) = 1$, $I(CI) = 0$, tj. lagale su Ana i Cvijeta.

d) Pretpostavimo li krivicu svih triju djevojčica, tko je sve lagao?
U zadnjem je redu tablice $I(A) = I(B) = I(C) = 1$, a u tom redu je $I(AI) = 0$, $I(BI) = 1$, $I(CI) = 0$, tj. lagale su Ana i Cvijeta.

e) Pretpostavimo li lažnu izjavu od krivaca, a istinitu od nevinih, tko je slagao, a tko ne? Tko je u tom slučaju kriv?
Promotrimo tablicu detaljnije. Tražimo red u kojem su ispod A i AI suprotne

vrijednosti, ispod B i BI suprotne vrijednosti, ispod C i CI suprotne vrijednosti. To je šesti red za koji je $I(A) = 1$, $I(B) = 0$, $I(C) = 1$ te $I(AI) = 0$, $I(BI) = 1$, $I(CI) = 0$. To znači: Ana je kriva i dala je lažnu izjavu, Barbara nije kriva i rekla je istinu, Cvijeta je kriva i lagala je.

1.2.8. A moramo okrenuti jer možda s druge strane nije parni broj pa ćemo ga moći uhvatiti u laži.
Ako je iza A zaista parni broj, dalje treba okrenuti B. Ako je s druge strane samoglasnik, našli smo situaciju u kojoj je, dakle, s jedne strane samoglasnik, a s druge strane, nije parni broj nego B. Tu možemo dokazati da je izjava laž.
4 ne treba okretati. Ako s druge strane imamo samoglasnik, u redu je sve, izjava je točna. Ako s druge strane nije samoglasnik, opet je izjava točna (vidi prvi red $0 \to 0 = 1$ za implikaciju).

Dalje treba okrenuti i 9 jer možda je s druge strane samoglasnik pa je izjava laž. Ako s druge strane nije samoglasnik, izjava nije laž.

Dakle, u najgorem slučaju, morat ćemo okrenuti A, B i 9. 4 svakako ne treba okretati.

1.2.9. Okrećemo prvo kartu na kojoj je 8.
Ako s druge strane nije paran broj, izjava je istinita ($0 \to 0 = 1$ i $0 \to 1 = 1$).
Ako je s druge strane također neki paran broj, moramo okrenuti i kartu na kojoj je \$. Ako je i s druge strane \$, izjava je istinita. Ako s druge strane nije \$, izjava je lažna.
U ovakvim zadacima pomaže nam rješavanje zadataka pomoću blok dijagrama ili dijagrama toka (dijagram koji koristimo kod programiranja, kod početne konstrukcije algoritma).

1.2.10. Naravno da ne. Što god se u kovčezima nalazilo, netko je na njih mogao jednostavno nalijepiti te dvije izjave.

Pretpostavimo sada da je zaista u jednom od kovčega zlato i da možemo na osnovu izjava saznati u kojemu.

Moguća su, kao i do sada, četiri slučaja s obzirom na istinitost napisanih izjava.

U ovom kovčegu nije blago	Točno jedna od ovih dviju rečenica je istinita	Komentar
0	0	U prvom kovčegu je blago.

U ovom kovčegu nije blago	Točno jedna od ovih dviju rečenica je istinita	Komentar
0	1	U prvom kovčegu je blago.
1	0	Ovo je nemoguća situacija, jer ako je druga tvrdnja laž kao što piše, slijedi da su obje tvrdnje istina ili su obje tvrdnje laž, a nisu, nego je situacija 1. istina, 2. laž.
1	1	Ovo je nemoguća situacija, jer ako je druga tvrdnja istinita kao što piše, slijedi da je samo jedna tvrdnja istinita, a nije, nego su obje.

Pod pretpostavkom da je svaka od tvrdnji ili istinita ili lažna, blago mora biti u prvom kovčegu. Naravno da tamo možda nije pa je iz ovog zadatka lijepo vidljivo kako je uvjet da zadana rečenica bude ili istina ili laž jak uvjet.
Promislimo li dalje, kao što smo već rekli, lako ćemo uvidjeti da je za većinu rečenica iz razgovornog jezika teško utvrditi istinosnu vrijednost.

1.2.11. Ne.
Bez obzira kako interpretirali varijablu A, formula $A \wedge \neg A$ je antitautologija.

1.3. Konjunktivna i disjunktivna normalna forma. Odnosi među veznicima

Cilj je ovog potpoglavlja pokazati kako za zadanu formulu logike sudova postoji druga formula koja je zadanoj formuli ekvivalentna, a oblik joj je takav da sadrži samo veznike "i", "ili" i niječnicu "ne". Čitatelj će naučiti kako se navedena formula nalazi te postupak nalaženja primijeniti u rješavanju konkretnih problema.

Nakon usvojenih znanja iz potpoglavlja 1.3., čitatelj će znati konstruirati konjunktivnu i disjunktivnu formulu zadane formule te zadanu formulu logike sudova zapisati pomoću drugih veznika (točnije, naći zadanoj formuli ekvivalentnu formulu koja sadrži samo unaprijed zadane veznike ako je to izvedivo).

Literatura za 1.3. sljedeće su knjige i skripte:

1. R. Cori, D. Lascar, *Mathematical logic: a course with exercises (Part I)*, Oxford University Press, 2000.

2. M. Vuković, *Matematička logika*, Element, Zagreb, 2009.

3. M. Vuković, *Matematička logika 1*, skripta.
http://www.mathos.unios.hr/logika/Logika_skripta.pdf (zadnji pristup travanj 2022.)

Definicija 1.3.1. *Propozicionalnu varijablu ili njenu negaciju zovemo* ***literal****.*

Primjer 1.3.1. A, B, $\neg C$, $\neg M$ su literali. $A \to B$, (, $A\neg C$, $A \models \neg\neg A$ nisu literali.

Definicija 1.3.2. *Disjunkciju literala nazivamo* ***elementarna disjunkcija****.*

Primjer 1.3.2. Elementarne su disjunkcije $A \vee B \vee \neg X$, Z, $U \vee V \vee \neg U$, $\neg M$.
Elementarne disjunkcije nisu $A \to (\neg X)$, $Z \to Z$.

Definicija 1.3.3. *Konjunkciju literala nazivamo* ***elementarna konjunkcija****.*

Primjer 1.3.3. Elementarne su konjunkcije $A \wedge B \wedge \neg X$, Z, $U \wedge V \wedge \neg U$, $\neg M$.
Elementarne konjunkcije nisu $A \to (\neg X)$, $Z \to Z$.

Definicija 1.3.4. *Konjunkciju elementarnih disjunkcija oblika*

$$(A_{11} \vee A_{12} \vee \dots) \wedge (A_{21} \vee A_{22} \vee \dots) \wedge (A_{31} \vee A_{32} \vee \dots) \wedge \dots$$

s konačno puno zagrada i ukupno konačno puno literala A_{ij}, $i = 1, 2, \dots,$ $j = 1, 2, \dots$ nazivamo ***konjunktivna normalna forma*** *(skraćeno:* ***KNF****).*

Primjer 1.3.4. $(A \vee B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge (A \vee \neg C)$, $(P \vee R) \wedge (P \vee \neg P)$ su formule koje su u konjunktivnoj normalnoj formi.

Kako su A i B posebni slučajevi "jednočlanih" elementarnih disjunkcija, slijedi da je $(A) \wedge (B)$, odnosno $A \wedge B$ također poseban slučaj KNF-a.

Dalje, kako je $A \vee B$ elementarna disjunkcija, slijedi da je i $(A \vee B)$ formula u KNF obliku s ukupno jednom elementarnom konjunkcijom, tj. i $A \vee B$ je također poseban slučaj KNF-a. Svaki literal je također kao poseban slučaj u KNF obliku.

Definicija 1.3.5. *Disjunkciju elementarnih konjunkcija oblika*

$$(A_{11} \wedge A_{12} \wedge \dots) \vee (A_{21} \wedge A_{22} \wedge \dots) \vee (A_{31} \wedge A_{32} \wedge \dots) \vee \dots$$

s konačno puno zagrada i ukupno konačno puno literala A_{ij}, $i = 1, 2, \dots,$ $j = 1, 2, \dots$ nazivamo ***disjunktivna normalna forma*** *(skraćeno:* ***DNF****).*

Primjer 1.3.5. $(\neg P \wedge R \wedge \neg S \wedge T) \vee (P \wedge \neg R \wedge S) \vee (P \wedge \neg R)$, $(A \wedge A) \vee (A \wedge \neg A)$ su formule koje su u disjunktivnoj normalnoj formi.

Kako su A i B posebni slučajevi "jednočlanih" elementarnih konjunkcija, slijedi da je $(A) \vee (B)$ odnosno $A \vee B$ također poseban slučaj DNF-a.

Dalje, kako je $A \wedge B$ elementarna konjunkcija, slijedi da je i $(A \wedge B)$ formula u DNF obliku s ukupno jednom elementarnom konjunkcijom, tj. i $A \wedge B$ je također poseban slučaj DNF-a.

Formula oblika

$$(A_{11} \wedge A_{12} \wedge \ldots) \vee (A_{21} \wedge A_{22} \wedge \ldots) \vee (A_{31} \wedge A_{32} \wedge \ldots) \vee \ldots$$

ima vrijednost 1 ako i samo ako je bilo koja (bar jedna) od njenih zagrada, elementarnih konjunkcija vrijednosti 1. Iz tog razloga lako je za zadanu tablicu istinitosti, ako ne znamo od koje smo formule tu tablicu pronašli, pronaći bar jednu formulu kojoj bi ta tablica pripadala. Pronaći ćemo formulu u DNF-u za koju vrijedi da je zadana tablica njena tablica istinitosti. Jednostavno ćemo za svaki red koji završava s 1 zapisati jednu zagradu u kojoj je elementarna konjunkcija svih varijabli iz tablice, pri čemu ćemo varijable koje su jednake nula u tom redu negirati.

Primjer 1.3.6. Odredi neku formulu F čija je tablica dana s

Tablica 1.3.1: Za zadanu tablicu istinitosti pronađi njenu formulu.

P	R	S	F
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Rješenje. Formula F ima vrijednost 1 u prvom redu. Kreiramo $(\neg P \wedge \neg R \wedge \neg S)$ (minusi su ispred svih varijabli jer su i P i R i S u prvom redu nula, a formula oblika $A \wedge B \wedge C$ je 1 samo ako su i A i B i C jedan).
Formula F ima vrijednost 1 u trećem redu. Kreiramo $(\neg P \wedge R \wedge \neg S)$ (minusi su ispred

varijabli P i S jer su P i S u trećem redu nula).
Formula F ima vrijednost 1 u petom redu. Kreiramo $(P \wedge \neg R \wedge \neg S)$.
Formula F ima vrijednost 1 u sedmom redu. Kreiramo $(P \wedge R \wedge \neg S)$.

Ukupno za traženu formulu definiramo

$$F \equiv (\neg P \wedge \neg R \wedge \neg S) \vee (\neg P \wedge R \wedge \neg S) \vee (P \wedge \neg R \wedge \neg S) \vee (P \wedge R \wedge \neg S).$$

Čitamo: F će imati vrijednost 1 ako su i P i R i S nule (prvi red i prva zagrada) ili ($\vee$) ako je $P = 0$ i $R = 1$ i $S = 0$ ili ...

Zaključujemo: Ako za zadanu formulu logike sudova F želimo pronaći njoj logički ekvivalentnu formulu G koja je u disjunktivnoj normalnoj formi, prvo ćemo naći tablicu istinitosti formule F, a zatim za svaku jedinicu formule F iz tablice, kreirati po jednu zagradu u kojoj će biti sve varijable koje se pojavljuju u formuli F i pri tome ćemo ispred varijabli koje u promatranom redu imaju vrijednost nula postaviti negaciju. Ako je F antitautologija, tj. ima samo nule u svom stupcu tablice, ne možemo pomoću jedinica kreirati DNF. No, u tom slučaju uzet ćemo bilo koju varijablu V koja se pojavljuje u F i proglasiti $G \equiv V \wedge \neg V$.

Analogno, ako za zadanu formulu logike sudova F želimo pronaći njoj logički ekvivalentnu formulu G koja je u konjunktivnoj normalnoj formi, prvo ćemo naći tablicu istinitosti formule F, a zatim za svaku nulu formule F iz tablice, kreirati po jednu zagradu u kojoj će biti sve varijable koje se pojavljuju u formuli F i pri tome ćemo ispred varijabli koje u promatranom redu imaju vrijednost jedan postaviti negaciju. Ako je F tautologija, tj. ima samo jedinice u svom stupcu tablice, ne možemo pomoću nula kreirati KNF. Opet, u tom slučaju uzet ćemo bilo koju varijablu V koja se pojavljuje u F i proglasiti $G \equiv V \vee \neg V$.

Primjer 1.3.7. Odredi KNF i DNF formule $F \equiv (A \to B) \wedge (C \to A)$.

Rješenje.

Tablica 1.3.2: Odredi KNF i DNF zadane formule

A	B	C	F
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0

A	B	C	F
1	1	0	1
1	1	1	1

F ima četiri nule pa će njena KNF imati četiri zagrade, a i četiri jedinice, stoga će i DNF imati četiri zagrade.

$I(F) = 0$ u drugom, četvrtom, petom i šestom redu.
Stoga je

$$G \equiv (A \vee B \vee \neg C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee C) \wedge (\neg A \vee B \vee \neg C)$$

tražena KNF.

$I(F) = 1$ u prvom, trećem, sedmom i osmom redu.
Stoga je

$$H \equiv (\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)$$

tražena DNF.

Teorem koji kaže kako za svaku formulu logike sudova postoje formule G i H koje su joj logički ekvivalentne, a koje su u KNF i DNF, i njegov dokaz, nalaze se u knjizi *Matematička logika* navedenoj u početku ovog potpoglavlja.

Primjer 1.3.8. U formuli $A \wedge B = \neg(\neg A \vee \neg B)$ (jedna od De Morganovih[1] formula) uočavamo kako svaki nastup veznika "i" u bilo kojoj formuli logike sudova možemo zamijeniti korištenjem veznika $\vee$ i $\neg$. Kažemo da se veznik "i" može izraziti pomoću $\vee$ i $\neg$.

Definicija 1.3.6.

1. *Za skup veznika V kažemo da je* **potpun** *za $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ ako se svaki od veznika iz skupa $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ može izraziti pomoću veznika iz skupa V.*

2. *Za skup veznika V reći ćemo da je* **baza** *za skup $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ ako je potpun i ako se niti jedan veznik iz V ne može izraziti pomoću ostalih iz V.*

Primjer 1.3.9. Dokaži: Za proizvoljno zadanu formulu logike sudova F, postoji njoj ekvivalentna formula koja se sastoji samo od veznika $\neg$, $\wedge$.

[1] Augustus de Morgan (1806. – 1871.) – britanski matematičar i logičar koji se bavio algebrom, logikom i poviješću znanosti. Pridonio je razvoju simboličke logike te je definirao matematičku indukciju.

Rješenje. Do sada znamo kako se svaka formula može napisati u KNF ili DNF obliku, tj. samo pomoću tri veznika, $\neg$, $\wedge$ i $\vee$.
Kada bismo sada mogli pokazati i da se svaka pojava veznika $\vee$ može zamijeniti veznicima $\neg$ i $\wedge$, zadatak bi bio gotov.

No, upravo po De Morganovim formulama možemo zamijeniti $\wedge$ s $\vee$ i obrnuto:

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

Sve se, dakle, formule logike sudova mogu zapisati u njima ekvivalentnom obliku koristeći samo veznike iz skupova $\{\neg, \wedge, \vee\}$ ili $\{\neg, \wedge\}$. Kako druga De Morganova formula osigurava da se i veznik $\wedge$ može napisati pomoću $\neg$ i $\vee$, slijedi da je, na isti način kao gore, i skup $\{\neg, \vee\}$ dovoljan za prezentaciju svih formula logike sudova.

Primjer 1.3.10. Zapiši formulu $A \wedge (\neg B \vee C)$ koristeći samo veznike $\neg$ i $\vee$.

Rješenje.

$$A \wedge (\neg B \vee C) = \neg(\neg A \vee \neg(\neg B \vee C)).$$

Primjer 1.3.11. Zapiši formulu $A \wedge (\neg B \vee C)$ koristeći samo veznike $\neg$ i $\wedge$.

Rješenje.

$$A \wedge (\neg B \vee C) = A \wedge \neg(\neg\neg B \wedge \neg C) = A \wedge \neg(B \wedge \neg C).$$

Dalje, kako se $\neg$ ne može izraziti pomoću $\wedge$, a ni $\wedge$ pomoću $\neg$, a isto vrijedi i za $\vee$, skupovi $\{\neg, \vee\}$ i $\{\neg, \wedge\}$ su baze za skup svih veznika logike sudova. Jer, svi se veznici mogu zapisati pomoću veznika iz skupa $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$, a svaki se od tih veznika može zapisati samo pomoću $\neg$ i $\wedge$ (ili samo pomoću $\neg$ i $\vee$). $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$ je potpun skup za skup svih veznika, a $\{\neg, \vee\}$ je baza za $\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow\}$. Dakle, $\{\neg, \vee\}$ je baza za sve veznike.

Zanimljivo je da postoje i jednočlane baze za skup svih propozicionalnih veznika logike sudova. To su $\{\uparrow\}$ i $\{\downarrow\}$.

Veznik $\uparrow$ zove se veznik "ni" ili Shefferova[2] operacija i zadan je tablicom na sljedeći način:

Tablica 1.3.3

A	B	$A \uparrow B = \neg(A \wedge B)$
0	0	1
0	1	1
1	0	1
1	1	0

[2]Henry Maurice Sheffer (1882. – 1964.) – američki logičar

Ostali se veznici mogu dobiti pomoću veznika $\uparrow$ na sljedeći način:

$$\neg A = A \uparrow A.$$

Kako je $A \uparrow B = \neg(A \wedge B)$, slijedi (negacijom tog reda) da je

$$A \wedge B = \neg(A \uparrow B) = (\text{zbog prve formule}) = (A \uparrow B) \uparrow (A \uparrow B).$$

Dalje,

$$\begin{aligned} A \vee B &= (\text{po De Morganu}) = \neg(\neg A \wedge \neg B) = (A \uparrow A) \uparrow (B \uparrow B), \\ A \to B &= A \uparrow (B \uparrow B) = A \uparrow (A \uparrow B), \\ A \leftrightarrow B &= (A \uparrow A) \uparrow (B \uparrow B) \uparrow (A \uparrow B). \end{aligned}$$

Veznik $\downarrow$ zove se veznik "nili" ili Lukasiewiczeva[3] operacija ili Peirceova[4] strijela ili Quineov[5] bodež i zadan je tablicom na sljedeći način:

Tablica 1.3.4

A	B	$A \downarrow B = \neg(A \vee B)$
0	0	1
0	1	0
1	0	0
1	1	0

Dovoljno je sada pokazati da se Shefferova operacija može izraziti pomoću Lukasiewiczeve i bit će jasno da se onda svaki od naših pet veznika može izraziti pomoću Lukasiewiczeve operacije. To prepuštamo čitatelju, odnosno riješeno je u sklopu zadatka 1.3.3.

[3]Jan Łukasiewicz (1878. – 1956.) – poljski logičar koji je tvorac trovalentne logike i novog logičkog simbolizma.

[4]Charles Sanders Peirce (1839. – 1914.) – američki filozof, logičar i znanstvenik koji razvijao teoriju vjerojatnosti i simboličku logiku te je utemeljio pragmatizam u američkoj filozofiji.

[5]Willard Van Orman Quine (1908. – 2000.) – američki filozof koji se zalagao da se logika odijeli kao neovisna disciplina od filozofije.

Zadaci za vježbu

Zadatak 1.3.1. Odredi konjunktivnu i disjunktivnu formu formule

$$(A \to B) \land (B \to A).$$

Zadatak 1.3.2. Zapiši veznike iz skupa $\{\neg, \land, \lor, \to\}$ pomoću veznika $\downarrow$.

Zadatak 1.3.3. Zapiši veznik $\downarrow$ pomoću veznika $\uparrow$ i obrnuto.

Zadatak 1.3.4. Zapiši formulu $A \to (C \land \neg B)$ samo pomoću:

a) veznika iz skupa $\{\neg, \land\}$,

b) veznika iz skupa $\{\neg, \lor\}$,

c) veznika $\uparrow$.

Rješenja

1.3.1.

A	B	$A \to B$	$B \to A$	$(A \to B) \land (B \to A)$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

KNF: $G = (A \lor \neg B) \land (\neg A \lor B)$
DNF: $H = (\neg A \land \neg B) \lor (A \land B)$

1.3.2.

1. $\neg A = A \downarrow A$.
2. $A \downarrow B = \neg(A \lor B)$. Dakle, $A \lor B = \neg(A \downarrow B) = (A \downarrow B) \downarrow (A \downarrow B)$.
3. $A \land B = \neg(\neg A \lor \neg B) = \neg A \downarrow \neg B = (A \downarrow A) \downarrow (B \downarrow B)$.
4. $A \to B = \neg A \lor B = (\neg A \downarrow B) \downarrow (\neg A \downarrow B) = (A \downarrow A \downarrow B) \downarrow (A \downarrow A \downarrow B)$.

1.3.3. $A \downarrow B = \neg(A \vee B) =$

$$= \big(\text{po De Morganu}\big) = \neg A \wedge \neg B =$$
$$= \big(\text{jer } A \wedge B = \neg(A \uparrow B)\big) = \neg(\neg A \uparrow \neg B) =$$
$$= \neg\big((A \uparrow A) \uparrow (B \uparrow B)\big) =$$
$$= \big((A \uparrow A) \uparrow (B \uparrow B)\big) \uparrow \big((A \uparrow A) \uparrow (B \uparrow B)\big)$$

$A \uparrow B = \neg(A \wedge B) =$

$$= \big(\text{po De Morganu}\big) = \neg A \vee \neg B =$$
$$= \big(\text{jer } A \vee B = \neg(A \downarrow B)\big) = \neg(\neg A \downarrow \neg B) =$$
$$= \neg\big((A \downarrow A) \downarrow (B \downarrow B)\big) =$$
$$= \big((A \downarrow A) \downarrow (B \downarrow B)\big) \downarrow \big((A \downarrow A) \downarrow (B \downarrow B)\big)$$

1.3.4. a) $A \to (C \wedge \neg B) = \neg A \vee (C \wedge \neg B) = \neg\big(A \wedge \neg(C \wedge \neg B)\big)$

b) $A \to (C \wedge \neg B) = \neg A \vee \neg(\neg C \vee B)$

c) $A \to (C \wedge \neg B) = A \uparrow \big(A \uparrow (C \wedge \neg B)\big) =$

$$= A \uparrow \Big(A \uparrow \big(C \wedge (B \uparrow B)\big)\Big) =$$
$$= A \uparrow \Big(A \uparrow \Big(\big(C \uparrow (B \uparrow B)\big) \uparrow \big(C \uparrow (B \uparrow B)\big)\Big)\Big)$$

1.4. Sudovne jednadžbe

U ovom dijelu gradiva vidjet ćemo kako i sud može biti rješenje jednadžbe, naravno, one koja je napisana jezikom logike sudova i u kojoj je nepoznanica traženi sud koji mora udovoljavati zadanim uvjetima.

Iz ovog potpoglavlja čitatelj će naučiti konstruirati sud koji je potreban da bi određeni zadani logički izraz ili grupa logičkih izraza imala unaprijed zadana tražena svojstva.

Literatura za 1.4. sljedeće su knjige i skripte:

1. R. Cori, D. Lascar, *Mathematical logic: a course with exercises (Part I)*, Oxford University Press, 2000.

2. M. Vuković, *Matematička logika*, Element, Zagreb, 2009.

3. M. Vuković, *Matematička logika 1*, skripta.
http://www.mathos.unios.hr/logika/Logika_skripta.pdf (zadnji pristup travanj 2022.)

Primjer 1.4.1. Odredi formulu X za koju je formula $(X \vee P) \leftrightarrow (X \vee R)$ tautologija.

Rješenje.

Tablica 1.4.1: Sudovna jednadžba

P	R	X	$(X \vee P) \leftrightarrow (X \vee R)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Uočavamo:
Za $I(P) = 0$, $I(R) = 0$, bez obzira je li $I(X) = 0$ ili $I(X) = 1$, zadana formula je svakako tautologija, tj. ima vrijednost 1 (prva dva reda tablice).
Za $I(P) = 0$, $I(R) = 1$, mora biti $I(X) = 1$ jer za $I(X) = 0$, zadana formula ima vrijednost 0 (druga dva reda tablice).
Za $I(P) = 1$, $I(R) = 0$, mora biti $I(X) = 1$ jer za $I(X) = 0$, zadana formula ima vrijednost 0 (treća dva reda tablice).
Na kraju, za $I(P) = 1$, $I(R) = 1$, bez obzira je li $I(X) = 0$ ili $I(X) = 1$, zadana formula je svakako tautologija, tj. ima vrijednost 1 (zadnja dva reda tablice).

Sve skupa:

Tablica 1.4.2: Kakav mora biti X obzirom na P i R.

P	R	X
0	0	0 ili 1
0	1	1
1	0	1
1	1	0 ili 1

Kako možemo birati prvu i zadnju vrijednost za X, odaberimo

Tablica 1.4.3: Odabir pogodnog X-a

P	R	X
0	0	0
0	1	1
1	0	1
1	1	1

jer takav X je očito $X = P \vee R$.
Provjerimo dobiveno rješenje: uvrstimo $X = P \vee R$ u početnu formulu. Dobivamo

$$\begin{aligned}(X \vee P) \leftrightarrow (X \vee R) &\Leftrightarrow (P \vee R \vee P) \leftrightarrow (P \vee R \vee R) \Leftrightarrow \\ &\Leftrightarrow (P \vee R) \leftrightarrow (P \vee R)\end{aligned}$$

što je očito tautologija.

U slučaju da tablicu za X nismo odabrali tako da formula za X bude očita, npr. uzmemo li za X

Tablica 1.4.4: Odabir drugačijeg X-a

P	R	X
0	0	0
0	1	1
1	0	1
1	1	0

možemo naći X u konjunktivnoj ili disjunktivnoj normalnoj formi.
Odaberimo ovdje KNF: $X \equiv (P \vee R) \wedge (\neg P \vee \neg R)$. I ovo je rješenje dobro.

Ako ovakva sudovna jednadžba ima rješenje, npr. formulu X, onda je i

$$X \vee 0 \Leftrightarrow X \vee (\neg P \wedge P)$$

također rješenje pa je jasno kako sudovne jednadžbe ili nemaju rješenja ili imaju beskonačno puno rješenja.

Primjer 1.4.2. Odredi formulu X za koju će F i G biti logički ekvivalentne, ako je

$$\begin{aligned}F &\equiv (X \vee A) \rightarrow (\neg X \wedge B),\\ G &\equiv A \vee B.\end{aligned}$$

Rješenje.

Tablica 1.4.5: Sudovna jednadžba s logički ekvivalentnim formulama

A	B	X	F	G
0	0	0	1	0
0	0	1	0	0
0	1	0	1	1
0	1	1	0	1
1	**0**	**0**	**0**	**1**
1	**0**	**1**	**0**	**1**
1	1	0	1	1
1	1	1	0	1

Tablica 1.4.6: Kakav mora biti X s obzirom na A i B.

A	B	X
0	0	1
0	1	0
1	**0**	**-**
1	1	0

U deblje označenom petom i šestom redu tablice 1.4.5, $I(F) = 0$ i $I(G) = 1$ u oba reda bez obzira na vrijednost formule X, ili, bez obzira koliki je X, F i G, ne mogu biti logički ekvivalentne formule, tj. zadana jednadžba "nema rješenja".

Zadaci za vježbu

Zadatak 1.4.1. Odredi formulu X za koju će formule

$$
\begin{aligned}
F &\equiv A \wedge X \\
G &\equiv \neg A \wedge \neg B \wedge \neg X \\
H &\equiv \neg A \wedge B \wedge X
\end{aligned}
$$

biti antitautologije.

Zadatak 1.4.2. Odredi X za kojeg je

$$X \to (P \to R) \Leftrightarrow (P \to R) \to X.$$

Zadatak 1.4.3. Riješi sustav jednadžbi

$$\begin{aligned} P \wedge X \to Q \wedge Y &\Leftrightarrow X \to Y \\ P \wedge X &\Leftrightarrow Q \wedge Y \\ P \wedge Q \to X &\Leftrightarrow Y \to (P \vee Q), \end{aligned}$$

gdje su P i Q propozicionalne varijable, a X i Y nepoznate formule.

Rješenja

1.4.1.

Tablica 1.4.7: Sudovna jednadžba s antitautologijama

A	B	X	$F \equiv A \wedge X$	$G \equiv \neg A \wedge \neg B \wedge \neg X$	$H \equiv \neg A \wedge B \wedge X$
0	0	0	0	1	0
0	0	1	0	0	0
0	1	0	0	0	0
0	1	1	0	0	1
1	0	0	0	0	0
1	0	1	1	0	0
1	1	0	0	0	0
1	1	1	1	0	0

Tablica 1.4.8: Kakav mora biti X s obzirom na A i B.

A	B	X
0	0	1
0	1	0
1	0	0
1	1	0

Odmah se nameće rješenje $X \equiv \neg(A \vee B) = A \downarrow B = \neg A \wedge \neg B$, itd.

1.4.2.

Tablica 1.4.9: Sudovna jednadžba s implikacijama

P	R	X	$X \to (P \to R)$	$(P \to R) \to X$
0	0	0	1	0
0	0	1	1	1
0	1	0	1	0
0	1	1	1	1
1	0	0	1	1
1	0	1	0	1
1	1	0	1	0
1	1	1	1	1

Tablica 1.4.10: Kakav mora biti X s obzirom na P i R.

P	R	X
0	0	1
0	1	1
1	0	0
1	1	1

Odmah se nameće rješenje $X \equiv P \to R$ koje nas uvrštavanjem odmah uvjerava u ekvivalentnost dviju očitih tautologija.

1.4.3.

Tablica 1.4.11: Sustav sudovnih jednadžbi

P	Q	X	Y	$P \wedge X \to Q \wedge Y$	$X \to Y$	$P \wedge X$	$Q \wedge Y$	$P \wedge Q \to X$	$Y \to (P \vee Q)$
0	0	0	0	1	1	0	0	1	1
0	0	0	1	1	1	0	0	1	0
0	0	1	0	1	0	0	0	1	1
0	0	1	1	1	1	0	0	1	0
0	1	0	0	1	1	0	0	1	1

P	Q	X	Y	$P \wedge X \to Q \wedge Y$	$X \to Y$	$P \wedge X$	$Q \wedge Y$	$P \wedge Q \to X$	$Y \to (P \vee Q)$
0	1	0	1	1	1	0	1	1	1
0	1	1	0	1	0	0	0	1	1
0	1	1	1	1	1	0	1	1	1
1	0	0	0	1	1	0	0	1	1
1	0	0	1	1	1	0	0	1	1
1	0	1	0	0	0	1	0	1	1
1	0	1	1	0	1	1	0	1	1
1	1	0	0	1	1	0	0	0	1
1	1	0	1	1	1	0	1	0	1
1	1	1	0	0	0	1	0	1	1
1	1	1	1	1	1	1	1	1	1

Tablica 1.4.12: Kakvi moraju biti X i Y s obzirom na P i Q.

P	Q	X	Y
0	0	0	0
0	1	0	0
1	0	0	0 ili 1
1	1	1	1

Konačno je $X = P \wedge Q$, $Y = P$ jedno rješenje.
Drugo elegantno rješenje je $X = Y = P \wedge Q$.

1.5. Prirodna dedukcija

Cilj je ovog potpoglavlja pokazati što su teorem i dokaz te što je formalno teorem i što je njegov dokaz (izvod teorema).
Nakon ovog potpoglavlja čitatelj će, koristeći sustav prirodne dedukcije, znati dokazati neku formulu na osnovu zadanih formula.

Literatura za 1.5. sljedeće su knjige i skripte:

1. R. Cori, D. Lascar, *Mathematical logic: a course with exercises (Part I)*, Oxford

University Press, 2000.

2. M. Vuković, *Matematička logika*, Element, Zagreb, 2009.

3. M. Vuković, *Matematička logika 1*, skripta.
http://www.mathos.unios.hr/logika/Logika_skripta.pdf (zadnji pristup travanj 2022.)

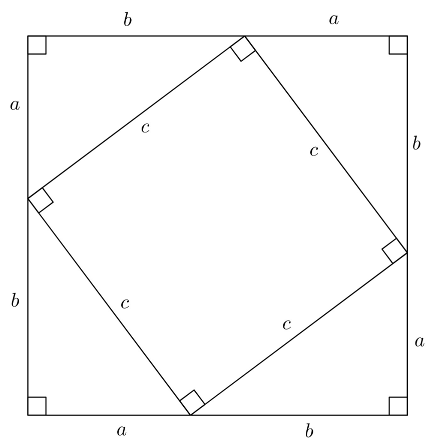
U matematici, važnu i lijepu istinu zovemo teorem. "Manju" takvu tvrdnju zovemo propozicija. Posljedicu teorema, također "manje važnu" tvrdnju, zovemo korolar, a pripremnu manju tvrdnju koju ćemo najčešće koristiti kasnije u dokazu nekog teorema zovemo lema.

Teoreme, leme, korolare i propozicije dokazujemo. Matematički dokaz je "obrazloženje" zašto je dana tvrdnja istinita. Polazimo od jednostavnih i lako shvatljivih istina ili polazimo od nečega za što već znamo da je istina ili polazimo od aksioma za koje ne možemo znati jesu ili istina ili ne, ali su toliko jednostavni da ih po dogovoru prihvaćamo za istinite, i kombinacijom svega gore navedenoga nizom zaključaka dobivamo iskaz (potvrdu) "važne zadane tvrdnje".

Dokazati nešto znači u stvari krenuti od zadane već dokazane sigurne istine, koristiti zadana pravila i doći do druge istine za koju tada kažemo da je dokazana.

Primjer 1.5.1. Teorem (Pitagorin): *Ako su a i b duljine kateta, a c duljina hipotenuze pravokutnog trokuta, onda vrijedi $a^2 + b^2 = c^2$.*

Dokaz 1. Zadani pravokutni trokut proširimo produljenjem kateta do kvadrata sa stranicom $a + b$, kao na slici.



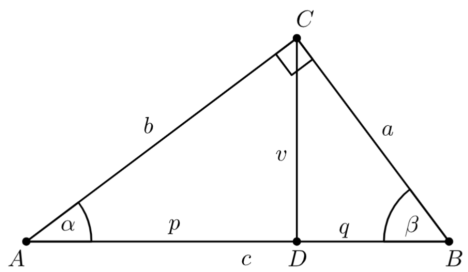
U velikom kvadratu sa stranicom $a+b$ nalazi se također kvadrat, sa stranicom c. Radi se zaista o kvadratu (premda to možda i nije odmah očito) budući da su mu suprotne stranice paralelne jer pravci na kojima se nalaze pod istim kutom sijeku stranice velikog kvadrata, a unutrašnji kutovi su mu 90° jer su dva kuta uz njih ukupno 90°.

Sada se veliki kvadrat sastoji od četiriju malih pravokutnih trokuta i unutrašnjeg kvadrata, tj.

$$\begin{aligned}(a+b)^2 &= 4\cdot\frac{ab}{2}+c^2\\ a^2+2ab+b^2 &= 2ab+c^2\\ a^2+b^2 &= c^2.\end{aligned}$$

Zadani Pitagorin teorem dokazali smo tako što smo se sjetili zgodne slike iz koje smo, koristeći neke tvrdnje iz osnova geometrije i osnova algebre iz osnovne škole, direktno dokazali traženu relaciju. □

Dokaz 2. Na početku opet moramo krenuti od nečega što već znamo.



Euklidov poučak za pravokutni trokut ABC, čije su katete a i b i hipotenuza c, uz oznake kao na slici, gdje je v visina iz vrha C na hipotenuzu kaže:

$$a=\sqrt{qc},\quad b=\sqrt{pc}.$$

Dakle,

$$a^2+b^2=qc+pc=(q+p)c=c\cdot c=c^2.$$

Pitagorin teorem dokazali smo tako što smo pošli od Euklidovog teorema, uvrstili njegove tvrdnje u a^2+b^2 i koristili pravilo distributivnosti množenja prema zbrajanju. □

Kao što logiku sudova ne zanimaju sve riječi zadanog alfabeta (tablice istinitosti, KNF, DNF, jednadžbe sa sudovima, …, sve smo to radili samo s posebnim i smislenim riječima koje nazivamo formule), tako znanost zanimaju samo one rečenice, samo oni sudovi koji su istiniti. Tautologije su matematici ili računalstvu važnije nego oborive formule ili antitautologije.

Stoga, zbog zahtjeva "izvana", logika se posebno bavi tautologijama ili valjanim formulama: kako ih sve naći, kako za formulu dokazati da je tautologija, kako iz jedne tautologije dobiti drugu, itd.

Jedan od najzanimljivijih postupaka (načina razmišljanja) kako od zadanih tautologija dobiti nove tautologije, i samo tautologije i sve tautologije, zove se sustav prirodne dedukcije.

Na početku ćemo imati zadan skup pretpostavki, skup $S = \{F_1, F_2, \ldots, F_k\}$. Cilj će nam biti dokazati neku novu formulu koristeći te pretpostavke (uzimajući ih kao istinite) i koristeći dolje navedena pravila zaključivanja.

"Iz skupa $\{F_1, F_2, \ldots, F_k\}$ zaključujemo formulu F" zapisat ćemo s

$$\{F_1, F_2, \ldots, F_k\} \vdash_{(PD)} F.$$

U ovom ćemo se paragrafu također upoznati s pojmom teorema i dokaza.

Sustav prirodne dedukcije zadan je sljedećim pravilima:

1. $\dfrac{F \wedge G}{F}\,(\wedge I)$

   Crta znači da od formule iznad crte možemo zaključiti formulu ispod crte. Naravno, ako je točno $F \wedge G$, onda je točno i F. Pored crte u zagradi ime je pravila $(\wedge I)$, što znači veznik $\wedge$ izbacujemo (I).

2. $\dfrac{F \wedge G}{G}\,(\wedge I)$

3. $\dfrac{F}{F \vee G}\,(\vee U)$

   Ovo pravilo zove se $\vee U$ jer $\vee$ uvodimo u formulu. Na prirodan način, naravno, jer ako je F istina, onda je sigurno i $F \vee G$ istina kakav god bio G.

4. $\dfrac{G}{F \vee G}\,(\vee U)$

5. $\dfrac{F \quad G}{F \wedge G}\,(\wedge U)$

   Ako su i F i G istinite, onda je sigurno istinita i formula $F \wedge G$. (Iza ovoga stoji u stvari $\{F, G\} \models F \wedge G$ tj. $\{F, G\} \Rightarrow F \wedge G$.)

6. $\dfrac{F \quad \neg F}{0}\,(\neg I)$

   Ako iz nekog postupka zaključimo kako vrijedi i formula F i formula $\neg F$, onda možemo zaključiti da to nije moguće, tj. zaključujemo laž koju ćemo označiti kao u tablicama istinitosti s 0.

7. $$\frac{\neg\neg F}{F}\,(DN)$$

DN znači dvojna negacija. Dvostruko negiran F iste je vrijednosti kao i F.

8. $$\frac{F \qquad F \to G}{G}\,(\to I)$$

9. $$\frac{F \leftrightarrow G}{F \to G}\,(\leftrightarrow I)$$

10. $$\frac{F \leftrightarrow G}{G \to F}\,(\leftrightarrow I)$$

11. $$\frac{F \to G \qquad G \to F}{G \leftrightarrow F}\,(\leftrightarrow U)$$

12. $$\begin{array}{ccc} & \overline{F}^{\,n} & \overline{G}^{\,m} \\ & \vdots & \vdots \\ F \vee G & H & H \\ \hline & H & \end{array}\ {}_{n,m}(\vee I)$$

Ovo pravilo najčešće koristimo kada se želimo riješiti disjunkcije. Značenje je postupka sljedeće:
Ako znamo da je $F \vee G$ točno, onda možemo pretpostaviti da je točna ili formula F i posebno, odvojeno, ili da je točna G. Ako pod pretpostavkom da je F točna dobivamo zaključak (npr. nekim preostalim pravilima) H, i ako pod pretpostavkom da je G točna dobivamo isti zaključak H, jasno je da ako je točna formula $F \vee G$, onda je točna H.
Potez iznad formule F, u ovom i sljedećim pravilima, i pokraj poteza broj n govori nam kako u izvodu samo pretpostavljamo da je F točna, i to nam je n-ta pretpostavka u izvodu. Ovaj broj važan je jer nas podsjeća da "otvorenu" pretpostavku moramo i zatvoriti i to kao i zagrade u matematici koje su jedna unutar druge ili kao petlje u programiranju koje su također jedna unutar druge. Pretpostavku moramo zatvoriti prije zaključka koji se na nju odnosi. To su oznake m i n desno od crte prije zaključka H.

13. $$\begin{array}{c} \overline{F}^{\,n} \\ \vdots \\ 0 \\ \hline \neg F \end{array}\ {}_{n}(\neg U)$$

I ovo je pravilo jasno: Ako pretpostavimo da vrijedi formula F, i iz te pretpostavke dobijemo laž, naravno da onda F nije istina, tj. istina je $\neg F$. Ili, $F \to 0 \Leftrightarrow \neg F$.

14.
$$\dfrac{\begin{matrix}\overline{F}^{\,n}\\ \vdots \\ G\end{matrix}}{F \to G}\;{}_n(\to U)$$

Ako pretpostavimo da vrijedi formula F, i iz te pretpostavke dobijemo formulu G, vrijedi $F \to G$. Prije zaključka $F \to G$ zatvaramo pretpostavku F (malo n desno od crte zaključka).

Primjer 1.5.2. Dokaži: $\{P \wedge R, R \to S\} \vdash_{(PD)} S$.

Rješenje. Zadatak nam kaže, točnije, da treba dokazati da ako su $P \wedge R$ i $R \to S$ istinite formule, onda je uz pravila prirodne dedukcije i S istinita formula.

Sada dolazi najzanimljiviji dio: treba, polazeći od formula iz zadanog skupa, složiti konstrukciju (ta konstrukcija zove se dokaz formule S iz skupa pretpostavki $\{P \wedge R,\ R \to S\}$ primjenom pravila sustava prirodne dedukcije) koja će završiti formulom S. U tom postupku treba prvo pažljivo čitati zadane formule i formulu koju treba dokazati dok ne shvatimo kako izgraditi dokaz. No, ovaj je primjer lagan: Ako znamo da je zima i da je danas petak, a znamo i da petkom idemo na fitnes, lako je dokazati da danas idemo na fitnes. Iz $P \wedge R$, slijedi da vrijedi R po pravilu 2. Kako vrijedi R, a pretpostavka je $R \to S$, odmah je po pravilu 8. jasno da vrijedi S. Ovo je u stvari bio spomenuti dokaz.

U nekim knjigama dokaz je proveden po koracima, tj. na sljedeći način:

1. $P \wedge R$ (pretpostavka)

2. $P \wedge R \to R$ (pravilo izvoda 2.)

3. R (iz 1. i 2. pravilom 8.)

4. $R \to S$ (pretpostavka)

5. S (iz 3. i 4. pravilom 8.)

I ovo je bio dokaz, u drugačijem obliku.

No, smatramo kako je nešto lakše pronaći izvod tražene formule pomoću sheme, kao što smo zadali i gornja pravila 1. do 14. na sljedeći način:

$$\dfrac{\dfrac{P \wedge R}{R}\,(\wedge I) \qquad R \to S}{S}\,(\to I)$$

I ova je shema također, treća vrsta dokaza.

Primjer 1.5.3. Dokaži: $\{P \land R \to S \land V, R, \neg\neg P\} \vdash V$.

Rješenje. Dokažimo na sva tri načina (tekstom, zaključcima navedenima po rednim brojevima i shemom izvoda kao kod pravila gore) željenu formulu V.

Prva pretpostavka kaže da ako imamo i P i R, onda se može dokazati S i V.
R već imamo zadano. No, nemamo P nego $\neg\neg P$. Očito ćemo P dobiti iz $\neg\neg P$ pravilom 7. koje kaže kako je dvostruka negacija jednaka afirmaciji. Iz $P \land R$, dobit ćemo $S \land V$, a onda i samo V iz $S \land V$ pravilom 2.

Ili:

1. $\neg\neg P$ (pretpostavka)
2. $\neg\neg P \to P$ (pravilo izvoda)
3. P (iz 1. i 2. pravilom 8.)
4. R (pretpostavka)
5. $P \land R$ (iz 3. i 4. pravilom 5.)
6. $P \land R \to S \land V$ (pretpostavka)
7. $S \land V$ (iz 5. i 6. pravilom 8.)
8. V (iz 7. pravilom 2.)

Rješenje pomoću sheme odnosno grafa izvoda:

$$\dfrac{\dfrac{\dfrac{\neg\neg P}{P}\,{\scriptstyle (DN)} \qquad R}{P \land R}\,(\land U) \qquad P \land R \to S \land V}{\dfrac{S \land V}{V}\,(\land I)}\,(\to I)$$

Na svaku od crta, kao pretpostavku za zaključak koji će slijediti ispod crte, možemo postaviti ili pretpostavku iz zadanog skupa pretpostavki ili nešto što smo već dokazali (ili pretpostavili) u istom izvodu.

Ukupno, nakon ovih dvaju primjera uočavamo:

Iznad crte (koja znači iz pretpostavki iznad dobit ćemo nekim od 14 pravila zaključak ispod), možemo postaviti:

- nešto od pretpostavki iz zadanog skupa pretpostavki;
- nešto što pretpostavljamo po nekom od pravila 12., 13. ili 14.;
- nešto što smo u dosadašnjem dijelu postupka dokazali;
- nešto što smo u dosadašnjem dijelu dokaza pretpostavili, a pretpostavku nismo zatvorili.

Na kraju, ne zaboravimo kako zadnji red mora obavezno biti tvrdnja koju dokazujemo.

Primjer 1.5.4. Dokaži $\{\} \vdash A \vee \neg A$. Tj., bez ikakvih pretpostavki u skupu S, dokaži da vrijedi $A \vee \neg A$.

Rješenje.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{^{1}}
\UnaryInfC{$\neg(A \vee \neg A)$}
\AxiomC{$\overline{A}^2$}
\RightLabel{$(\vee U)$}
\UnaryInfC{$A \vee \neg A$}
\RightLabel{$(\neg I)$}
\BinaryInfC{O}
\RightLabel{$_2(\neg U)$}
\UnaryInfC{$\neg A$}
\RightLabel{$(\vee U)$}
\UnaryInfC{$A \vee \neg A$}
\AxiomC{}
\RightLabel{^{1}}
\UnaryInfC{$\neg(A \vee \neg A)$}
\RightLabel{$(\neg I)$}
\BinaryInfC{O}
\RightLabel{$_1(\neg U)$}
\UnaryInfC{$\neg\neg(A \vee \neg A)$}
\RightLabel{(DN)}
\UnaryInfC{$A \vee \neg A$}
\end{prooftree}
$$

Definicija 1.5.1. *Ako je formula F dokaziva iz praznog skupa, tj. vrijedi $\vdash_{(PD)} F$, kažemo da je F **teorem sustava prirodne dedukcije**. U tom slučaju, formulu F zovemo **teorem sustava prirodne dedukcije**, a za izvod formule F kažemo da je **dokaz** tog teorema.*

Za sustav prirodne dedukcije vrijede sljedeći teoremi čiji se dokazi mogu naći u knjizi *Matematička logika* (navedenoj na početku ovog potpoglavlja):

Teorem 1.5.1. (Teorem adekvatnosti za sustav prirodne dedukcije)
Ako vrijedi $\vdash_{(PD)} F$, onda je F tautologija, tj. valjana formula.

Drugim riječima, sustav prirodne dedukcije daje samo valjane formule. (Sustav prirodne dedukcije jest adekvatan, "prikladan", za dobivanje tautologija.)
Vrijedi i općenitija tvrdnja: Ako vrijedi $S \vdash_{(PD)} F$, tada vrijedi $S \models F$, tj. F logički slijedi iz skupa S.

Korolar 1.5.1. (Teorem konzistentnosti za sustav prirodne dedukcije)
Sustav prirodne dedukcije jest konzistentan, tj. iz njega ne možemo izvući i neku formulu i njenu negaciju.

Teorem 1.5.2. (Teorem potpunosti za sustav prirodne dedukcije)
Ako je formula F tautologija, onda za F postoji dokaz u sustavu prirodne dedukcije tj. F je teorem sustava prirodne dedukcije.

ZADACI ZA VJEŽBU

Zadatak 1.5.1. Dokaži $\vdash_{(PD)} F \to (G \to F)$.

Zadatak 1.5.2. Dokaži: $\vdash_{(PD)} P \to (P \vee Q)$.

Zadatak 1.5.3. Dokaži: $(P \vee Q) \to R \vdash_{(PD)} P \to R$.

Zadatak 1.5.4. Dokaži: $\vdash_{(PD)} (A \to B) \to \neg(A \wedge \neg B)$.

Veći broj ovakvih zadataka čitatelj može naći u knjizi *Matematička logika* navedenoj na početku ovog potpoglavlja.

RJEŠENJA

1.5.1.

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{F}^{\,1} \qquad \overline{G}^{\,2}}{F \wedge G}\,(\wedge U)}{F}\,(\wedge I)}{G \to F}\,{}_2(\to U)}{F \to (G \to F)}\,{}_1(\to U)$$

1.5.2.

$$\dfrac{\dfrac{\overline{P}^{\,1}}{P \vee Q}\,(\vee U)}{P \to (P \vee Q)}\,{}_1(\to U)$$

1.5.3.

$$\dfrac{\dfrac{\dfrac{\overline{P}^{\,1}}{P \vee Q}\,(\vee U) \qquad (P \vee Q) \to R}{R}\,(\to I)}{P \to R}\,{}_1(\to U)$$

1.5.4.

$$\cfrac{\cfrac{\cfrac{\cfrac{\overline{A \to B}^{\,1} \qquad \cfrac{\overline{A \land \neg B}^{\,2}}{A}\,(\land I)}{B}\,(\to I) \qquad \cfrac{A \land \neg B}{\neg B}\,(\land I)}{O}\,(\neg I)}{\neg(A \land \neg B)}\,{}_2(\neg U)}{(A \to B) \to \neg(A \land \neg B)}\,{}_1(\to U)$$

1.6. Logika prvog reda

Cilj je ovog potpoglavlja predstaviti logiku prvog reda, jaču i složeniju (aparaturu za modeliranje izjava iz matematike, logike, ...) od logike sudova.

Nakon ovog potpoglavlja čitatelj će koristiti formule logike prvog reda za modeliranje jednostavnijih matematičkih tvrdnji te će razumjeti problem traženja modela za zadanu formulu logike prvog reda.

Literatura za 1.6. sljedeće su knjige i skripte:

1. R. Cori, D. Lascar, *Mathematical logic: a course with exercises (Part I)*, Oxford University Press, 2000.
2. M. Vuković, *Matematička logika*, Element, Zagreb, 2009.
3. M. Vuković, *Matematička logika 1*, skripta. http://www.mathos.unios.hr/logika/Logika_skripta.pdf (zadnji pristup travanj 2022.)

U dosadašnjem dijelu knjige istraživali smo logiku sudova ili propozicionalnu logiku ili logiku izjava. Tako se zove jer osnovni (najsitniji, atomarni) dio te logike jest izjava ili sud i ne dozvoljava detaljnije raščlanjivanje svojih rečenica, tj. nije moguća dublja, detaljnija analiza rečenica. Iz izjava $A =$ "Danas je petak." i $B =$ "Pada kiša.", slažemo izjave oblika $A \land B$, $A \lor B \to B$, itd. Elementarnu izjavu "Pada kiša." više ne možemo analizirati dalje. Možemo joj eventualno samo nešto dodati i stvoriti složenu izjavu.

Logika prvog reda često se naziva u literaturi predikatna logika. Iz osnovne škole sjećamo se kako je predikat dio rečenice koji govori što subjekt radi ili što se sa subjektom događa. Predikatna logika, dakle, na jedan način ulazi unutar rečenice, u strukturu rečenice. Kod logike prvog reda možemo detaljnije i "finije" analizirati zadane sudove.

Neka je P podskup skupa svih stvari (ili bića), tj. skup svih onih stvari (ili bića) koje padaju (npr. upravo sada, bar negdje na svijetu). S $P(x)$ označimo izjavu “x ima svojstvo P.”, tj. svojstvo da pada. $P(x)$ je drugi zapis za $x \in P$.

Neka je $P = \{$meteor, led, kiša, jabuka, zrakoplov, padobranac, lišće$\}$.
Pitamo se ima li kiša svojstvo da pada. Odgovor je DA jer kiša $\in P$. $P($kiša$)$ ili drugačije napisano kiša $\in P$ ili “Pada kiša” je istinita izjava.

“Pada standard.” nije istinita izjava jer standard nije element skupa P. Kiša i standard ovdje su neki elementi skupa “svih stvari”, općenito, neke konstantne stvari pa ćemo ono što zamijeni varijablu x, zvati konstanta (i u osnovnoj školi u npr. $f(x) = 2x + 3$ uvrštavamo konstantu 14 kako bismo izračunali $f(14) = 2 \cdot 14 + 3 = 31$ itd.).

Je li općenito $P(x)$ istinita izjava? Očito to ne možemo znati dok ne znamo što je x i koji su elementi skupa P. Dakle, za zadanu formulu predikatne logike $P(x)$, mi ne znamo je li ta formula istinita ili lažna dok ne “uvrstimo” nešto iz skupa svih stvari, skupa M, umjesto varijable x. Taj postupak davanja značenja određenoj varijabli zovemo valuacija. Za zadanu formulu $P(x)$ interpretiranje i relacije P i elementa x zovemo interpretacija (formule $P(x)$).

Ako je M skup svih europskih država, a predikat P čine sve države čije ime na hrvatskom jeziku započinje slovom P, onda formula $P(x)$ nije niti istinita niti neistinita (nije tautologija niti antitautologija). Ispunjiva je jer za $x =$ Portugal, $P(x)$ je istinita formula. Oboriva je jer za $x =$ Island, $P(x)$ je neistinita formula.

Na kraju, za $M = \{1, 2, 3\}$, za dvomjesnu relaciju ili dvomjesni predikat

$$P = \{(3,3), (3,1), (2,2), (2,1), (1,1)\} = \{(x, y) : x \,\text{je djeljiv s}\, y\},$$

- $P(3, 1)$ je istinita izjava,
- $P(1, x)$ je ispunjiva i oboriva izjava,
- $P(x, 1)$ je istinita izjava bez obzira na valuaciju varijable x. U ovom slučaju, zato što je formula $P(x, 1)$ uvijek istinita, bez obzira koliki je x, kažemo da je (M, P) model za formulu $P(x, 1)$. Kod dvomjesnih relacija, kao u ovom primjeru, još jasnije vidi se smisao imena predikatna logika. U $P(x, y)$ x je subjekt, a “je djeljiv s y” predikatni skup.

Predikatna logika sadrži sve što i logika sudova, s gotovo istim pravilima te predikat, odnosno relaciju i to je najvažnija novost u ovoj teoriji. Novi su i znakovi $\forall$ i $\exists$. Također, kao argument relacije može se pojaviti, osim varijable i konstante kao gore, i funkcija jedne ili više varijabli.

Logika sudova imala je, vidjeli smo, alfabet sačinjen od varijabli, veznika i zagrada (samo to). Od tih znakova sastavljali smo formule, ispitivali ih i s njima modelirali razne pojave iz "stvarnosti".

Evo nekoliko primjera formula logike prvog reda:

1. $F \equiv R(x, y)$. $R(x, y)$ je dvomjesna relacija (ima dva argumenta, x i y).
2. $F \equiv \forall x \Big(N(x) \to N\big(f(x)\big) \Big)$.
   Ova formula kaže: Za svaki x vrijedi: Ako x ima svojstvo N, onda i $f(x)$ ima svojstvo N.
   $N(x)$ je jednomjesna relacija (njeno je značenje $x \in N$), $f(x)$ uobičajena je funkcija s jednim argumentom (x). Ako sve gledamo na "prostoru" realnih brojeva, ako s N označimo prirodne brojeve i ako je $f(x) = x^2$, ova je formula dobar model za rečenicu "Kvadrat prirodnog broja je prirodan broj", tj. ako je broj prirodan, $x \in N$ ili $N(x)$, onda je i $f(x) = x^2$ također prirodan, tj. vrijedi $f(x) \in N$, tj. $N\big(f(x)\big)$.

Primjer 1.6.1. Primjer zaključivanja koje ne može opisati logika sudova, a može logika prvog reda:
Svi koji piju puno vode dobro vide.
Vinko ne vidi dobro.
Dakle, Vinko ne pije puno vode.

U logici sudova ne možemo napraviti (smislenu, korisnu) strukturu za ovakvo zaključivanje. U logici prvog reda možemo.

Označimo s M skup svih ljudi.
Skup svih ljudi koji piju puno vode označit ćemo s P. Tada će $x \in P$ ili kraće $P(x)$ (x ima karakteristiku P) značiti da osoba x pije puno vode.
Skup onih koji dobro vide označimo s D.
Među ljudima je i spomenuti Vinko kojeg ćemo (kao konstantu) označiti s v.
Sada je napokon model sljedeći:

Svi koji piju puno vode dobro vide.	$\forall x\,(x \in P \to x \in D)$ ili, kraće, $\forall x \,\big(P(x) \to D(x)\big)$.
Vinko ne vidi dobro.	$v \notin D$ ili, kraće, $\neg D(v)$.
Dakle, Vinko ne pije puno vode.	$v \notin P$ ili, kraće, $\neg P(v)$.

Ukupno, formula $\forall x \,\big(P(x) \to D(x)\big) \wedge \neg D(v) \to \neg P(v)$ je tautologija tj. valjana formula bez obzira kako interpretirali P, D, x ili v.

Definicija 1.6.1. *Alfabet logike prvog reda unija je sljedećih skupova*

$A_1 = \{x_0, x_1, x_2, \ldots\}$, (Članove skupova A_1 zovemo varijable ili, u nekim knjigama, individualne varijable. Postoji ih beskonačno. Označavat ćemo ih najčešće malim slovom, bez indeksa: x, y, z, u, v, ...)

$A_2 = \{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists\}$, ($A_2$ je skup znakova ili logičkih simbola, s istim imenima kao u logici sudova, uz $\forall$ koji zovemo univerzalni kvantifikator i $\exists$ koji zovemo kvantifikator egzistencije.)

$A_3 = \{R_k^{n_k} : k \in I\}$ *gdje je* I *neki beskonačan skup indeksa,* (U A_3 su relacije – jednomjesne, dvomjesne, ... ili nul-mjesne. Broj n_k, broj argumenata, zovemo mjesnost relacije. Najčešće taj broj nećemo pisati jer će se iz oblika odmah vidjeti mjesnost, tj. broj argumenata. Pisat ćemo jednostavnije: $R(x, y)$, $P(x)$, S, $T(i)$, ... Na propozicionalne varijable "iz logike sudova" gledamo kao na nul - mjesne relacije. A_3 sadrži, po dogovoru, i dvomjesnu relaciju "=", $= (x, y)$ koju zovemo jednakost.)

$A_4 = \{f(x), g(x, y), h(j), \ldots\}$, ($A_4$ je skup funkcija, jedne ili više varijabli.)

$A_5 = \{a, b, c, \ldots\}$, ($A_5$ je skup konstanti.)

$A_6 = \{(,)\} \cup \{,\}$ (To su zagrade i zarez, pomoćni simboli.)

Unija skupova A_3, A_4 i A_5 je skup nelogičkih znakova koji zovemo i signatura.

Skupovi A_3, A_4 i A_5 sadrže beskonačno relacija svih "mjesnosti", beskonačno funkcija svih brojeva argumenata i beskonačno konstanti.

Kod nekih autora konstante su specijalni slučaj funkcija, tj. konstanta je funkcija s nula argumenata.

U nekim knjigama ili člancima, alfabet logike sudova sadrži i konstante 0 ili 1 (ili $\perp$ i $\top$).

Definicija 1.6.2. *Riječ je konačan "niz" znakova alfabeta.*

Primjer riječi: $R(a, b) \wedge \wedge f(x)$, $\big(()\big)$, $f\big(R(u, v)\big)$, $\forall x\, P(x) \rightarrow \exists x\, Q(x)$.

No, naravno, nije nam svaka riječ zanimljiva. Koristit ćemo samo smislene koje ćemo zvati, opet kao i u logici sudova, formule.
Koja je riječ formula?

Prvo definirajmo pojam term.

Definicija 1.6.3. *Term je svaka varijabla i svaka konstanta.*
Također, term je i svaka funkcija, iz A_4, oblika $f(t_1, t_2, \ldots, t_n)$, gdje su t_1, t_2, ... , t_n neki termi.

Primjer 1.6.2. Termi su t, c_1, $g(x, y)$, $j\big(f(x), f(c), h(x, y, z)\big)$, c_2, $f(x, y)$, ...
Termi nisu $R(x, z)$, $\neg A$, ...

Definicija 1.6.4. *Ako je R neki n-mjesni relacijski simbol iz A_3 (moguće i nul - mjesni), a t_1, ... , t_n termi, tada riječ $R(t_1, \ldots, t_n)$ zovemo atomarna formula.*
(Dakle, atomarna formula mora sadržavati relaciju.)

Primjer 1.6.3. Atomarne su formule A, $P\big(v, f(v)\big)$, $J(x)$.
Atomarne formule nisu v, x, c_1, $f(x)$, $A(x) \to B$.

Definicija 1.6.5.

a) Svaka atomarna formula je formula.

b) Ako su A i B formule, tada su $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \to B)$ i $(A \leftrightarrow B)$ također formule.

c) Ako je A formula, a x varijabla, tada su i $(\forall\, x\, A)$ i $(\exists\, x\, A)$ također formule.

d) Riječ je formula ako i samo ako je nastala konačnim brojem primjena pravila a), b) i c).

Zagrade ćemo redovito propuštati pisati ako je jasno gdje se nalaze. Primjerice, umjesto $F = (A \to B)$, pisat ćemo $F = A \to B$, a umjesto $F = \Big(\big(\forall\, x\, (R(x))\big) \to G\Big)$, pisat ćemo $F = \forall\, x\, R(x) \to G$.

U propuštanju pisanja zagrada poštujemo sljedeći prioritet veznika i kvantifikatora:

- Najveći prioritet (i međusobno jednak) imaju $\neg$, $\forall$ i $\exists$.

- Zatim $\wedge$ i $\vee$.

- Zatim $\to$ i $\leftrightarrow$.

Primjer 1.6.4. Formule su: $A(x) \to \forall\, x\; F(x)$, $A \wedge B$, $\exists\, y\; (E \vee F)$, ...
Formule nisu: $A \to\to$, $\to$, $\forall\, R\,\big(R(x)\big) \to G$ (jer u logici prvog reda ne može iza kvantifikatora stajati relacija nego samo varijabla), $\bigwedge\limits_{i \in \mathbb{N}} A_i = A_1 \wedge A_2 \wedge A_3 \wedge \ldots$, $i \in \mathbb{N}$ (jer riječ je formula ako i samo ako je nastala primjenom konačnog, a ne kao ovdje beskonačnog broja pravila a), b) i c)).

Sada nam se postavlja osnovno pitanje konstrukcije sustava logike prvog reda, a to je kako interpretirati elemente formula, a onda i cijele formule ove logike. Za potrebe razumijevanja logike prvog reda, ovdje donosimo jednostavnije objašnjenje. Detaljnije, točnije (i kompliciranije) objašnjenje dano je u knjizi *Matematička logika* navedenoj u početku ovog potpoglavlja.

Definicija 1.6.6. *Struktura je uređeni par (M, φ) gdje je M neprazan skup kojeg zovemo* **univerzum** *(ili* **svijet** *ili* **nosač** *ili* **domena***), a φ je preslikavanje koje:*

a) svakoj relaciji iz A_3 pridružuje relaciju (te iste mjesnosti, naravno) s M,

b) svakoj funkciji iz A_4 pridružuje funkciju (istog broja varijabli, naravno) i

c) svakoj konstanti iz A_5 pridružuje element skupa M.

Primjer 1.6.5.

a) Za zadanu formulu $F \equiv P(a, b)$, definiramo strukturu (M, φ) gdje je $M = \{e, r, t\}$, $\varphi(P) = \{(e, e), (e, t)\}$.

b) Za zadanu formulu $F \equiv \forall x\, R(x) \to \exists y\, S(y)$, definiramo strukturu (M, φ) gdje je $M = \{1, 2, 3\}$, $\varphi(R) = \{1, 2\}$, $\varphi(S) = \{1,\ 3\}$.

Definicija 1.6.7. *Svaku funkciju v sa skupa varijabli A_1, u univerzum M zovemo* **valuacija***.*

Primjer 1.6.6.

a) Ako za zadanu formulu $F \equiv P(a, b)$ definiramo strukturu (M, φ) gdje je $M = \{e, r, t\}$, $\varphi(P) = \{(e, e), (e, t)\}$, onda je jedna valuacija $v(a) = r$, $v(b) = e$.

b) Ako za zadanu formulu $F \equiv \forall x\, R(x) \to \exists y\, S(y)$, definiramo strukturu (M, φ) gdje je $M = \{1, 2, 3\}$, $\varphi(R) = \{1, 2\}$, $\varphi(S) = \{1, 3\}$, onda je jedna valuacija $v(x) = 1$, $v(y) = 1$.

Često ćemo, umjesto $\varphi(P) = \{(e, e), (e, t)\}$, kratko pisati $P = \{(e, e), (e, t)\}$ (kao što smo i u logici sudova umjesto npr. $I(A) = 1$ pisali kratko $A = 1$). Isto ćemo tako, umjesto $v(x) = e$, kratko pisati $x = e$.

Definicija 1.6.8. *Uređeni par strukture i valuacije zovemo* **interpretacija***.*

Sada kada smo za zadanu formulu odlučili kako ćemo interpretirati njene relacije (interpretirat ćemo ih nečim iz nosača M), funkcije, konstante i varijable možemo reći napokon i kada je formula logike prvog reda istinita, a kada ne. Podsjetimo se: M je svemir, φ nam kaže što je u relacijama i funkcijama, v daje vrijednost varijablama.

Definicija 1.6.9. *Neka je* $\big((M,\varphi),v\big)$ *neka interpretacija.*

1. *Ako je* F *atomarna formula oblika* $F \equiv R(a,b,c,\ldots)$*, onda je* F *istinita ako je* $\big(v(a),v(b),v(c),\ldots\big) \in \varphi(R)$*.*

2. *Ako je* F *formula oblika* $\neg G$*, onda je formula* F *istinita ako formula* G *nije istinita.*

3. *Ako je* F *formula oblika* $G \wedge H$*, onda je formula* F *istinita ako je formula* G *istinita i ako je formula* H *istinita.*

4. *Ako je* F *formula oblika* $G \vee H$*, onda je formula* F *istinita ako je formula* G *istinita ili ako je formula* H *istinita.*

5. *Ako je* F *formula oblika* $G \to H$*, onda je formula* F *istinita ako formula* G *nije istinita ili ako je formula* H *istinita.*

6. *Ako je* F *formula oblika* $G \leftrightarrow H$*, onda je formula* F *istinita ako su formule* G *i* H *obje istinite ili ako ni* G *ni* H *nisu istinite.*

7. *Ako je* F *formula oblika* $\forall\, x\, G$*, onda je formula* F *istinita ako je formula* G *istinita za svaku valuaciju* v*, tj. kako god zamijenili* x *s nekim elementom univerzuma.*

8. *Ako je* F *formula oblika* $\exists\, x\, G$*, onda je formula* F *istinita ako je formula* G *istinita za bar jednu valuaciju* v*, tj. postoji bar jedan element* e *univerzuma* M *za koji vrijedi da je formula* G *istinita ako u njoj svaki nastup od* x *zamijenimo s tim elementom* e*.*

Definicija 1.6.10. *Formula* F *je:*

a) ispunjiva *ako postoji interpretacija* $\big((M,\varphi),v\big)$ *za koju je* F *istinita,*

b) oboriva *ako postoji interpretacija* $\big((M,\varphi),v\big)$ *za koju* F *nije istinita,*

c) valjana *ili* tautologija *ako je istinita za svaku interpretaciju.*

Definicija 1.6.11. *Struktura* (M,φ) *je* model *za formulu* F *ako je to struktura za* F *i ako je* F *istinita u toj strukturi bez obzira kakva bila valuacija varijabli iz* F*, tj. ako je* F *istinita u navedenoj strukturi za svaku valuaciju* v*.*

Dakle, ako je formula tautologija, onda je svaka struktura (M,φ) model za tu formulu.

Logika sudova	Logika prvog reda
Zadana je formula. Prvo varijablama A, B, C, ... pridružujemo ili 1 ili 0, a onda na osnovu pravila za veznike i zagrade, "izračunamo" vrijednost cijele formule koja se od tih varijabli sastoji.	Zadana je formula. Prvo odaberemo univerzum (bilo koji neprazan skup na kojem će se "sve događati") M pa za zadanu formulu svakoj relaciji, funkciji, konstanti i varijabli te formule pridružimo neku relaciju koja je relacija na M, funkciju sa $M \to M$, konstantu iz M ili element iz M. Nakon toga jednostavno odredimo istinosnu vrijednost formule.
Primjer: Za zadanu formulu $F \equiv \neg A \wedge (B \to C)$, za $I(A) = 0$, $I(B) = 0$, $I(C) = 1$ dobivamo $I(F) = 1$.	**Primjer:** Za zadanu formulu $F \equiv \forall x \big(R(x) \to S(x)\big)$, ako za univerzum M odaberemo $M = \{1, 2, 3\}$, ako za R i S odaberemo $R = \{1, 3\}$ i $S = \{3\}$, tada ne vrijedi za svaki $x \in M$ formula $$R(x) \to S(x) \text{ , tj. } x \in R \;\to\; x \in S.$$ Za $x = 1$ ne vrijedi $x \in R \to x \in S$. Dakle, formula $\forall x \big(R(x) \to S(x)\big)$ je oboriva. Isto tako, ako za univerzum M odaberemo $M = \{\alpha, \beta, \gamma, \delta\}$, ako za R odaberemo $R = \{\alpha, \beta, \gamma\}$, a za $S = \{\alpha, \beta, \gamma, \delta\}$, tada formula $R(x) \to S(x)$ vrijedi za svaki $x \in M$, tj. $x \in R \to x \in S$ je istina za sve elemente skupa M. Dakle, formula $\forall x \big(R(x) \to S(x)\big)$ je ispunjiva. Struktura $M = \{\alpha, \beta, \gamma, \delta\}$, $R = \{\alpha, \beta, \gamma\}$, $S = \{\alpha, \beta, \gamma, \delta\}$ je model za danu formulu.

ZADACI ZA VJEŽBU

Zadatak 1.6.1. Jesu li formule

a) $F \equiv P(x, y) \wedge P(x, z)$,

b) $F \equiv P(x, y) \leftrightarrow R(x)$,

c) $F \equiv \forall x \, P(a, x)$

ispunjive? Jesu li oborive? Jesu li su tautologije?
Pokušaj dati odgovore koristeći strukturu $M = \{a, b, c, d\}$, $P = \{(a, a), (a, b), (a, c)\}$, $R = \{b, c\}$.

Zadatak 1.6.2. Odredi model za formulu

a) $A(x) \to B(y)$

b) $\exists\, z\, P\big(f(z)\big)$

c) $P(x, y, z) \leftrightarrow \forall\, u\, R(u)$

Zadatak 1.6.3. Na univerzumu M svih živih bića (ljudi i biljke u ovom slučaju) označimo s

$R(x)$ – x je ratar

$V(x)$ – x je voće

$P(x)$ – x je povrće

$U(x, y)$ – x uzgaja y

$J(x, y)$ – x i y su jednaki, tj, $x = y$.

Zapišite formulu logike predikata koja opisuje sljedeću rečenicu

a) Nijedno voće nije povrće.

b) Samo ratari nešto uzgajaju.

c) Neki ratari ne uzgajaju ništa.

d) Svi ratari uzgajaju voće ili povrće.

e) Svako povrće ima najviše jednog uzgajatelja.

f) Svako povrće ima točno jednog uzgajatelja.

g) Svako voće ima točno dva uzgajatelja.

Zadatak 1.6.4. Neka su A i B skupovi. Funkcija $f : A \to B$ je

a) injekcija ako različite elemente domene A preslikava u različite elemente kodomene B,

b) surjekcija ako je svakom elementu kodomene B pridružen neki element domene A,

c) bijekcija ako je injekcija i surjekcija.

Zapiši ove tvrdnje jezikom logike prvog reda. Poradi određenosti, uzmimo da je $A = B = \mathbb{R}$.

RJEŠENJA

1.6.1. a) $F \equiv P(x,y) \wedge P(x,z)$ će biti ispunjiva ako nađemo neku valuaciju njenih varijabli x, y, i z za koju su i $P(x,y)$ i $P(x,z)$ istinite. Možemo li x, y i z zamijeniti s nekim elementima iz M tako da $P(x,y)$ i $P(x,z)$ budu istinite, tj. tako da vrijedi $(x,y) \in P$ i $(x,z) \in P$? Očito za $x = a$, $y = a$, $z = a$ vrijedi $P(a,a)$ i vrijedi $P(a,a)$ (opet isti par) pa je $F \equiv P(x,y) \wedge P(x,z)$ ispunjiva. Naravno, mogli smo odabrati i $x = a$, $y = b$, $z = c$. Nismo, za potrebe ovog zadatka, mogli odabrati $x = b$, $y = a$, $z = a$.

$F \equiv P(x,y) \wedge P(x,z)$ će biti oboriva ako nađemo neku valuaciju njenih varijabli x, y, i z za koju je ili $P(x,y)$ neistinita ili $P(x,z)$ neistinita. Možemo li x, y i z zamijeniti nekim elementima iz M tako da ili $P(x,y)$ ili $P(x,z)$ budu neistinite, tj. tako da vrijedi $(x,y) \notin P$ ili $(x,z) \notin P$? Očito za $x = b$, $y = b$, $z = c$ ne vrijedi $P(b,b)$, a čak ne vrijedi ni $P(b,c)$ pa je $F \equiv P(x,y) \wedge P(x,z)$ oboriva. Naravno, mogli smo odabrati i $x = b$, $y = b$, $z = a$. Nismo, za potrebe ovog zadatka, mogli odabrati $x = a$, $y = b$, $z = c$.

Budući da je F oboriva, tj. postoji valuacija uz danu strukturu, tj. postoji interpretacija za koju F nije istinita, F ne može biti tautologija.

b) $F \equiv P(x,y) \leftrightarrow R(x)$ će biti ispunjiva ako nađemo neku valuaciju njenih varijabli x i y za koju su $P(x,y)$ i $R(x)$ obje istinite ili obje lažne. Možemo li x i y zamijeniti nekim elementima iz M tako da $P(x,y)$ i $R(x)$ budu obje istinite ili obje lažne, tj. tako da vrijedi $(x,y) \in P$ i $x \in R$ ili možda $(x,y) \notin P$ i $x \notin R$? Ako odaberemo $x = a$, tada će $P(x,y)$ biti istina bez obzira što uzeli za y, a $R(x)$ će biti laž. Ako uzmemo $x = b$ ili $x = c$, tada će $P(x,y)$ biti laž bez obzira što uzeli za y, a $R(x)$ će biti istina.
Slijedi da zadana formula uz zadanu strukturu nije ispunjiva. Ona je zbog gore navedenih valuacija oboriva. Stoga nije tautologija. No, možda je ispunjiva u nekoj drugoj strukturi. Uzet ćemo za tu potrebu strukturu $M = \{a,b,c,d\}$, $P = \{(a,a),(a,b),(a,c)\}$, $R = \{a\}$. Sada je očito $(x,y) \in P$ ako i samo ako je $x \in R$, tj. $P(x,y) \leftrightarrow R(x)$.

c) $F \equiv \forall x\, P(a,x)$
Pogledajmo što kaže gornja definicija istinitosti formule, pod 7.

Ako je F formula oblika $\forall x\, G$, onda je formula F istinita ako je formula G istinita za svaku valuaciju v, tj. kako god zamijenili x s nekim elemetom univerzuma.
Za $v(x) = a$ moralo bi biti $P(a, a)$ istinito. A jest jer zaista je $(a, a) \in P$.
Za $v(x) = b$ moralo bi biti $P(a, b)$ istinito. A jest jer zaista je $(a, b) \in P$.
Za $v(x) = c$ moralo bi biti $P(a, c)$ istinito. A jest jer zaista je $(a, c) \in P$.

Zaključak: Za svaku valuaciju varijable x vrijedi $(a, x) \in P$, tj. $P(a, x)$ je istina. Dana formula ispunjiva je u gore određenoj interpretaciji $\big((M, \varphi), v\big)$. Uočimo kako je $M = \{a, b, c, d\}$, $P = \{(a, a), (a, b), (a, c)\}$, $R = \{b, c\}$ model za formulu F jer je ona u toj strukturi istinita bez obzira na valuaciju v.

1.6.2. a) Potrebno je pronaći univerzum M i na njemu relacije A i B tako da formula $A(x) \to B(y)$ bude istinita bez obzira kako valuirali varijable koje se u njima pojavljuju.
$A(x) \to B(y)$ će biti istinita kad god je $A(x)$ laž ili je $B(y)$ istinita.
Odaberimo $M = \{1, 2, 3\}$, $A = \emptyset$, $B = \{1, 2\}$.
Sada je za svaki $x \in M$, $A(x)$ laž, tj. $x \in A$ je laž jer je A prazan skup, tj. nikada nije $x \in A$, ni za koji $x \in M$.
Drugi model je $M = \{1, 2, 3\}$, $A = \{1, 2, 3\}$, $B = \{1, 2, 3\}$.

b) Potrebno je pronaći univerzum M i na njemu relaciju P i funkciju f tako da formula $\exists z\, P\big(f(z)\big)$ bude istinita bez obzira kako valuirali varijablu z.
Odaberimo $M = \{1, 2, 3\}$, $f(x) = 4 - x$ (tj. $f(1) = 3$, $f(2) = 2$, $f(3) = 1$), $P = \{1, 2\}$.
$\exists z\, P\big(f(z)\big)$ znači u stvari da postoji neki element z iz M za koji vijedi da je $f(z)$ u P.
Za $v(z) = 1$ ili $z = 1$ vrijedi $f(1) = 3 \notin P$.
Za $z = 2$ vrijedi $f(2) = 2 \in P$. Pronašli smo z.

Zaključak: Formula $\exists z\, P\big(f(z)\big)$ je istinita na strukturi (M, φ) gdje je

$$M = \{1, 2, 3\},\ \varphi\big(f(x)\big) = 4 - x,\ \varphi(P) = \{1, 2\},$$

ili kratko

$$M = \{1, 2, 3\},\ f(x) = 4 - x,\ P = \{1, 2\}.$$

c) Potrebno je pronaći univerzum M i na njemu relacije P i R tako da formula $P(x, y, z) \leftrightarrow \forall u\, R(u)$ bude istinita bez obzira kako valuirali varijable koje se u njima pojavljuju.
$P(x, y, z) \leftrightarrow \forall u\, R(u)$ će biti istinita kad god su $P(x, y, z)$ i $\forall u\, R(u)$ obje istina

ili obje laž.
Odaberimo $M = \{1, 2, 3\}$, $P = R = \emptyset$.

Sada je za sve $x \in M$, $y \in M$, $z \in M$, $P(x, y, z)$ laž jer je P prazan, no i $\forall\, u\, R(u)$ je također laž (jer $\forall\, u\, R(u)$, znači $\forall\, u \in M$ je $u \in R$).

Drugi model je $M = \{1\}$, $P = \{(1, 1, 1)\}$, $R = \{1\}$. $P(x, y, z)$ je uvijek istina i $\forall\, u\, R(u)$ također.

1.6.3. a) $V(x) \to \neg P(x)$.
(Uočimo da zbog kontrapozicije implikacije odmah imamo i $\neg\neg P(x) \to \neg V(x)$, tj. $P(x) \to \neg V(x)$, tj. ako niti jedno voće nije povrće, odmah slijedi i da niti jedno povrće nije voće. Dalje, uočimo i kako ne možemo zaključiti da $\neg P(x) \to V(x)$, tj. da ako nešto nije povrće da je voće. Čovjek npr. koji nije povrće, ipak nije voće.)

b) Rečenica kaže: Ako netko nešto uzgaja, onda je taj netko ratar.
Dakle: $U(x, y) \to R(x)$.

c) Postoje ratari koji ne uzgajaju ništa: $\exists\, x\, \big(R(x) \land \neg\exists\, y\, U(x, y)\big)$.
Ili: $\exists\, x\, \big(R(x) \land \forall\, y\, \neg U(x, y)\big)$.

d) Ako je x ratar, onda on uzgaja nešto i to što on uzgaja je ili voće ili povrće. To jest:

$$R(x) \to \Big(U(x, y) \land \big(V(y) \lor P(y)\big)\Big).$$

e) Ovaj je zadatak za nijansu teži. Rečenica kaže da svako povrće ima nula ili jednog uzgajatelja. Ako povrće uzgaja uzgajatelj x i uzgajatelj y, onda su ti uzgajatelji u stvari jedan te isti uzgajatelj. To je jedan od više načina na koje zadatak možemo riješiti. Drugim riječima, ako je z neko povrće, onda ako postoji njegov uzgajatelj i ako ga uzgajaju x i y, onda je $x = y$.

$$P(z) \to \big(U(x, z) \land U(y, z) \to J(x, y)\big).$$

f) Rečenica kaže da svako povrće ima uzgajatelja i da ako povrće uzgaja uzgajatelj x i uzgajatelj y, onda su ti uzgajatelji u stvari jedan te isti uzgajatelj. Drugim riječima, ako je z neko povrće, onda postoji njegov uzgajatelj i ako ga uzgajaju x i y, onda je $x = y$.

$$P(z) \to \Big(\exists\, x\; U(x, z) \land \big(U(x, z) \land U(y, z) \to J(x, y)\big)\Big).$$

g) Za rješenje ovog zadatka potreban nam je opet za nijansu kompliciraniji model. Moramo uzeti dva uzgajatelja, x i y. Treba pokazati da su različiti i da uzgajaju navedeno voće te da je svaki treći uzgajatelj u stvari ili x ili y.

$$\begin{aligned} V(z) \to \exists\, x\, \exists\, y\ \big(\neg J(x,y) \wedge U(x,z) \wedge U(y,z)\big) \wedge \\ \wedge \neg\Big(\exists\, x\, \exists\, y\, \exists\, w\ \big(U(x,z) \wedge U(y,z) \wedge U(w,z) \wedge \neg J(x,y) \wedge \\ \wedge \neg J(x,w) \wedge \neg J(y,w)\big)\Big). \end{aligned}$$

(Ako je z voće, onda postoje x i y za koje vrijedi: nisu jednaki i oba uzgajaju z. Također, ne postoje tri uzgajatelja koji uzgajaju z i koji su svi međusobno različiti). Zadatak se može riješiti na više načina, ali ne puno jednostavnije od ovoga.

1.6.4. Neka je M skup realnih brojeva.

a) Potrebno je zapisati kako je za svaki odabir brojeva x i y iz domene točno: ako su x i y različiti, onda su i $f(x)$ i $f(y)$ različiti.

$$\forall\, x\, \forall\, y\ \Big(\neg J(x,y) \to \neg J\big(f(x), f(y)\big)\Big)$$

Ovdje treba uočiti kako će u slučaju različitih A i B i relacija J biti različita na A i B. Tada će definicija injektivnosti glasiti

$$\forall x\, \forall y\ \Big(D(x) \wedge D(y) \wedge \neg J_A(x,y) \to \neg J_B\big(f(x), f(y)\big)\Big),$$

gdje su J_A i J_B relacije jednakosti na domeni i kodomeni.
Dalje, iz formule kontrapozicije kondicionala iz logike sudova koja kaže

$$(A \to B) \leftrightarrow (\neg B \to \neg A),$$

jasno je da smo injektivnost funkcije f mogli opisati kao

$$\forall\, x\, \forall\, y\ \Big(J\big(f(x), f(y)\big) \to J(x,y)\Big).$$

b) $\forall\, y\, \exists\, x\ \big(J(f(x), y)\big)$.

c) Očito je rješenje:

$$\forall\, x\, \forall\, y\ \Big(J\big(f(x), f(y)\big) \to J(x,y)\Big) \wedge \forall\, y\, \exists\, x\ \big(J(f(x), y)\big).$$

2

Teorija skupova

2.1. Skupovi i operacije sa skupovima

Cilj je potpoglavlja 2.1. čitatelju dati osnovna znanja iz teorije skupova (povijest, zadavanje skupova, odnosi među skupovima i osnovne operacije) koja će se koristiti u nadolazećim potpoglavljima.

Čitatelj bi nakon potpoglavlja 2.1. trebao razumjeti kako je i zašto teoriju skupova bilo teško strogo zasnovati (i još uvijek je). Dalje, trebao bi znati modelirati probleme iz okolnog svijeta i rješavati zadatke koristeći skup, element, partitivni skup, prazan skup, uniju skupova i ostale osnovne relacije među skupovima i operacije sa skupovima.

Literatura za potpoglavlje 2.1. sljedeće su knjige:

1. B. Dakić, N. Elezović, *Matematika 1 1. dio. Udžbenik i zbirka zadataka za prvi razred gimnazije*, Element, Zagreb, 2009. godina.
2. V. Devide, *Matematička čitanka*, Školska knjiga, Zagreb, 1991.
3. P. Papić, *Uvod u teoriju skupova*, HMD, Zagreb, 2000.
4. N. J. Vilenkin, *Priče o skupovima*, Školska knjiga, Zagreb, 1975.
5. M. Vuković, *Teorija skupova*, predavanja. https://web.math.pmf.unizg.hr/nastava/ts/materijali/ts-skripta-2015.pdf (zadnji pristup travanj 2022.)
6. https://www.onlinemath4all.com/subsets-worksheet.html (zadnji pristup travanj 2022.)

Teorija skupova u samom je temelju matematičkih objekata. Stoga je teško postaviti temelje ovakvoj disciplini (teško je naći ono na što se "sve" iz okolnog svijeta može smisleno "svesti"). Matematička logika u temelju je matematičkog razmišljanja, ona nas uči *kako* razmišljati u matematici, a teorija skupova unosi objekte u matematiku, tj. uvest će nam stvari *o kojima* ćemo razmišljati, početak onoga što matematika izučava.

Teorija skupova izdvaja se među matematičkim i logičkim disciplinama po svojoj dugoj i zanimljivoj povijesti.

George Cantor[1] je oko 1870. godine započeo sustavan i strog (matematički) pristup teoriji skupova. Ipak, bez ozbiljnijih temelja, njegov pristup danas je poznat kao naivna teorija skupova (uspio je matematički opisati teoriju, no nije to napravio "dovoljno konzistentno" ili strogo pa su neki matematičari tog doba iz njegove teorije izveli razne paradokse, rečenice koje mogu biti i istina i laž).

U prvoj polovici 20. stoljeća matematičari (koji su u isto vrijeme bili i logičari) pokušali su teoriju skupova zasnovati aksiomatski, tj. nabrojati određeni broj aksioma, nedvojbenih (i "neprovjerljivih") istina iz kojih će se izvesti teorija koja će biti najbolji model za "matematiku skupova".

1908. godine njemački logičar i matematičar Ernst Zermelo dao je prvi prijedlog takvog skupa aksioma, a 1922. ga je godine zajedno s njemačkim matematičarom Abrahamom Fraenkelom[2] dodatno poboljšao te se pojavio Zermelo-Fraenkelov (Z - F) skup od osam aksioma koji se do danas smatra najboljim sustavom za temelje teorije skupova. Kasnije je Z - F sustavu dodan i deveti aksiom, aksiom izbora pa se Z - F sustav danas najčešće koristi kao ZFC (slovo C dolazi od "Axiom of Choice"). Unatoč općoj prihvaćenosti ZFC sustava kao temelja teorije skupova (i matematike u neku ruku), ZFC aksiomi imaju svojih loših strana. (No, i dalje nema nekog "boljeg" sustava, tj. i ostali sustavi aksioma imaju svojih (i većih) loših strana. Npr. postoje matematičke tvrdnje koje ZFC ne može niti potvrditi niti oboriti.)

Skup se (kao niti pojam "biti element") nigdje u matematici, gotovo bez obzira na pristup, ne definira. Skup je prejednostavan, osnovni pojam i nema drugih jednostavnijih pojmova koji bi ga mogli objasniti.

Skupovi se zadaju nabrajanjem elemenata ili pravilom, kao npr.

$$S = \{1, 2, 4\}$$

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$$

[1]George Cantor (1845. – 1918.) – njemački matematičar

[2]Abraham Fraenkel (1891. – 1965.) – izraelski matematičar njemačkog porijekla

$P = \{2x \mid x \in \mathbb{N}\}$

$P = \{x \mid x \in \mathbb{N} \text{ i } x \text{ je djeljiv s } 2\}$

$P = \{x : x \in \mathbb{N} \text{ i } x \text{ je djeljiv s } 2\}$ (ponekad se za uvjet koji elementi moraju zadovoljavati piše i ":").

$P = \{2, 4, 6, 8, \ldots\}$ itd.

I skupovi mogu biti elementi skupova. Npr., osnovna škola skup je razreda, a svaki je razred skup učenika.

Primjer 2.1.1. Za $A = \{1, \{1, 2\}\}$ vrijedi $1 \in A$, $\{1, 2\} \in A$, $2 \notin A$. Ovo ponekad pišemo kao $A \ni 1$ (skup A sadrži 1 kao svoj element), $A \ni \{1, 2\}$ (skup A sadrži skup $\{1, 2\}$ kao svoj element), $A \not\ni 2$ (skup A ne sadrži 2 kao svoj element).

Dalje, nakon skupa i elementa, sve ostalo definiramo.

Na početku, kako je sve oko nas neki skup (čak i pojedinačna stvar skup je atoma od kojih se sastoji), pokušajmo među sve te skupove uvesti neki red. Pokušajmo usporediti skupove po veličini. Bit će to samo djelomičan uspjeh jer se ne mogu svi skupovi uspoređivati dolje navedenim relacijama, ali za skupove koji su dijelovi nekih većih skupova, možemo ipak reći koji je od njih "veći", a koji "manji", koristeći relaciju "biti podskup", tj. "$\subseteq$".

Definicija 2.1.1. *Kažemo da je skup A* **podskup** *skupa B i pišemo $A \subseteq B$ ako je izjava $\forall x\,(x \in A \to x \in B)$ tautologija.*
Drugim i jednostavnijim riječima: A će biti podskup od B ako vrijedi da svaki element koji je u skupu A, postoji i u skupu B. Pišemo i $B \supseteq A$, što čitamo B je **nadskup od** A. Ako A nije podskup od B, pišemo $A \not\subseteq B$ i analogno $B \not\supseteq A$.

Primjer 2.1.2. Za $A = \{1, 2\}$, $B = \{1, 2, 7\}$ vrijedi $A \subseteq B$, $B \supseteq A$, $B \not\subseteq A$, $A \not\supseteq B$.

Definicija 2.1.2. *Kažemo da je skup A* **jednak** *skupu B i pišemo $A = B$ ako vrijedi $A \subseteq B$ i $B \subseteq A$.*
Drugim riječima: Skupovi A i B jednaki su ako je A podskup od B i B je podskup od A, tj. svaki element iz A postoji i u B i svaki element iz B postoji i u A. Ako nije $A = B$, pišemo $A \neq B$.

Primjer 2.1.3. Za $A = \{1, 2\}$, $B = \{1, 2, 7\}$ ne vrijedi $A = B$ jer nije $B \subseteq A$. Vrijedi $A \neq B$.

Definicija 2.1.3. *Kažemo da je skup A* **pravi podskup** *skupa B i pišemo $A \subset B$ (ili rjeđe $A \subsetneq B$) ako vrijedi $A \subseteq B$ i $A \neq B$.*
Drugim riječima: A će biti pravi podskup od B ako je A podskup od B, no oni nisu

jednaki, tj. B nije podskup od A. Pišemo i $B \supset A$, što čitamo B sadrži A kao svoj pravi podskup. Ako A nije pravi podskup od B, pišemo $A \not\subset B$ i analogno $B \not\supset A$.

Primjer 2.1.4. Za $A = \{1, 2\}$, $B = \{1, 2, 7\}$ vrijedi $A \subset B$, $B \supset A$, $B \not\subset A$, $A \not\supset B$.

Primjer 2.1.5. Za $A = \{1, 2\}$, $B = \{1, 2, 1\}$ vrijedi $A \subseteq B$ (jer svaki element koji je u A nalazi se i u B). Je li i $B \subseteq A$? Provjerimo.
U B su redom nabrojani: 1 – on je i u A, 2 – i on je i u A, 1 – i on je i u A. Svatko tko je nabrojan u B je i u A. Dakle, $B \subseteq A$. No, ako je sada i $A \subseteq B$ i $B \subseteq A$, slijedi da su skupovi A i B jednaki, tj. $A = B$. Dakle, kod skupova nije važno u kojem se poretku nalaze elementi niti koliko smo puta koji element nabrojali; primjerice, $\{1, 2, 3\} = \{3, 3, 1, 2, 1, 3\}$.

Definicija 2.1.4. *Prazan skup je skup koji nema elemenata. Označavat ćemo ga kao u većini literature s $\emptyset$ (česta je i oznaka $\{\}$).*

Definicija 2.1.5. *Neka je S skup. Skup svih podskupova skupa S označavamo s $\mathscr{P}(S)$ (ili rjeđe s 2^S) i zovemo ga partitivni skup skupa S.*

Ovako definirana relacija biti podskup, tj. relacija "$\subseteq$" ima sljedeća svojstva:

1. Za svaki skup A vrijedi $A \subseteq A$.
2. Ako je $A \subseteq B$ i $B \subseteq A$, onda je $A = B$.
3. Ako je $A \subseteq B$ i $B \subseteq C$, onda je $A \subseteq C$.

Za relaciju koja ima ta svojstva kažemo da je relacija djelomičnog ili parcijalnog uređaja.

Primjer 2.1.6.

a) Ako je $A = \{e, f\}$, onda je $\mathscr{P}(A) = \{\emptyset, \{e\}, \{f\}, \{e, f\}\}$.

b) Ako je $A = \{\&\}$, onda je $\mathscr{P}(A) = \{\emptyset, \{\&\}\}$.

c) Ako je $A = \emptyset$, onda je $\mathscr{P}(A) = \{\emptyset\}$.

Ako skup S ima n elemenata, onda njegov partitivni skup ima 2^n elemenata (iz te činjenice i dolazi oznaka 2^S za partitivni skup skupa S).

Broj elemenata skupa S označit ćemo s $k(S)$ (u literaturi su česte oznake $|S|$ i $\#S$).

Primjer 2.1.7. Za $A = \{\delta\}$ odredimo $\mathscr{P}(\mathscr{P}(A))$.

Rješenje. Očito A ima jedan element (grčko slovo "delta").
$\mathscr{P}(A)$ će, dakle, imati $2^1 = 2$ elementa, a $\mathscr{P}(\mathscr{P}(A)) = 2^2 = 4$ elementa.

$$\mathscr{P}(A) = \{\emptyset, \{\delta\}\}.$$
$$\mathscr{P}(\mathscr{P}(A)) = \{\emptyset, \{\emptyset\}, \{\{\delta\}\}, \{\emptyset, \{\delta\}\}\}.$$

Definicija 2.1.6. *Neka su A i B skupovi.*

1. $A \cup B = \{x : x \in A \text{ ili } x \in B\}$ *(čitamo: A* **unija** *B)*

2. $A \cap B = \{x : x \in A \text{ i } x \in B\}$ *(čitamo: A* **presjek** *B)*

3. $A \setminus B = \{x : x \in A \text{ i } x \notin B\}$ *(čitamo: A* **bez** *B)*

4. $B \setminus A = \{x : x \in B \text{ i } x \notin A\}$

5. $A \triangle B = \{x : x \in A \setminus B \text{ ili } x \in B \setminus A\}$ *(čitamo: A delta B).*
   Operacija $\triangle$ zove se **simetrična razlika.**

6. *Ako je A podskup nekog (većeg) skupa $\mathcal{U}$ ("***univerzalni skup***"), onda definiramo i skup $A^C = \mathcal{U} \setminus A$ i zovemo ga "A* **komplement***".*

7. $A \times B = \{(x, y) : x \in A \text{ i } y \in B\}$ *($A \times B$ čitamo A* **puta** *B).*
   $A \times B$ zovemo **Kartezijev produkt** *skupova A i B.*

8. $A^2 = A \times A = \{(x, y) : x \in A \text{ i } y \in A\}$ *(čitamo: A* **na kvadrat***).*

9. $A^3 = A \times A \times A = \{(x, y, z) : x \in A \text{ i } y \in A \text{ i } z \in A\}$

Primjer 2.1.8. Za $A = \{1, 2\}, B = \{2, 3, 4\}$ vrijedi:

- $A \cup B = \{1, 2, 3, 4\}$

- $A \cap B = \{2\}$

- $A \setminus B = \{1\}$

- $B \setminus A = \{3, 4\}$

- $A \triangle B = \{1, 3, 4\}$

- Ako je $A \subseteq \mathbb{N}$, tada je

$$A^C = \mathbb{N} \setminus A = \{3, 4, 5, 6, \ldots\} = \{x : x \text{ je prirodan broj veći od } 2\}$$

- $A \times B = \{(1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4)\}$

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

- $A^3 = \{(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)\}$

Za skupove A i B za koje vrijedi $A \cap B = \emptyset$ kažemo da su disjunktni.

Ako skup A ima m elemenata, a skup B n elemenata, onda skup $A \times B$ sadrži $m \cdot n$ elemenata. Analogno, ako A ima n elemenata, onda A^2 ima n^2 elemenata, a A^3 ima n^3 elemenata, itd.

Postoji trik kako možemo lakše shvatiti i obavljati operacije sa skupovima. Skupove po tom principu treba gledati kao vreće s nekim sadržajem. $\{\}$ predstavljaju samu vreću, a ono što se nalazi unutar skupa sada je unutar vreće. Naći uniju skupova znači uzeti novu vreću i u nju "istresti" ono što se nalazi u vrećama od kojih pravimo uniju. $\{4,5\} \cup \{7,8\} = \{4,5,7,8\}$, a ako se neki element pojavi više puta, pišemo ga, naravno, samo jednom. $\{4,5\} \cup \{5,8\} = \{4,5,5,8\} = \{4,5,8\}$. Analogno vrijedi za presjek.

Primjer 2.1.9. Odredimo $\{\emptyset, \{\emptyset\}, 4\} \cup \emptyset \setminus \{\emptyset\}$. Prvo uzmemo novu vreću za uniju prvih dvaju skupova. U nju iz prvog ubacimo elemente $\emptyset$, $\{\emptyset\}$ i 4 te iz druge vreće ne ubacimo ništa jer u $\emptyset = \{\}$ nema ništa između { i }. Sada iz te nove vreće samo izvadimo ono što vidimo u $\{\emptyset\}$, a to je samo prazna vreća koja zaista jest u tom prvom skupu. U vreći ostaje $\{\emptyset\}$ i 4 pa je konačno rješenje $\{\{\emptyset\}, 4\}$.

ZADACI ZA VJEŽBU

Zadatak 2.1.1. Za skupove $A = \{1,2,6\}$, $B = \{n \in \mathbb{N} : n^2 < 12\}$, $C = \{\sin \frac{k\pi}{2}, k \in \mathbb{Z}\}$ odredi $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $A \triangle B$, $A \setminus B \setminus C$, $A \setminus (B \setminus C)$, $B \triangle (A \triangle C)$.

Zadatak 2.1.2. Odredi neke skupove A i B za koje je i $A \subseteq B$ i $A \in B$.

Zadatak 2.1.3. Je li

a) $\emptyset \subseteq \emptyset$?

b) $\emptyset \in \emptyset$?

c) $\emptyset \subseteq \{1,2\}$?

d) $\emptyset \in \{1,2\}$?

e) $S \subseteq \emptyset$ za neki skup S?

f) $A \in \mathscr{P}(A)$ za neki skup A?

g) $A \subseteq \mathscr{P}(A)$ za neki skup A?

h) $\emptyset \in \mathscr{P}(A) \setminus \mathscr{P}(B)$ za neke skupove A i B?

i) $\emptyset \subseteq \mathscr{P}(A) \setminus \mathscr{P}(B)$ za neke skupove A i B?

Zadatak 2.1.4. Odredi $\mathscr{P}(\mathscr{P}(\emptyset))$.

Zadatak 2.1.5. Odredi $\mathscr{P}(\mathscr{P}(\{\emptyset,+\}) \setminus \{\emptyset,\{+\}\})$.

Zadatak 2.1.6. Za $A=\{1,2,B\}$, $B=\{1,2\}$ odredi $A \triangle B$.

Zadatak 2.1.7. Odredi neka dva skupa A i B za koja je $\mathscr{P}(A)\cup\mathscr{P}(B)=\mathscr{P}(A\cap B)$.

Zadatak 2.1.8. Odredi neka tri skupa A, B i C za koje vrijedi: $A\cap B\subseteq C\subseteq A\cup B$, $C\in B\setminus A$.

Zadatak 2.1.9. Odredi neka tri skupa A, B i C za koje vrijedi: $A\cap C = A\cup B$, $A\cap B=A\cup C$ i niti jedan od skupova A, B i C nije prazan.

Zadatak 2.1.10. Odredi neke skupove A i B za koje je $k(\mathscr{P}(A))-k(\mathscr{P}(B))=2$.

Zadatak 2.1.11. Odredi skupove A, B i C za koje je

$$\begin{aligned} A\cap B &\neq \emptyset,\\ A\cap C &\neq \emptyset,\\ B\cap C &\neq \emptyset,\\ A\cap B\cap C &= \emptyset. \end{aligned}$$

Rješenja

2.1.1. $A=\{1,2,6\}$,
$B=\{n\in\mathbb{N} : n^2<12\}=\{1,2,3\}$,
$C=\{\sin\frac{k\pi}{2}, k\in\mathbb{Z}\}=\{-1,0,1\}$

$A\cup B=\{1,2,3,6\}$
$A\cap B=\{1,2\}$
$A\setminus B=\{6\}$
$B\setminus A=\{3\}$
$A\triangle B=\{3,6\}$
$A\setminus B\setminus C=\{6\}$
$A\setminus(B\setminus C)=\{1,2,6\}\setminus\{2,3\}=\{1,6\}$
$B\triangle(A\triangle C)=\{1,2,3\}\triangle\{-1,0,2,6\}=\{-1,0,1,3,6\}$.

2.1.2. Uzmimo bilo koji skup A. Npr. $A=\{g,h\}$.
Sada B mora sadržavati, kao i A, elemente g i h. No, mora sadržavati i A pa je $B=\{g,h,\{g,h\}\}$.

2.1.3. a) Ako želimo pokazati da je $\emptyset \subseteq \emptyset$, moramo pokazati da je $x \in \emptyset \Rightarrow x \in \emptyset$ istina. No, $x \in \emptyset$ je uvijek laž, tj. 0, kako smo to označavali u prvom poglavlju ove knjige, a znamo da laž implicira bilo što, tj. da je $0 \to 0$ istina i $0 \to 1$ također istina. Dakle, $\emptyset \subseteq \emptyset$.

b) $\emptyset \notin \emptyset$ jer prazan skup (ovaj s desne strane) nema elemenata.

c) $\emptyset \subseteq \{1,2\}$ je istina jer $\emptyset \subseteq S$ za svaki skup S jer $x \in \emptyset \to x \in S$ je istina jer je $x \in \emptyset$ laž pa nas ne zanima je li $x \in S$ istina ili ne.

d) $\{1,2\}$ ima dva elementa, 1 i 2. $\emptyset$ ne nalazi se kao element u tom skupu pa $\emptyset \notin \{1,2\}$.

e) Je li $S \subseteq \emptyset$ za neki skup S? Ako je $S = \emptyset$, onda je po zadatku a) $\emptyset \subseteq \emptyset$. Odgovor je, dakle, da, $S = \emptyset \subseteq \emptyset$. (No, ako je S bilo koji drugi skup, različit od praznog skupa, tj. ako ima bar jedan element, npr. element $\check{z}$, onda ne vrijedi $S \subseteq \emptyset$ jer bi $S \subseteq \emptyset$ značilo $x \in S \Rightarrow x \in \emptyset$, $\forall x$. A za $x = \check{z}$, $x \in S$ je istina, $x \in \emptyset$ je laž, a $1 \to 0$ je laž pa je $x \in S \Rightarrow x \in \emptyset$ u tom slučaju laž, tj. vrijedi $S \not\subseteq \emptyset$, $\forall S \notin \emptyset$.

f) $A \in \mathscr{P}(A)$ za svaki skup A jer je $\mathscr{P}(A)$ skup svih podskupova skupa A, a i A je jedan od podskupova skupa A, tj. vrijedi $A \subseteq A$ za svaki skup A.

g) Ako je $A = \emptyset$, onda je $A = \emptyset \subseteq \mathscr{P}(A)$ jer je $\emptyset$ podskup svakog skupa. Uočimo kako ovo nije jedini skup s traženim svojstvom, tj. zadatak ima još rješenja.

h) $\emptyset \notin \mathscr{P}(A) \setminus \mathscr{P}(B)$ jer i $\mathscr{P}(A)$ i $\mathscr{P}(B)$ oba sadrže $\emptyset$.

i) $\emptyset \subseteq \mathscr{P}(A) \setminus \mathscr{P}(B)$ za sve skupove A i B jer je $\mathscr{P}(A) \setminus \mathscr{P}(B)$ skup, a $\emptyset$ je podskup svakog skupa, pa onda specijalno i ovoga.

2.1.4. $\mathscr{P}(\emptyset) = \{\emptyset\}$ (jer samo je prazan skup podskup od praznog skupa).
$\mathscr{P}(\mathscr{P}(\emptyset)) = \mathscr{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

2.1.5. $\mathscr{P}(\{\emptyset,+\}) \setminus \{\emptyset,\{+\}\} = \{\emptyset,\{\emptyset\},\{+\},\{\emptyset,+\}\} \setminus \{\emptyset,\{+\}\} = \{\{\emptyset\},\{\emptyset,+\}\}$
$\mathscr{P}(\mathscr{P}(\{\emptyset,+\}) \setminus \{\emptyset,\{+\}\}) = \mathscr{P}(\{\{\emptyset\},\{\emptyset,+\}\}) = \{\emptyset,\{\{\emptyset\}\},\{\{\emptyset,+\}\},\{\{\emptyset\},\{\emptyset,+\}\}\}$.

2.1.6. $\{1,2,B\} \triangle \{1,2\} = \{1,2,\{1,2\}\} \triangle \{1,2\} \overset{(*)}{=} \{\{1,2\}\}$.
(*) i prvi i drugi skup sadržavaju 1 i 2. No, prvi skup ima i skup $\{1,2\}$ kao svoj element, dok drugi skup nema ništa što bi imao samo on, a ne i prvi skup.

2.1.7. Dovoljno je uzeti dva jednaka skupa, tj. $A = B$. Tada je

$$\mathscr{P}(A) \cup \mathscr{P}(A) = \mathscr{P}(A) = \mathscr{P}(A \cap A).$$

2.1.8. $A \cap B \subseteq C \subseteq A \cup B$. C mora biti neki skup "između" $A \cap B$ i $A \cup B$. To nije teško postići. No, C mora u isto vrijeme biti i element od $B \setminus A$, dakle element od B koji nije u A. Dakle, B mora kao element sadržavati skup C.
Uzmimo $A = \emptyset$, $B = \{\beta, \gamma, \{\gamma\}\}$. Sada je $A \cap B = \emptyset$, $A \cup B = B = \{\beta, \gamma, \{\gamma\}\}$. $C \subseteq B$ i C mora biti i element od B. Očito možemo uzeti $C = \{\gamma\}$.

2.1.9. Dovoljno je uzeti bilo koja tri jednaka skupa, tj. $A = B = C$.
Npr. $A = B = C = \{1, 2\}$.
Dalje, iz $A \cap C = A \cup B$ slijedi: Budući da je $A \cap C \subseteq A$ i $A \cap C \subseteq C$, slijedi da je i $A \cup B \subseteq A$ i $A \cup B \subseteq C$, tj. $B \subseteq A$, $A \subseteq C$, $B \subseteq C$. Budući da je $A \cap B \subseteq A$ i $A \cap B \subseteq B$, slijedi da je i $A \cup C \subseteq A$ i $A \cup C \subseteq B$, tj. $C \subseteq A$, $A \subseteq B$, $C \subseteq B$.
Ukupno, i nužan uvjet je $A = B = C$.

2.1.10. Kako je broj elemenata partitivnog skupa skupa S jednak $2^{k(S)}$, tj. $k(\mathscr{P}(S)) = 2^{k(S)}$, tražimo dvije potencije od 2 koje se razlikuju za 2. Potencije broja 2 redom su 1, 2, 4, 8, 16, ... Za 2 se razlikuju 2^2 i 2^1.
Očito treba uzeti skup A od dvaju elemenata i skup B od jednog elementa. Provjerimo: Za $A = \{r, t\}$ i $B = \{e\}$ vrijedi $\mathscr{P}(A) = \{\emptyset, \{r\}, \{t\}, \{r, t\}\}$, $\mathscr{P}(B) = \{\emptyset, \{e\}\}$. $\mathscr{P}(A)$ ima 4 elementa, a $\mathscr{P}(B)$ dva elementa. $4 - 2 = 2$.

2.1.11. A i B imaju zajedničkih elemenata. A i C imaju zajedničkih elemenata. B i C imaju zajedničkih elemenata. No, ne postoji niti jedan element koji je i u A i u B i u C.
Uzmimo npr. $A = \{1, 2\}$, $B = \{1, 3\}$, $C = \{2, 3\}$.

2.2. Vennovi dijagrami. Jednakost skupova.

Cilj je potpoglavlja 2.2. predstaviti dvije metode za određivanje odnosa među skupovima: Vennove dijagrame koji će brzo i jednostavno grafički prikazati odnose zadanih skupova te princip strogog matematičkog dokaza (ili opovrgavanja) zadanog odnosa među zadanim skupovima.

Čitatelj bi nakon potpoglavlja 2.2. trebao znati dokazati u kojem se odnosu nalaze dva zadana skupa (za zadane A i B dokazati kako je $A = B$ ili $A \neq B$ ili $A \supseteq B$ i slično).

Literatura za potpoglavlje 2.2. sljedeće su knjige:

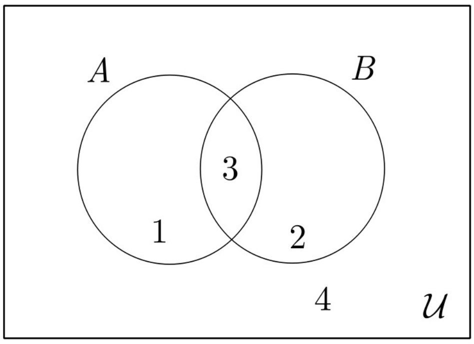
1. P. Papić *Uvod u teoriju skupova*, HMD, Zagreb, 2000.

2. M. Vuković, *Teorija skupova*, predavanja.
https://web.math.pmf.unizg.hr/nastava/ts/materijali/ts-skripta-2015.pdf (zadnji pristup travanj 2022.)

3. https://www.onlinemath4all.com/venn-diagram-problems-and-solutions.html (zadnji posjet stranici travanj 2022.)

Odnose među skupovima predstavljamo Vennovim dijagramima.

Opći položaj dvaju skupova Vennovim dijagramom prikazujemo na sljedeći način:



Slika 2.2.1: Opći položaj dvaju skupova s numeriranim nastalim područjem.

Prikaz je dobar, prikladan jer se na slici zaista nalaze četiri područja koja prikazuju sve četiri mogućnosti za točke s obzirom na pripadnost skupu A ili skupu B.

Točka može biti

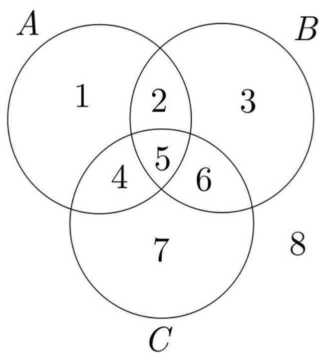
- i u skupu A i u skupu B – to je područje 3,
- može biti u skupu A, ali ne i u skupu B – to je područje 1,
- može biti u skupu B, ali ne i u skupu A – to je područje 2, i na kraju
- može biti izvan skupa A i izvan skupa B – to je područje 4.

Podsjetimo se malo prethodnog poglavlja o logici i tablicom prikažimo sve mogućnosti za točke (elemente) s obzirom na pripadnost nekom od skupova.

Tablica 2.2.1: Smještaj točaka obzirom na dva skupa, gdje nule znače "ne", jedinice "da".

$x \in A$	$x \in B$	Područje
0	0	4
0	1	2
1	0	1
1	1	3

Opći položaj triju skupova Vennovim dijagramom, analogno (sad će tablica imati osam redova za $2^3 = 8$ mogućnosti) prikazujemo na sljedeći način:



Slika 2.2.2: Opći položaj triju skupova.

Tablica 2.2.2: Smještaj točaka u Vennovom dijagramu s obzirom na tri skupa uz nule koje znače "ne" i jedinice koje znače "da".

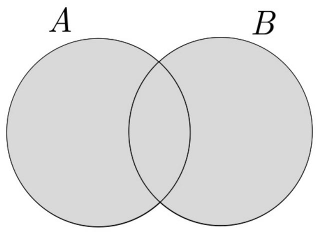
$x \in A$	$x \in B$	$x \in C$	Područje
0	0	0	8
0	0	1	7
0	1	0	3
0	1	1	6
1	0	0	1
1	0	1	4
1	1	0	2
1	1	1	5

Skica općeg položaja četiriju ili više skupova ne može se izvesti kružnicama.

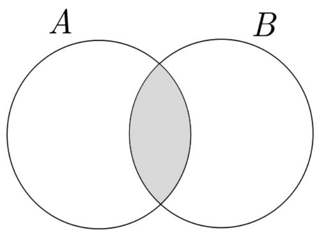
(U slučaju četiriju skupova pripadnost točke nekima od skupova mora biti prikazana s ukupno 16 područja. To je geometrijski nemoguće izvesti kružnicama jer kako god postavili prve tri kružnice, dok crtamo četvrtu, ona može svaku od prethodne tri sjeći u najviše dvije točke. Dakle, može napraviti najviše šest novih sjecišta. To znači da može u sliku uvesti šest novih lukova koji će presjeći šest do četvrte kružnice već prisutnih područja. To znači kako će podijeliti svako od šest navedenih područja na dva dijela. To na kraju znači da će se pojaviti najviše šest novih područja pa će ih uz prethodnih osam biti maksimalno 14, a za prikaz četiriju skupova treba nam 16.)

Ipak, Vennov dijagram za četiri skupa može se pregledno izvesti npr. elipsama.

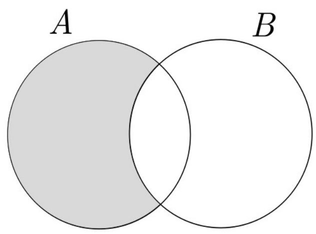
Pogledajmo sada Vennove dijagrame za uniju, presjek i razliku skupova te za simetričnu razliku i komplement skupa.



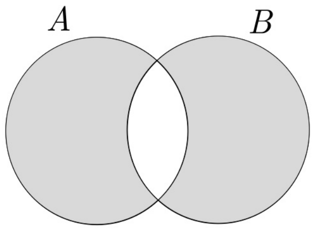
(a) Unija skupova, $A \cup B$



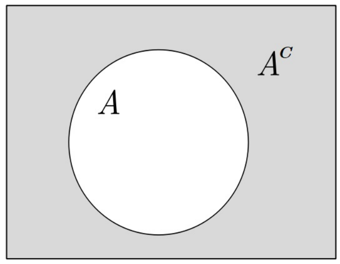
(b) Presjek skupova, $A \cap B$



(c) Razlika skupova, $A \setminus B$



(d) Simetrična razlika skupova, $A \triangle B$

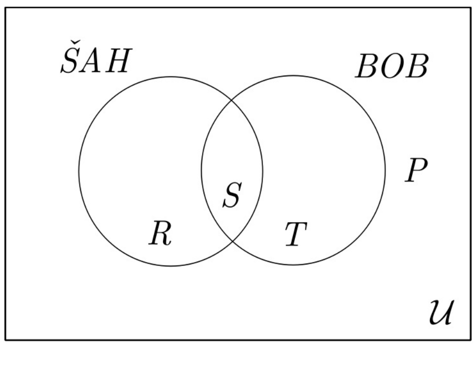


(e) Komplement skupa, A^C

Slika 2.2.3: Vennovi dijagrami za uniju, presjek i razliku skupova te za simetričnu razliku i komplement skupa.

Primjer 2.2.1. U sportskom kampu u kojem su ukupno 22 sportaša, onih koji se ne bave ni šahom ni bobom ima 9, a onih koji se bave samo šahom, i niti jednim sportom više, ima 7. Koliko ima onih koji se bave bobom?

Rješenje. Prikažimo situaciju Vennovim dijagramom.



Slika 2.2.4: Vennov prikaz osoblja kampa.

Cijeli pravokutnik, skup $\mathcal{U}$ broji 22 člana. U području P je 9 osoba, a u području R ih je 7. S i T čine osobe koje se bave bobom. Ukupno u području S i T mora biti ukupno $22 - 9 - 7 = 6$ osoba.

Primjer 2.2.2. Dokažimo komutativnost unije, tj. da za svaka dva skupa T i V vrijedi $T \cup V = V \cup T$.

Rješenje. Vennovim dijagramom, kako se radi o istoj slici (slika 2.2.3a), naslućujemo da zadana jednakost zaista vrijedi.
Dokažimo jednakost skupova $T \cup V$ i $V \cup T$. U tu svrhu, po definiciji jednakosti skupova, moramo dokazati da je $T \cup V \subseteq V \cup T$ i da je $T \cup V \supseteq V \cup T$.

1. Dokažimo $T \cup V \subseteq V \cup T$.
   Neka je $x \in T \cup V$. To znači da je $x \in T$ ili $x \in V$. To znači da je $x \in V$ ili $x \in T$. Dakle, $x \in V \cup T$.

2. Dokažimo $T \cup V \supseteq V \cup T$.
   Neka je $x \in V \cup T$. To znači da je $x \in V$ ili $x \in T$. To znači da je $x \in T$ ili $x \in V$. Dakle, $x \in T \cup V$.

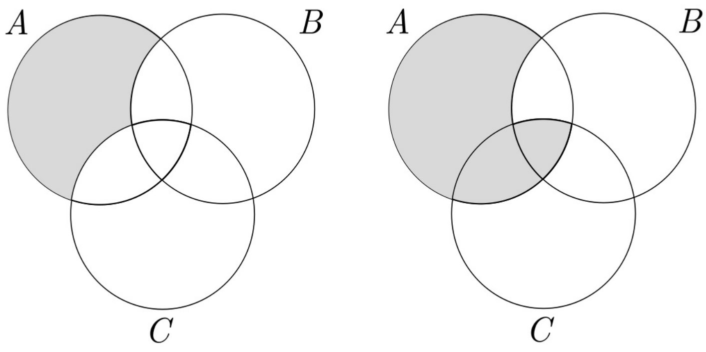
Uočimo kako je srce ovog dokaza formula $A \vee B = B \vee A$ matematičke logike.
Jednakost skupova uvijek se dokazuje po gornjem principu: dokazujemo "$\subseteq$" pa "$\supseteq$".
Ne zaboravimo da pred matematičkim tvrdnjama uvijek stoji izraz "za svaki". Tako da, ako dokazujemo da nešto ne vrijedi, dovoljno je pokazati da to ne vrijedi za jedan jedini primjer vrijednosti veličina koje se pojavljuju u zadanom matematičkom izrazu.

Učenicima osnovne škole objašnjavamo da x^2 nije isto što i $2x$. Tada napišemo: $x^2 \neq 2x$. To nismo smjeli napisati jer ta tvrdnja u stvari znači $\forall x \in \mathbb{R}\ x^2 \neq 2x$. No, za $x = 2$ je $x^2 = 2x$. Također, i za $x = 0$ opet je $x^2 = 2x$.

Primjer 2.2.3. Provjerimo Vennovim dijagramom vrijedi li za proizvoljne skupove A, B i C

$$(A \setminus B) \setminus C = A \setminus (B \setminus C).$$

Rješenje. Skicirajmo lijevu i desnu stranu jednakosti.



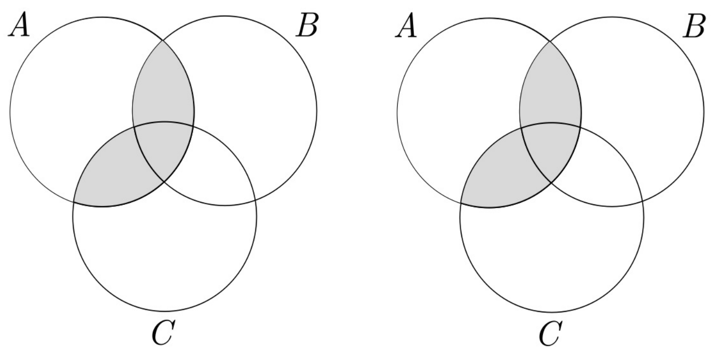
Slika 2.2.5: $(A \setminus B) \setminus C$ i $A \setminus (B \setminus C)$.

Odmah iz slike vidljivo je da zadani skupovi nisu jednaki. Razlikuju se u području $A \cap C$ koje nije podskup lijeve, a jest podskup desne strane jednakosti.
Kako bismo opovrgnuli zadanu matematičku jednakost, dovoljno je pronaći slučaj kada ta jednakost ne vrijedi. Ovdje ćemo uzeti tri skupa kojima je presjek neprazan.
Uzmimo $A = \{1, 2\}$, $B = \{1\}$, $C = \{1, 3\}$.
Sada je $(A \setminus B) \setminus C = \{2\} \setminus \{1, 3\} = \{2\}$, dok je $A \setminus (B \setminus C) = \{1, 2\} \setminus \{\emptyset\} = \{1, 2\}$.
Zaključak: Zadana jednakost nije istinita, jer da je istinita, morala bi biti istinita za sve skupove A, B i C, a nije za $A = \{1, 2\}$, $B = \{1\}$, $C = \{1, 3\}$.

Primjer 2.2.4. Provjerimo Vennovim dijagramom vrijedi li za proizvoljne skupove A, B i C

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{(distributivnost presjeka prema uniji).}$$

Rješenje. Skicirajmo lijevu i desnu stranu jednakosti.



Slika 2.2.6: $A \cap (B \cup C)$ i $(A \cap B) \cup (A \cap C)$

Sada su Vennovi dijagrami jednaki pa krećemo s pokušajem dokazivanja da zadana jednakost uvijek vrijedi. (Skica, naravno, nije matematički dokaz nego samo skica, tj. možda je netočna zbog npr. nepreciznosti ruke ili oka ili papira, ...).
Lijeva i desna strana jednakosti su skupovi pa ovdje moramo dokazati jednakost dvaju skupova. Dva su skupa jednaka ako je prvi podskup od drugoga i drugi podskup od prvoga. Ako želimo dokazati jednakost, moramo, dakle, dokazati dvije stvari:

1. $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ i
2. $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Dokaz tvrdnje 1.: Ovdje moramo dokazati da je lijeva strana podskup od desne, tj. da za svaki x vrijedi: ako je $x \in A \cap (B \cup C)$, onda je $x \in (A \cap B) \cup (A \cap C)$. (Simbol $\Rightarrow$ znači, podsjetimo se, da istinitost tvrdnji s lijeve strane povlači istinitost tvrdnje s desne strane ovog znaka.)

Krenimo:

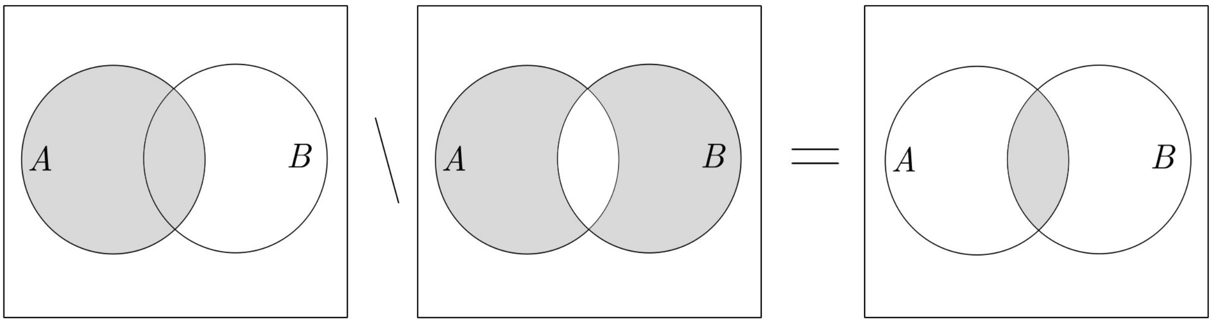
$$\begin{aligned}
x \in A \cap (B \cup C) &\Rightarrow \big(\text{po definiciji presjeka}\big) \Rightarrow x \in A \wedge x \in (B \cup C) \Rightarrow \\
&\Rightarrow \big(\text{po definiciji unije}\big) \Rightarrow x \in A \wedge (x \in B \vee x \in C) \Rightarrow \\
&\Rightarrow \big(\text{zbog distributivnosti konjunkcije prema disjunkciji (zad. 1.2.4. d), str. 24)}\big) \Rightarrow \\
&\Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Rightarrow \\
&\Rightarrow \big(\text{po definiciji presjeka}\big) \Rightarrow (x \in A \cap B) \vee (x \in A \cap C) \Rightarrow \\
&\Rightarrow \big(\text{po definiciji unije}\big) \Rightarrow x \in (A \cap B) \cup (A \cap C).
\end{aligned}$$

Dokaz tvrdnje 2.:

$$\begin{aligned}
x \in (A \cap B) \cup (A \cap C) &\Rightarrow \big(\text{po definiciji unije}\big) \Rightarrow (x \in A \cap B) \vee (x \in A \cap C) \Rightarrow \\
&\Rightarrow \big(\text{po definiciji presjeka}\big) \Rightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \Rightarrow \\
&\Rightarrow \big(\text{zbog distributivnosti (zad. 1.2.4. d), str. 24)}\big) \Rightarrow \\
&\Rightarrow x \in A \wedge (x \in B \vee x \in C) \Rightarrow \\
&\Rightarrow \big(\text{po definiciji unije}\big) \Rightarrow x \in A \wedge x \in (B \cup C) \Rightarrow \\
&\Rightarrow \big(\text{po definiciji presjeka}\big) \Rightarrow x \in A \cap (B \cup C).
\end{aligned}$$

Primjer 2.2.5. Za proizvoljne skupove A i B odredimo $A \setminus (A \triangle B)$.

Rješenje.



Slika 2.2.7: $A \setminus (A \triangle B)$

Dokažimo da je $A \setminus (A \triangle B) = A \cap B$.

$$\begin{aligned}
&x \in A \setminus (A \triangle B) \Rightarrow x \in A \wedge x \notin (A \triangle B) \Rightarrow x \in A \wedge x \notin ((A \setminus B) \cup (B \setminus A)) \Rightarrow \\
&\Rightarrow x \in A \wedge \neg(x \in ((A \setminus B) \cup (B \setminus A))) \Rightarrow x \in A \wedge \neg(x \in (A \setminus B) \vee x \in (B \setminus A)) \Rightarrow \\
&\Rightarrow x \in A \wedge \neg(x \in (A \setminus B)) \wedge \neg(x \in (B \setminus A)) \Rightarrow \\
&\Rightarrow x \in A \wedge \neg(x \in A \wedge x \notin B) \wedge \neg(x \in B \wedge x \notin A) \Rightarrow \\
&\Rightarrow x \in A \wedge (x \notin A \vee x \in B) \wedge (x \notin B \vee x \in A) \Rightarrow
\end{aligned}$$

$$\Rightarrow (x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B) \wedge (x \notin B \vee x \in A) \Rightarrow$$
$$\Rightarrow \emptyset \vee (x \in A \wedge x \in B) \wedge (x \notin B \vee x \in A) \Rightarrow (x \in A \wedge x \in B) \wedge (x \notin B \vee x \in A) \Rightarrow$$
$$\Rightarrow (x \in A \wedge x \in B \wedge x \notin B) \vee (x \in A \wedge x \in B \wedge x \in A) \Rightarrow$$
$$\Rightarrow \emptyset \vee (x \in A \wedge x \in B \wedge x \in A) \Rightarrow x \in A \wedge x \in B \wedge x \in A \Rightarrow x \in A \cap B.$$

Za suprotni smjer, za dokaz $x \in A \cap B \Rightarrow x \in A \setminus (A \triangle B)$, treba samo prethodni niz zaključaka prepisati od zadnjeg prema prvom ili, još jednostavnije, svaki $\Rightarrow$ pretvoriti u $\Leftrightarrow$.

ZADACI ZA VJEŽBU

Zadatak 2.2.1. Za skupove A, B i C u općem položaju skiciraj:

a) $A \cap (B \setminus C)$

b) $A \cup B \triangle C$

c) $C \triangle (A \setminus B)$

d) $A \setminus (B \setminus C)$

e) $A \triangle (B \triangle (A \setminus C))$

Zadatak 2.2.2. Vrijedi li distributivnost unije prema simetričnoj razlici, tj. je li

$$A \cup (B \triangle C) = (A \cup B) \triangle (A \cup C)?$$

Zadatak 2.2.3. Odredi neke skupove A, B i C za koje je

$$A \cup B \setminus C = A \cup (B \setminus C).$$

Zadatak 2.2.4. Neka su A i B skupovi, podskupovi nekog većeg skupa $\mathcal{U}$.
Dokaži:

a) $(A \cup B)^C = A^C \cap B^C$,

b) $(A \cap B)^C = A^C \cup B^C$.

Zadatak 2.2.5. Koristeći samo Vennove dijagrame (bez strogog dokaza) pokušaj naći zapis za skupovnu operaciju $\cap$ koristeći samo sudovne operacije $\cup$ i $\setminus$.

Zadatak 2.2.6. Za zadane skupove A i B riješi skupovnu jednadžbu

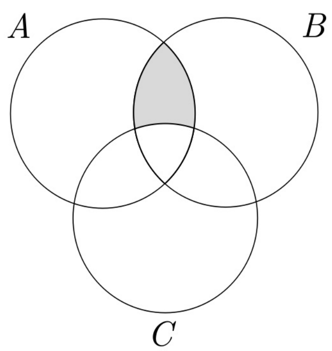
$$A \setminus X = X \setminus B.$$

Zadatak 2.2.7. Vrijedi li općenito $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$?

Zadatak 2.2.8. U nekom razredu ima 22 učenika. Svi su ili lijepi ili pametni ili dobri i nitko nema sve tri dobre karakteristike. Četiri učenika su samo lijepi, jedan učenik je samo pametan, troje samo dobri. Troje su lijepi i pametni, troje lijepi i dobri. Koliko je učenika koji su pametni i dobri?

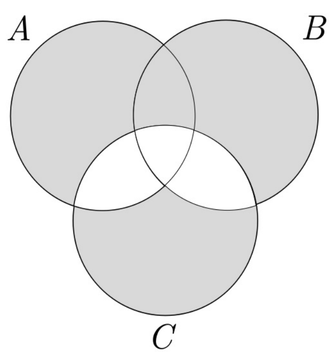
Rješenja

2.2.1. a)



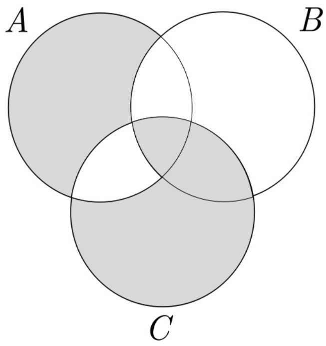
Slika 2.2.8: $A \cap (B \setminus C)$.

b)



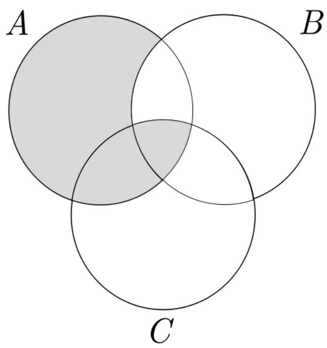
Slika 2.2.9: $A \cup B \triangle C$.

c)



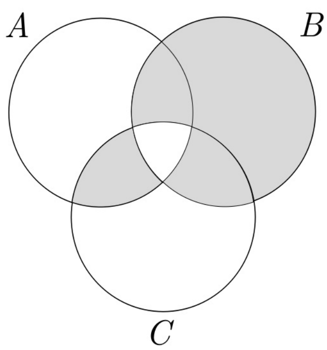
Slika 2.2.10: $C \triangle (A \setminus B)$.

d)



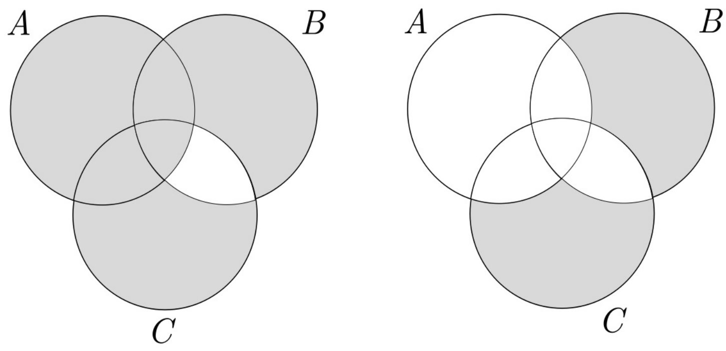
Slika 2.2.11: $A \setminus (B \setminus C)$.

e)



Slika 2.2.12: $A \triangle (B \triangle (A \setminus C))$.

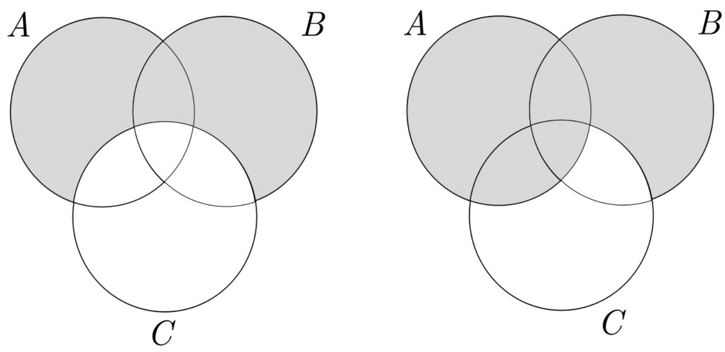
2.2.2.



Slika 2.2.13: $A \cup (B \triangle C)$ i $(A \cup B) \triangle (A \cup C)$.

Distributivnost očito ne vrijedi općenito.
Ne vrijedi na primjer za skupove: $A = \{1, 2\}$, $B = \{2, 3\}$, $C = \{3, 4\}$.
Sada je $A \cup (B \triangle C) = \{1, 2, 4\}$, $(A \cup B) \triangle (A \cup C) = \{4\}$.

2.2.3.



Slika 2.2.14: $A \cup B \setminus C$ i $A \cup (B \setminus C)$.

Očito se lijeva i desna slika razlikuju u dijelu $A \cap C$. Stoga treba odabrati bilo koje skupove A, B i C sa svojstvom da A i C nemaju presjek.
Npr. $A = \{1, 2\}$, $B = \{2, 3, 4\}$, $C = \{3, 4, 5\}$.
Sada je $A \cup B \setminus C = \{1, 2\}$ i $A \cup (B \setminus C) = \{1, 2\}$.

2.2.4. a) $x \in (A \cup B)^C \Leftrightarrow \neg(x \in (A \cup B)) \Leftrightarrow \neg(x \in A \vee x \in B) \Leftrightarrow$

$$\Leftrightarrow \neg(x \in A) \wedge \neg(x \in B) \Leftrightarrow x \in A^C \wedge x \in B^C \Leftrightarrow$$

$$\Leftrightarrow x \in A^C \cap B^C.$$

b) $x \in (A \cap B)^C \Leftrightarrow \neg(x \in (A \cap B)) \Leftrightarrow$

$$\Leftrightarrow \neg(x \in A \wedge x \in B) \wedge \neg(x \in A) \vee \neg(x \in B) \Leftrightarrow$$

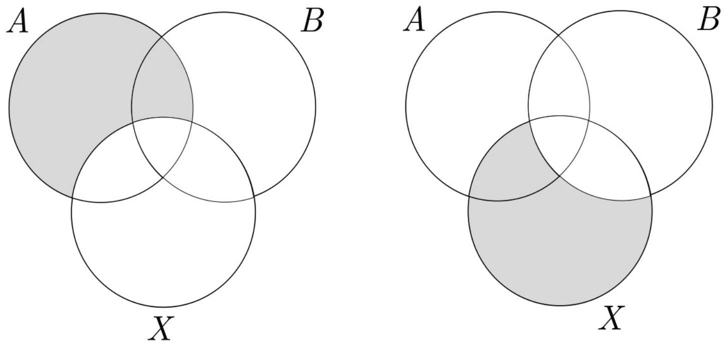
$$\Leftrightarrow x \in A^C \vee x \in B^C \Leftrightarrow x \in A^C \cap B^C.$$

De Morganove formule za skupove direktna su poljedica De Morganovih formula za propozicionalne varijable logike sudova.

2.2.5. Pogledamo li Vennove dijagrame skupova $A \cap B$, $A \cup B$ i $A \setminus B$, uočavamo kako se presjek može dobiti tako da iz cjelokupne unije obaju skupova izbacimo ono što je u $A \setminus B$ i ono što je u $B \setminus A$. Dakle,

$$A \cap B = (A \cup B) \setminus (A \setminus B) \setminus (B \setminus A).$$

2.2.6.



Slika 2.2.15: $A \setminus X$ i $X \setminus B$.

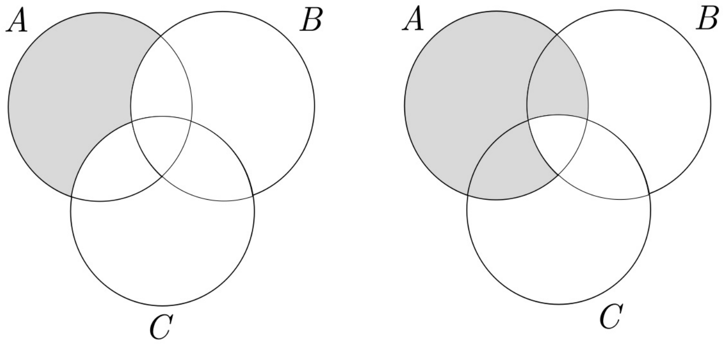
Iz slike 2.2.15 jasno je kako $A \setminus X$ i $X \setminus B$ nemaju niti jedno zajedničko područje ako su A i B u općem položaju pa se čini da ova jednadžba općenito nema rješenje.

$A \setminus X \subseteq X \setminus B \Rightarrow A \setminus X \subseteq X \Rightarrow A \setminus X = \emptyset \Rightarrow A \subseteq X$.
$X \setminus B \subseteq A \setminus X = \emptyset \Rightarrow X \setminus B = \emptyset \Rightarrow X \subseteq B$.

Dakle, rješenje X mora zadovoljavati uvjet $A \subseteq X \subseteq B$.
Za $A \subseteq X \subseteq B$ uvijek će biti $A \setminus X = \emptyset = X \setminus B$.
Dakle, jednadžba ima rješenje samo ako je $A \subseteq B$ i onda je rješenje svaki skup X za kojega vrijedi $A \subseteq X \subseteq B$.
U općem slučaju, ako A nije podskup od B, tj. ako postoji bar jedan element $z \in A \setminus B$, onda u slučaju $z \in X$ vrijedi $z \notin A \setminus X$ i $z \in X \setminus B$, a u slučaju $z \notin X$ vrijedi $z \in A \setminus X$ i $z \notin X \setminus B$.

Kratko, ako nije $A \subseteq B$, onda jednadžba nema rješenja.

2.2.7.

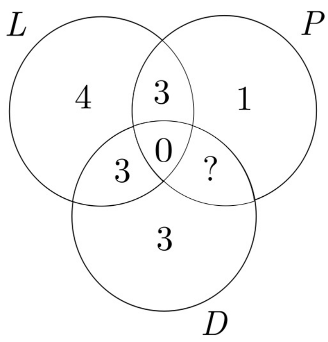


Slika 2.2.16: $A \setminus (B \cup C)$ i $(A \setminus B) \cup (A \setminus C)$.

Iz slike je jasno da navedena relacija ne vrijedi. Iz slike je također jasno kakve A, B i C treba odabrati kako bismo opovrgnuli zadanu izjavu.

Navedena relacija nije točna jer ne vrijedi za $A = \{a, b, c, d\}$, $B = \{a, c\}$, $C = \{b, c\}$. Za te je skupove $A \setminus (B \cup C) = \{d\}$, $(A \setminus B) \cup (A \setminus C) = \{a, b, d\}$.

2.2.8. Na osnovu podataka iz zadatka, označimo tri skupa u općem položaju s L (lijepi), P (pametni) i D (dobri) te upišimo poznate podatke.



Slika 2.2.17: Raspodjela učenika po karakteristikama.

Iz slike je vidljivo kako je samo jedno područje nepoznato. (Uočimo da niti jedno dijete nema sve tri karakteristike pa je u sjecištu svih triju skupova nula, a izvan svih triju skupova je također nula jer svako dijete ima bar jednu od navedenih karakteristika). Ukupno je 22 učenika u razredu pa je $22-(4+3+1+3+0+3) = 8$. Osam je učenika koji su i pametni i dobri.

2.3. Relacije

Do sada smo se u ovom poglavlju bavili uglavnom odnosima između dvaju skupova (skupovi su jednaki ili je jedan podskup od drugoga i slično) i operacijama sa skupovima (kako sve možemo od zadanih skupova kreirati novi skup). U ovom potpoglavlju ući ćemo u strukturu skupa i pokušati uvesti red u njegove elemente, tj. ili ih grupirati po nekom svojstvu (klasificirati ih, razvrstati ih u neke grupe ili podskupove) ili elemente poredati po nekom svojstvu (od najvećeg do najmanjeg, od najjednostavnijeg do najkompliciranijeg itd.).

Cilj je potpoglavlja 2.3. je čitatelju dati osnovna znanja o relacijama i njihovoj ulozi u grupiranju i uspoređivanju elemenata skupova.

Čitatelj bi nakon potpoglavlja 2.3. trebao znati što su relacije te ispitati je li zadana relacija refleksivna, irefleksivna, simetrična, antisimetrična, tranzitivna ili linearna. Dalje, trebao bi znati je li zadana relacija relacija ekvivalencije i ako jest, odrediti klase ekvivalencije te je li zadana relacija relacija uređaja i ako jest, skicirati odnose među elementima te odrediti minimum, minimalni element, maksimum i maksimalni element.

Literatura za potpoglavlje 2.3. sljedeće su knjige:

1. P. Papić, *Uvod u teoriju skupova*, HMD, Zagreb, 2000.
2. M. Vuković, *Teorija skupova*, predavanja.
   https://web.math.pmf.unizg.hr/nastava/ts/materijali/ts-skripta-2015.pdf (Poglavlje 1.6. str. 42)
   (zadnji pristup travanj 2022.)

Podsjetimo se: Ako je A skup, onda je $A^2 = A \times A = \{(x, y) : x \in A, y \in A\}$.

Primjer 2.3.1. Ako je $A = \{a, b, c\}$, onda je

$$A^2 = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c)\}.$$

Definicija 2.3.1. *Neka je A neki skup i A^2 kartezijev produkt skupa A sa samim sobom.* Binarna relacija *na A svaki je podskup od A^2.*

Budući da ćemo promatrati samo binarne relacije, umjesto binarna relacija reći ćemo samo kratko relacija.

Relacije ćemo najčešće označavati grčkim slovom ρ (ro).

Primjer 2.3.2. Za $A = \{a, b, c\}$, $\rho = \{(a, a), (b, b), (a, c)\}$ je jedna relacija na A.

Ako je par (a, b) element relacije ρ, pišemo $(a, b) \in \rho$, ali često i $a \,\rho\, b$ ili $\rho(a, b)$ te za elemente a i b kažemo da su usporedivi s obzirom na relaciju ρ.

Ako skup A ima n elemenata (n je neki prirodan broj), A^2 ukupno ima n^2 elemenata (prvi element para može biti bilo koji od njih n i za taj odabrani prvi element i drugi element para može biti bilo koji od njih n pa je po teoremu o uzastopnom prebrojavanju ukupno n^2 parova u A^2). Samo je jedna relacija s nula elemenata, $\emptyset$. Postoji točno n^2 relacija koje sadrže samo jedan par. Relacija koje sadrže točno dva para ima $\binom{n^2}{2}$, itd. Ukupno, broj svih relacija je

$$\binom{n^2}{0} + \binom{n^2}{1} + \ldots + \binom{n^2}{n^2}$$

a to je binomna formula za $(1+1)$ na potenciju n^2, odnosno 2^{n^2}. Konačno, ako skup A ima n elemenata, onda se na skupu A može odabrati ukupno 2^{n^2} relacija.
Npr. za skup $A = \{d, e, f\}$ koji ima samo tri elementa, sve moguće relacije na skupu A su

$$\emptyset, \{(d, d)\}, \{(d, e)\}, \{(d, f)\}, \{(e, d)\}, \{(e, e)\}, \ldots, A^2,$$

tj. ima ih čak $2^{3^2} = 2^9 = 512$.

Relacije možemo lijepo predstaviti pojavama iz svakodnevnog života jer je sve oko nas u nekoj relaciji s nečim.

Primjer 2.3.3. Pretpostavimo da u kući žive otac Oto (star je 39 godina), majka Maja (stara je 36 godina), sin Silvio (star je 18 godina), kći Ksenija (stara je 16 godina), djed (očev otac) Dino (star je 61 godinu) i baka (očeva majka) Bernarda (stara je 59 godina).

Pogledajmo kako na ovom skupu osoba izgleda relacija "biti u braku". U paru (a, b) bit će osobe koje su u braku, tj. relacija će se sastojati od svih onih parova (a, b) za koje vrijedi da je osoba a u braku s osobom b. Relaciju označimo s BB, a članove obitelji samo prvim slovom njihova imena.

$$BB = \{(a, b) : \text{osoba } a \text{ u braku je s osobom } b\} = \{(O, M), (M, O), (D, B), (B, D)\}.$$

Primjer 2.3.4. Pogledajmo kako na ovom istom skupu osoba izgleda relacija "biti stariji" koja će se sastojati od svih onih uređenih parova (a, b) za koje vrijedi da je osoba a starija od osobe b. Relaciju označimo s BS.

$$\begin{aligned} BS =& \{(D, B), (D, O), (D, M), (D, S), (D, K), (B, O), (B, M), (B, S), (B, K), (O, M), \\ & (O, S), (O, K), (M, S), (M, K), (S, K)\}. \end{aligned}$$

Primjer 2.3.5. Pogledajmo kako na istom skupu izgleda relacija "biti predak od" u kojoj su svi oni parovi (a, b) za koje vrijedi da je a predak od b. Relaciju označimo s BP.

$$BP = \{(D, O), (D, S), (D, K), (B, O), (B, S), (B, K), (O, S), (O, K), (M, S), (M, K)\}.$$

Primjer 2.3.6. Pogledajmo kako na ovom istom skupu izgleda relacija "biti jednako star kao". Relaciju označimo s BJS.

$$\begin{aligned} BJS &= \{(a,b) : \text{osoba } a \text{ jednako je stara kao i osoba } b\} \\ &= \{(D,D),(B,B),(O,O),(M,M),(S,S),(K,K)\}. \end{aligned}$$

Primjer 2.3.7. Pogledajmo kako na ovom istom skupu izgleda relacija "biti istog spola kao". Relaciju označimo s BIS.

$$\begin{aligned} BIS =&\{(a,b) : \text{osoba } a \text{ istog je spola kao i osoba } b\} \\ =&\{(D,D),(D,O),(O,D),(O,O),(D,S),(S,D),(S,S),(O,S),(S,O),(B,B), \\ &(B,M),(M,B),(M,M),(B,K),(K,B),(M,K),(K,M),(K,K)\}. \end{aligned}$$

Primjer 2.3.8. Na skupu svih prirodnih brojeva kreirajmo relaciju "biti iste parnosti" u kojoj su dva broja u paru ako su ili oba parna ili oba neparna.

$$\begin{aligned} &P = \{(x,y) : x \text{ i } y \text{ su ili oba parni brojevi ili oba neparni brojevi}\} \subseteq \mathbb{N}^2 \\ &P = \{(1,1),(1,3),(1,5),\dots,(2,2),(2,4),(2,6),\dots\} \end{aligned}$$

Primjer 2.3.9. Na skupu $\mathbb{N}$ kreirajmo relaciju "dijeli" u kojoj su svi oni parovi prirodnih brojeva sa svojstvom da prvi broj dijeli drugog, tj. da je drugi broj djeljiv s prvim.

$$\begin{aligned} &D = \{(x,y) : x \mid y\} \subseteq \mathbb{N}^2 \\ &D = \{(1,1),(1,2),(1,3),\dots,(2,2),(2,4),(2,6),\dots,(3,3),(3,6),(3,9),\dots\} \end{aligned}$$

Na različitim skupovima možemo, dakle, uvesti različite relacije. Na skupu svih predmeta u sobi možemo gledati što se nalazi iznad čega – dva su predmeta u relaciji "biti ispod" ako je prvi predmet ispod drugog po visini. Ili relaciju "biti lakši od" gdje su opet dva predmeta u relaciji ako je prvi lakši od drugoga.

Bilo koji podskup skupa svih parova elemenata neka je relacija, od praznog skupa pa do skupa svih parova. No, nisu nam sve relacije jednako zanimljive. Promatrat ćemo samo relacije koje imaju neke "lijepe" karakteristike, relacije u sklopu kojih postoji neka pravilnost među navedenim parovima.

Definicija 2.3.2. *Neka je A skup.*

a) Za relaciju $\rho \subseteq A^2$ kažemo da je **refleksivna** *ako vrijedi*

$$\forall\, a \,\big(a \in A \Rightarrow (a,a) \in \rho\big).$$

(Relacija je refleksivna ako vrijedi: koji god element a odaberemo iz skupa A, par (a,a) je u ρ.)

b) Za relaciju $\rho \subseteq A^2$ kažemo da je **irefleksivna** *ako vrijedi*

$$\forall\, a \,\big(a \in A \Rightarrow (a,a) \notin \rho\big).$$

(Relacija je irefleksivna ako vrijedi: koji god element a odaberemo iz skupa A, par (a,a) nije u ρ.)

c) Za relaciju $\rho \subseteq A^2$ kažemo da je **simetrična** *ako vrijedi*

$$\forall\, a\, \forall\, b\, \big((a,b) \in \rho \Rightarrow (b,a) \in \rho\big).$$

(Relacija ρ je simetrična ako vrijedi: ako u ρ postoji par (a,b), onda u ρ mora postojati i suprotni par, (b,a). Suprotan par para (x,y) je par (y,x).)

d) Za relaciju $\rho \subseteq A^2$ kažemo da je **antisimetrična** *ako vrijedi*

$$\forall\, a\, \forall\, b\, \Big(\big((a,b) \in \rho \text{ i } (b,a) \in \rho\big) \Rightarrow a = b\Big).$$

(Relacija ρ je antisimetrična ako vrijedi: ako u ρ postoji par (a,b) i njemu suprotni (b,a), onda su a i b jednaki, tj. $a = b$. Drugim riječima, relacija je antisimetrična ako se u njoj nigdje ne pojavljuje simetrija, tj. i par (a,b) i par (b,a), osim kada se radi o paru jednakih elemenata.)

e) Za relaciju $\rho \subseteq A^2$ kažemo da je **tranzitivna** *ako vrijedi*

$$\forall\, a\, \forall\, b\, \forall\, c\, \Big(\big((a,b) \in \rho \text{ i } (b,c) \in \rho\big) \Rightarrow (a,c) \in \rho\Big).$$

(Relacija ρ je tranzitivna ako vrijedi: ako u ρ postoje parovi (a,b) i (b,c), onda mora postojati i (a,c).)

f) Za relaciju $\rho \subseteq A^2$ kažemo da je **linearna** *ako vrijedi*

$$\forall\, a\, \forall\, b\, ((a \in A \text{ i } b \in A) \;\Rightarrow\; \big((a,b) \in \rho \text{ ili } (b,a) \in \rho\big)).$$

(Relacija ρ je linearna ako vrijedi: koja god dva elementa a i b odabrali iz skupa A, oni su u paru u ρ, tj. u ρ je ili par (a,b) ili par (b,a) ili oba ta para).

Primjer 2.3.10. Neka je $A = \{a,b,c\}$. Neka je

$$\rho = A^2 = \{(a,a),(a,b),(a,c),(b,a),(b,b),(b,c),(c,a),(c,b),(c,c)\}.$$

a) Relacija ρ je refleksivna jer za svaki element x iz A postoji par (x,x) u ρ. Konkretno, u A je element a, a u ρ je par (a,a), u A je element b pa je i u ρ element (b,b), u A je element c, u ρ je element (c,c). Svi iz A u paru su sa samim sobom u ρ.
(Postupak: pregledavamo skup A od elementa do elementa. Ako je svaki od tih elemenata negdje u ρ u paru sa samim sobom, relacija je refleksivna. Ako bar jedan element iz A nije u ρ u relaciji sa samim sobom, zadana relacija nije refleksivna.)

b) Relacija ρ nije irefleksivna jer postoji element u A (npr. element c) koji se nalazi u paru sa samim sobom u ρ (par (c, c) je u ρ). Čim u relaciji postoji par jednakih elemenata, odmah znamo da ta relacija nije irefleksivna.
(Postupak: prolazimo kroz skup A od elementa do elementa, a relacija je irefleksivna ako niti jedan nije u ρ u paru sa samim sobom.)

c) Relacija ρ jest simetrična jer ako je par (x, y) u ρ, onda je i njemu suprotni par također negdje u ρ. Zaista, u ρ je (a, a), a i njemu suprotni (a, a) također je u ρ (to je, naravno, taj isti). Dalje, u ρ je (a, b) pa mora biti negdje i (b, a). I jest. Dalje, u ρ je (a, c) pa mora biti negdje i (c, a). I jest. I tako dalje.
(Postupak: prolazimo kroz skup ρ od para do para i provjeravamo postoji li u ρ za svaki od tih parova i njemu suprotni par u ρ. Ako postoje i svi suprotni parovi, relacija je simetrična. Ako bar jedan suprotni par nedostaje, relacija nije simetrična).

d) Relacija ρ nije antisimetrična jer sadrži i par (a, b) uz par (b, a). (Naravno, sadrži i druge "simetrije" različitih elemenata, npr. (c, b) i (b, c) itd.)
(Postupak: prolazimo kroz skup ρ i pokušavamo za svaki par različitih elemenata pronaći njemu suprotan par u ρ. Nađemo li to, relacija nije antisimetrična. Ne nađemo li slučaj da je u ρ i neki par različitih elemenata (x, y) i njemu suprotan (y, x), relacija je antisimetrična.)

e) Relacija ρ je tranzitivna jer kad se god u njoj pojavljuje neki par (u, v) i drugi (v, z) (prvi par završava s elementom s kojim sljedeći par počinje), onda u relaciji postoji i par (u, z). Zaista, u relaciji je par (a, a), par (a, b), pa je tu i par (a, b). U relaciji je par (c, a), par (a, b), pa je u njoj i par (c, b) itd. U ovom slučaju tranzitivnost je posljedica činjenice da su u relaciji baš svi parovi elemenata iz A, pa onda i specijalni koji će potvrditi tranzitivnost.
(Postupak: prolazimo kroz relaciju i tražimo parove (x, y) i (y, z) za koje u relaciji ne postoji par (x, z). Nađemo li takvu situaciju, relacija nije tranzitivna. Ne nađemo li takvu situaciju, tranzitivna je.)

f) Relacija ρ je linearna jer koje god elemente x i y odabrali iz skupa A, oni se u paru nalaze negdje u relaciji ρ.
(Postupak: provjeravamo postoje li neki elementi x i y u skupu A (možda i jednaki) za koje vrijedi da ni par (x, y) ni par (y, x) nisu u ρ. Nađemo li takve elemente, relacija nije linearna. Ne nađemo li ih, tj. točnije, ako takvi elementi ne postoje, linearna je.)

Uočimo da za provjeru refleksivnosti, irefleksivnosti i linearnosti provjeravamo elemente zadanog skupa A, dok za simetričnost, antisimetričnost i tranzitivnost skup A ne moramo ni poznavati, nego samo parovi u ρ odlučuju vrijede li ta svojstva ili ne (svakako se podrazumijeva $\rho \subseteq A^2$).

Primjer 2.3.11. Neka je $X = \{a, b, c\}$, $R = \{(a, a), (b, b), (a, c)\} \subseteq X^2$.

a) $a \in X$ i $(a, a) \in R$.
$b \in X$ i $(b, b) \in R$.
$c \in X$, ali $(c, c) \notin R$.
Zbog $c \in X$ i $(c, c) \notin R$ relacija nije refleksivna.

b) Relacija R nije irefleksivna jer sadrži par (a, a) jednakih elemenata.

c) Relacija nije simetrična jer sadrži par (a, c), ali ne sadrži njemu suprotan par (c, a).

d) Relacija R jest antisimetrična jer ne sadrži i par (x, y) i (y, x) za neke različite x i y. Jedini par različitih elemenata koji se nalazi u R je par (a, c). Da je u R i par (c, a), R ne bi bila antisimetrična. Budući da para nema relacija je antisimetrična.

e) Relacija je tranzitivna.
Parovi koje možemo vezati su (a, a) i (a, a), a za njih je i $(a, a) \in R$, zatim parovi (a, a) i (a, c), a za njih je i $(a, c) \in R$ te na kraju parovi (b, b) i (b, b), a za njih je i $(b, b) \in R$. Za svaka dva para koji su povezani "srednjim" elementom postoji i treći par koji po definiciji tranzitivnosti tu mora biti.

f) Relacija nije linearna jer ako iz skupa odaberemo elemente a i b, vidimo da oni nisu usporedivi, tj. par (a, b) nije element relacije R. Mogli smo za "rušenje" svojstva linearnosti odabrati i elemente b i c jer relacija R ne sadrži ni (b, c) ni (c, b).

Primjer 2.3.12. Neka je Obitelj $= \{O, M, D, B, S, K\}$ (vidi primjer 2.3.3).
Ispitaj relaciju

$$BB = \{(O, M), (M, O), (D, B), (B, D)\}.$$

Rješenje.

a) <u>Refleksivnost:</u>
$O \in$ Obitelj i $(O, O) \notin BB$. Relacija nije refleksivna jer smo pronašli element iz skupa Obitelj za kojeg vrijedi da nije u paru sa samim sobom u zadanoj relaciji.

b) <u>Irefleksivnost:</u>
$O \in$ Obitelj i $(O, O) \notin BB$.
$M \in$ Obitelj i $(M, M) \notin BB$.
$D \in$ Obitelj i $(D, D) \notin BB$.
$B \in$ Obitelj i $(B, B) \notin BB$.
$S \in$ Obitelj i $(S, S) \notin BB$.
$K \in$ Obitelj i $(K, K) \notin BB$.
Niti jedan element iz polaznog skupa nije u paru sa samim sobom u relaciji.
Relacija je irefleksivna.

c) Simetričnost:
Za $(O,M) \in BB$ i $(M,O) \in BB$.
Za $(M,O) \in BB$ i $(O,M) \in BB$.
Za $(D,B) \in BB$ i $(B,D) \in BB$.
Za $(B,D) \in BB$ i $(D,B) \in BB$.
Za svaki, dakle, par koji se nalazi u BB, postoji i njemu simetrični koji se također nalazi u BB.
Relacija je simetrična.

d) Antisimetričnost:
$(O,M) \in BB$ i $(M,O) \in BB$ i $M \neq O$.
U relaciji postoje suprotni parovi različitih elemenata.
Relacija BB nije antisimetrična.

f) Tranzitivnost:
$(O,M) \in BB$ i $(M,O) \in BB$ i $(O,O) \notin BB$.
Relacija nije tranzitivna.

g) Linearnost:
$O \in$ Obitelj i $S \in$ Obitelj i $(O,S) \notin BB$ i $(S,O) \notin BB$.
Pronašli smo dva elementa iz zadanog skupa Obitelj, O i S, koji nisu usporedivi, tj. nisu u paru u BB.
Relacija nije linearna.

Definicija 2.3.3. *Relacija koja je refleksivna, simetrična i tranzitivna zove se **relacija ekvivalencije**.*

Primjer 2.3.13. Na skupu $A = \{f, g, h\}$ relacija

$$\rho = \{(f,f), (g,g), (h,h), (f,g), (g,f)\}$$

je refleksivna, simetrična i tranzitivna pa je ona relacija ekvivalencije.

Primjer 2.3.14. Na skupu $A = \{f, g, h\}$ relacija

$$\rho = \{(f,f), (g,g), (h,h), (f,g), (g,f), (f,h), (h,f)\}$$

je refleksivna i simetrična, ali nije tranzitivna pa ona nije relacija ekvivalencije.

Definicija 2.3.4. *Neka je A skup i ρ relacija ekvivalencije na A. Neka je x neki element iz skupa A. Za elemente koji su u relaciji s x (s njim u paru), kažemo da su **ekvivalentni s** x.*

Primjer 2.3.15. U primjeru 2.3.13. s elementom $f \in A$ u paru su f i g. Stoga kažemo da su f i g ekvivalentni s elementom f.
S elementom $g \in A$ ekvivalentni su f i g.
S elementom h ekvivalentan je samo h.

Definicija 2.3.5. *Neka je A skup i ρ relacija ekvivalencije na A. Za $x \in A$ skup svih onih elemenata koji su s njim u paru, tj. koji su (po prethodnoj definiciji) s njim ekvivalentni, zovemo* **klasa ekvivalencije elementa x po relaciji ρ**, *ili kraće,* **klasa od x po ρ**. *Često ćemo, ako je jasno o kojoj se relaciji radi, reći samo klasa od x. Klasu od x po ρ označavamo s $[x]$.*

Primjer 2.3.16. U primjeru 2.3.13. s elementom $f \in A$ u paru su f i g. Stoga je klasa od f skup $[f] = \{f, g\}$.
S elementom $g \in A$ ekvivalentni su f i g. Stoga je klasa od g skup $[g] = \{f, g\}$.
S elementom $h \in A$ ekvivalentan je samo h. Stoga je klasa od h skup $[h] = \{h\}$.

Uočimo da su klase od f i g jednake, tj. $[f] = [g]$, a klasa od f i klasa od h su disjunktne, tj. nemaju zajedničkih elemenata.

Teorem 2.3.1. *Neka je A skup i ρ relacija ekvivalencije na A. Neka su $x \in A$ i $y \in A$ dva elementa skupa A. Klase ekvivalencije elemenata x i y s obzirom na relaciju ρ, tj. $[x]$ i $[y]$ su ili jednake ili nemaju zajedničkih elemenata.*

Dokaz. Pokazat ćemo da ako $[x]$ i $[y]$ imaju bar jedan zajednički element, onda je i bilo koji preostali element iz bilo koje od tih klasa zajednički, tj. da su dvije klase, ako imaju bar jedan zajednički element, jednake.

Pretpostavimo da $[x]$ i $[y]$ imaju zajednički element z, tj. $z \in [x]$ i $z \in [y]$.
Ako je z jedini element u tim skupovima, oni su jednaki.
Ako u $[x]$ postoji osim tog elementa z i još bar jedan element u, tj. $u \in [x]$, $u \neq z$, slijedi:
Budući da je $u \in [x]$, slijedi da je $(u, x) \in \rho$.
Budući da je $z \in [x]$, slijedi da je $(x, z) \in \rho$.
Zbog tranzitivnosti, ako je $(u, x) \in \rho$ i $(x, z) \in \rho$, mora biti onda i $(u, z) \in \rho$.
Budući da je $z \in [y]$, slijedi da je $(z, y) \in \rho$.
Zbog tranzitivnosti, ako je $(u, z) \in \rho$ i $(z, y) \in \rho$, onda mora biti i $(u, y) \in \rho$, a to znači da je $u \in [y]$.
Iz ovoga u stvari slijedi da je $[x]$ podskup od $[y]$.
Na isti način pokazujemo da ako $[y]$ sadrži neki element u, onda je, uz pretpostavku da te dvije klase sadrže bar jedan zajednički element, u element i od $[x]$. Dakle, $[x]$ je podskup $[y]$ i obrnuto, što znači $[x] = [y]$.
Slijedi: Ako dvije klase imaju bar jedan zajednički element, one su jednake. □

Definicija 2.3.6. *Neka je S neki skup.* **Particija** *(negdje u literaturi* **podjela** *ili* **razredba***) skupa S je familija podskupova S_1, S_2, S_3, ... od S za koju vrijedi da su svi skupovi S_1, S_2, S_3, ... međusobno disjunktni (ne postoje dva od njih koja imaju zajednički element), neprazni (niti jedan od njih nije $\emptyset$) i u uniji čine cijeli skup S, tj. $S_1 \cup S_2 \cup S_3 \cup \ldots = S$. Pišemo: $\mathcal{P} = \{S_1, S_2, S_3, \ldots\}$ je particija skupa S.*

Primjer 2.3.17. Za $S = \{a, s, d, f\}$ jedna od particija je $\mathcal{P}_1 = \{\{a, s\}, \{d, f\}\}$. Druga je $\mathcal{P}_2 = \{\{s\}, \{d, a, f\}\}$.

Skup $\mathcal{P}_3 = \{\emptyset, \{a, s, d\}, \{f\}\}$ nije particija jer svi skupovi u particiji moraju biti neprazni, tj. particija ne smije sadržavati prazan skup.
Skup $\mathcal{P}_4 = \{\{a, s, d\}, \{s, f\}\}$ nije particija jer svi skupovi u particiji moraju biti disjunktni, a skupovi u $\mathcal{P}_4$ sadrže zajednički element s.

Svaka particija skupa (podjela skupa na podskupove) prirodno generira relaciju ekvivalencije na tom skupu. To jest, ako je zadan skup S i ako je $\mathcal{P} = \{S_1, S_2, S_3, \ldots\}$ neka particija od S, onda je

$$\rho = \{(a, b) : \text{ postoji } S_i, i = 1, 2, 3, \ldots \text{ takav da su i } a \text{ i } b \text{ elementi od } S_i\}$$

relacija ekvivalencije (u ρ su oni parovi elemenata skupa S koji pripadaju istom podskupu S_i iz particije).

Očito je relacija ρ refleksivna jer ako je $a \in S_i$ za neki $i = 1, 2, 3, \ldots$, onda je i $(a, a) \in \rho$ (jer i a i a pripadaju obama podskupovima S_i), a svi elementi skupa S u nekom su podskupu iz particije.

Očito je relacija ρ simetrična jer ako a i b pripadaju istom podskupu iz particije, onda mu, naravno, i b i a pripadaju, tj. iz $(a, b) \in \rho$ slijedi $(b, a) \in \rho$.

Relacija ρ je i tranzitivna jer $(a, b) \in \rho$ i $(b, c) \in \rho$ redom znači da su a i b iz jednog te istog podskupa zadane particije te su b i c iz nekog, jednog te istog, podskupa zadane particije. Kako se radi o particiji skupa, tj. dva skupa particije nemaju zajedničkih elemenata, slijedi da su i a i b i c iz istog podskupa zadane particije pa je $(a, c) \in \rho$.

Primjer 2.3.18. Za $S = \{a, b, c, d\}$ i za particiju je $\mathcal{P}_1 = \{\{a\}, \{b\}, \{c, d\}\}$, pripadna relacija ekvivalencije je

$$\rho = \{(a, a), (b, b), (c, c), (c, d), (d, c), (d, d)\}.$$

Za particiju $\mathcal{P}_2 = \{\{a, b, c\}, \{d\}\}$, pripadna relacija ekvivalencije je

$$\rho = \{(a, a), (a, b), (a, c), (b, a), (b, b), (b, c), (c, a), (c, b), (c, c), (d, d)\}.$$

Primjer 2.3.19. Skup svih pravaca neke ravnine M možemo podijeliti na podskupove tako da u svakom podskupu budu međusobno paralelni pravci. Sada ta particija "inducira" (potiče, stvara) relaciju ekvivalencije

$$\begin{aligned} \rho &= \{(a, b) : a \text{ i } b \text{ su međusobno paralelni pravci ravnine } M\} \\ &= \{(a, b) : a \in M, b \in M, a \parallel b\}. \end{aligned}$$

(Dogovorno uzimamo da je svaki pravac paralelan sa samim sobom.)

Primjer 2.3.20. Ako prirodne brojeve podijelimo na parne i neparne, to je očito particija skupa $\mathbb{N}$. Ali, onda je, naravno, i relacija

$$R = \{(a, b) : a \text{ i } b \text{ su iste parnosti, tj. ili su oba broja parna ili su oba neparna}\}$$

relacija ekvivalencije. Zaista,

1. a je iste parnosti kao i a za svaki prirodni broj a,
2. ako su a i b iste parnosti, onda su i b i a iste parnosti i
3. ako su a i b iste parnosti i b i c su iste parnosti, onda su i a i c iste parnosti.

Primjer 2.3.21. Ako sve pravokutnike zadane ravnine M podijelimo po površini, onda smo opet očito dobili particiju svih pravokutnika ravnine jer svaki je pravokutnik u nekoj klasi (jer ima površinu) i jer pravokutnik ne može pripadati različitim klasama (jer ima samo jednu, fiksnu, površinu). Onda je, naravno, i relacija

$$R = \{(K, L) : K \text{ i } L \text{ su pravokutnici iste površine}\}$$

relacija ekvivalencije.

Pokazali smo sada kako svaka particija skupa inducira neku relaciju ekvivalencije.

Također, i svaka relacija ekvivalencije inducira neku particiju.

Ako je ρ relacija ekvivalencije na skupu S, upravo će klase ekvivalencije činiti particiju zadanog skupa. Pokazali smo u teoremu 2.3.1 kako su klase ekvivalencije međusobno disjunktne i svaki se od elemenata zadanog skupa S nalazi u nekoj od klasa, to je baš definicija particije skupa.

Primjer 2.3.22. Neka je na skupu $\mathbb{N}$ zadana relacija $\rho = \{(a, b) : a + b \text{ je paran broj}\}$. Očito je ρ relacija ekvivalencije.

1. Refleksivnost: Zbroj svakih dvaju jednakih prirodnih brojeva je paran broj.
2. Simetričnost: Ako je $a + b$ paran broj, onda je i $b + a$ paran broj.
3. Tranzitivnost: Ako je $a + b$ paran broj i $b + c$ je paran broj, onda je i njihov zbroj $a+b+b+c$ paran broj. Ako tom parnom broju $a+b+b+c$ oduzmemo paran broj $b + b$, ono što ostane mora biti paran broj, tj. $a + c$ je paran broj.

Ova relacija ρ će podijeliti $\mathbb{N}$ na disjunktne klase ekvivalencije koje čine particiju skupa $\mathbb{N}$.

Dvije disjunktne klase koje u uniji čine cijeli $\mathbb{N}$ su

$$[1] = \{1, 3, 5, 7, 9, \ldots\} \quad \text{i}$$
$$[2] = \{2, 4, 6, 8, 10, \ldots\}.$$

Dalje, $[3] = [1]$, $[4] = [2]$, ...
Klasu $[1] = \{1, 3, 5, 7, 9, \ldots\}$ zovemo i $\mathbf{2\mathbb{N} - 1}$, a klasu $[2] = \{2, 4, 6, 8, 10, \ldots\}$ zovemo $\mathbf{2\mathbb{N}}$.

Definicija 2.3.7. *Ako je na nekom skupu S zadana relacija ekvivalencije ρ, onda skup svih klasa ekvivalencije, s obzirom na relaciju ρ, označavamo sa $S\mid_\rho$ i taj skup zovemo* **kvocijentni skup** *skupa S obzirom na relaciju ρ.*

Kažemo da se skup $\mathbb{N}$ s obzirom na relaciju ρ iz gornjeg primjera podijelio na klase ekvivelencije (podskupove) [1] i [2] i to zapisujemo s

$$\mathbb{N}\mid_\rho = \{[1],[2]\} = \{\{1,3,5,7,9,\ldots\},\{2,4,6,8,10,\ldots\}\}.$$

Za sljedeći primjer potrebna nam je točna definicija djeljivosti.

Definicija 2.3.8. *Neka je $a \in \mathbb{Z}$ i $b \in \mathbb{N}$. Kažemo da je cijeli broj a djeljiv prirodnim brojem b i pišemo $a \vdots b$ ako postoji cijeli broj k takav da je $a = kb$. Često kažemo i da b dijeli a i to pišemo u obliku $b|a$.*

Primjer 2.3.23. Broj -8 je djeljiv s 1, 2, 4 i 8. Broj 0 je djeljiva sa svim prirodnim brojevima.

Primjer 2.3.24. Neka je na skupu $\mathbb{Z}$ zadana relacija $R = \{(a,b) : a-b \text{ je djeljiv s } 3\}$. Očito je ρ relacija ekvivalencije.

1. Refleksivnost: Razlika svakih dvaju jednakih cijelih brojva je nula, a nula je djeljiva s 3.
2. Simetričnost: Ako je $a-b$ djeljiv s 3, onda je i $b-a = -(a-b)$ djeljiv s 3.
3. Tranzitivnost: Ako je $a-b$ djeljiv s 3 i ako je $b-c$ djeljiv s 3, onda je i njihov zbroj $a-b+b-c$ djeljiv s 3, a zbroj je $a-b+b-c = a-c$.

R će razdijeliti $\mathbb{Z}$ na disjunktne klase ekvivalencije koje čine particiju skupa $\mathbb{Z}$.

Disjunktne klase koje u uniji čine cijeli $\mathbb{Z}$ su

$$\begin{aligned}
[0] &= \{\ldots,-6,-3,0,3,6,9,12,\ldots\} = \mathbf{3\mathbb{Z}},\\
[1] &= \{\ldots,-5,-2,1,4,7,10,13,\ldots\} = \mathbf{3\mathbb{Z}+1} \quad \text{i}\\
[2] &= \{\ldots,-4,-1,2,5,8,11,14,\ldots\} = \mathbf{3\mathbb{Z}+2}.
\end{aligned}$$

Kažemo da se skup $\mathbb{Z}$ s obzirom na relaciju R podijelio na klase ekvivelencije (podskupove) [0], [1] i [2] i to zapisujemo na neki od sljedećih načina:

$$\begin{aligned}
\mathbb{Z}\mid_R =& \{[0],[1],[2]\} = \{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}\\
=& \{\{\ldots,-6,-3,0,3,6,9,12,\ldots\},\{\ldots,-5,-2,1,4,7,10,13,\ldots\},\\
& \{\ldots,-4,-1,2,5,8,11,14,\ldots\}\}.
\end{aligned}$$

U temelju prethodnog primjera nalazi se teorem o dijeljenju s ostatkom: Za brojeve $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ postoje brojevi $q \in \mathbb{Z}$ i $r \in \{0, 1, \ldots, b-1\}$ takvi da je $a = q \cdot b + r$. Broj q zovemo količnik (kvocijent), a r ostatak pri cjelobrojnom dijeljenju broja a brojem b. Npr. $17 : 3 = 5$ i ostatak je 2 ili $17 = 5 \cdot 3 + 2$, $(-9) : 5 = -2$ i ostatak 1, ili $-9 = (-2) \cdot 5 + 1$.

Na osnovu relacije ekvivalencije, dakle, (smisleno) po nekom svojstvu možemo grupirati elemente tog skupa.

Sada ćemo vidjeti što je to relacija uređaja i što znači po njoj uspoređivati elemente zadanog skupa, poredati ih u niz po nekom svojstvu i slično.

Definicija 2.3.9. *Neka je A skup. Relaciju ρ na skupu A koja je refleksivna, antisimetrična i tranzitivna zovemo* **uređaj**, *a za skup A kažemo da je zajedno s relacijom ρ uređen skup. Negdje se takva relacija zove i* **parcijalni uređaj**.

Primjer 2.3.25. Na skupu $\mathbb{N}$ uobičajeni "manje ili jednako od", oznaka $\leq$, je uređaj.

$$\text{“} \leq \text{”} = \{(a, b) : a \leq b\}$$

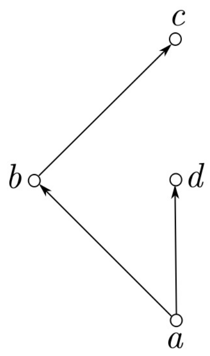
(Uočimo da $a \leq b$ iz početnih razreda osnovne škole u stvari znači $(a, b) \in \leq$. Možemo pisati i $\leq (a, b)$).
Zaista, svaki prirodan broj je manji ili jednakog od samog sebe, pa je $\leq$ refleksivna, nije moguće $a \leq b$ i $b \leq a$ za različite a i b, a ako je $a \leq b$ i $b \leq c$, vrijedi da je i $a \leq c$ pa je $\leq$ i tranzitivna relacija, dakle relacija uređaja.

Primjer 2.3.26. Neka je $A = \{a, b, c, d\}$. Neka je

$$\rho = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, c)\}.$$

Očito je relacija ρ refleksivna jer sadrži sve "jednake parove", očito je antisimetrična jer ne sadrži niti jedan par različitih elemenata i u isto vrijeme njemu suprotni par i na kraju je i tranzitivna jer (a, b) i (b, c) su jedini "netrivijalni" parovi koje možemo "spojiti" u tranzitivnosti, no i (a, c) je u ρ pa je ρ stoga tranzitivna.
Dakle, ρ je relacija uređaja.

Uređaj često prikazujemo slikom. Pri tom se, ako se u uređaju ρ, nalazi par (x, y), na slici crta usmjerena dužina (vektor) od točke x do točke y, najčešće odozdo prema gore. Dalje, ako se, kao u ovom primjeru, u relaciji nalaze u paru neki elementi (x, y) i (y, z), njih također crtamo, no budući da znamo da je ovakva relacija tranzitivna, par (x, z) nije potrebno crtati. Stoga skica uređaja iz primjera 2.3.26 izgleda ovako:



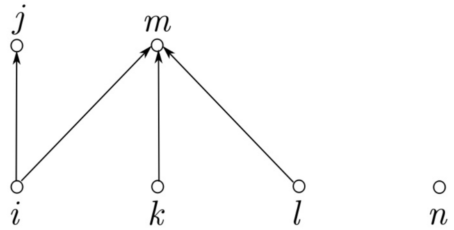
Slika 2.3.1: Uređaj $\rho = \{(a,a),(b,b),(c,c),(d,d),(a,b),(a,c),(a,d),(b,c)\}$ na skupu $\{a,b,c\}$.

Primjer 2.3.27. Neka je $B = \{i,j,k,l,m,n\}$. Neka je

$$\rho = \{(i,i),(j,j),(k,k),(l,l),(m,m),(n,n),(i,j),(i,m),(k,m),(l,m)\}.$$

ρ je relacija uređaja.

Skica uređaja iz primjera 2.3.27. izgleda ovako:



Slika 2.3.2: Uređaj $\rho = \{(i,i),(j,j),(k,k),(l,l),(m,m),(n,n),(i,j),(i,m),(k,m),(l,m)\}$ na skupu $B = \{i,j,k,l,m,n\}$.

Definicija 2.3.10. *Neka je S skup i neka je ρ relacija uređaja na S.*

a) Ako za neki element m skupa S (ako takav postoji) vrijedi da je

$$(m,s) \in \rho, \ \forall s \in S,$$

onda takav element m zovemo **minimum** *skupa S s obzirom na relaciju ρ.*
Minimum je drugim riječima element koji je usporediv sa svim elementima i uvijek je on prvi u paru u relaciji.

b) Ako za neki element M skupa S (ako takav postoji) vrijedi da je

$$(s,M) \in \rho, \ \forall s \in S,$$

onda takav element M zovemo **maksimum** *skupa S s obzirom na relaciju ρ.*
Maksimum je drugim riječima element koji je usporediv sa svim elementima i uvijek je on drugi u paru u relaciji.

c) *Ako za neki element m skupa S vrijedi $(a, m) \in \rho \to a = m, \forall a \in S$, onda takav element m zovemo* **minimalni element** *skupa S s obzirom na relaciju ρ.*
Minimalni je element drugim riječima element koji nikad nije drugi u paru u relaciji, osim kada je u relaciji sa samim sobom. Možda uopće nigdje nije u paru. No, ako jest u paru, onda je uvijek prvi.

d) *Ako za neki element M skupa S vrijedi $(M, a) \in \rho \to a = M, \forall a \in S$, onda takav element M zovemo* **maksimalni element** *skupa S obzirom na relaciju ρ.*
Maksimalni je element drugim riječima element koji nikad nije prvi u paru u relaciji, osim kada je u paru sa samim sobom.

Primjer 2.3.28. Neka je $S = \{g, h, j, k\}$. Neka je

$$\begin{aligned}
\rho_1 &= \{(g, g), (h, h), (j, j), (k, k), (j, h), (j, g), (j, k)\},\\
\rho_2 &= \{(g, g), (h, h), (j, j), (k, k), (j, h), (k, g)\} \quad \text{i}\\
\rho_3 &= \{(g, g), (h, h), (j, j), (k, k), (h, j)\}.
\end{aligned}$$

S obzirom na relaciju uređaja ρ_1, j je minimum i minimalni element u S, maksimuma nema, a g, h i k su maksimalni elementi.
S obzirom na relaciju uređaja ρ_2, minimuma nema, a minimalni elementi su j i k. Maksimuma nema, a h i g su maksimalni elementi.
S obzirom na relaciju uređaja ρ_3, h je minimalni element, j je maksimalni element, a minimuma i maksimuma nema. Također, g i k su i minimalni elementi i maksimalni elementi.

Ako je S skup i ρ relacija uređaja na S, onda minimum ili ne postoji ili postoji pa je jedinstven, tj. u relaciji uređaja ne mogu postojati dva minimuma.
(Jer, da su m i n dva minimuma, moralo bi biti i $(m, n) \in \rho$ i $(n, m) \in \rho$, pa bi zbog antisimetričnosti moralo biti $m = n$.)

Zadaci za vježbu

Zadatak 2.3.1. Neka je $A = \{1, 2, 3\}$. Ispitaj relaciju $I = \{(1, 1), (2, 2), (3, 3)\} \subseteq A^2$.
(Skup svih jednakih parova zadanog skupa zove se dijagonala tog skupa. Prikažemo li skup A^2 u kordinatnom sustavu, dobivamo 9 točaka koje "čine kvadrat", a I je dijagonala tog kvadrata. Za $A = [0, 1]$ A^2 je zaista kvadrat, a točke oblika (x, x), $x \in [0, 1]$ čine njegovu dijagonalu.)

Zadatak 2.3.2. Ispitaj relaciju $\rho = \{(x, y) : x \text{ je djeljiv s } y\} \subseteq \mathbb{N}^2$.
Ako je ρ relacija ekvivalencije, odredi klase ekvivalencije tj. kvocijentni skup skupa $\mathbb{N}$ s obzirom na relaciju ρ.
Ako je ρ relacija uređaja, odredi minimum, minimalne elemente, maksimum i maksimalne elemente skupa $\mathbb{N}$ s obzirom na relaciju ρ ako postoje.

Zadatak 2.3.3. Na skupu $\mathbb{N}_4 = \{1, 2, 3, 4\}$ zadana je relacija

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (2, 3), (3, 2)\}.$$

Ispitaj relaciju R i ako je R relacija ekvivalencije, odredi klase ekvivalencije tj. kvocijentni skup skupa $\mathbb{N}$ s obzirom na relaciju R.
Ako je R relacija uređaja, odredi minimum, minimalne elemente, maksimum i maksimalne elemente skupa $\mathbb{N}_4$ s obzirom na relaciju R ako postoje.

Zadatak 2.3.4. Na skupu svih cijelih brojeva $\mathbb{Z}$ zadana je relacija

$$R = \{(x, y) : x - y \text{ pri dijeljenju s 5 daju isti ostatak}\}.$$

Ispitaj relaciju R i ako je R relacija ekvivalencije, odredi klase ekvivalencije tj. kvocijentni skup skupa $\mathbb{Z}$ s obzirom na relaciju R.
Ako je R relacija uređaja, odredi minimum, minimalne elemente, maksimum i maksimalne elemente skupa $\mathbb{Z}$ s obzirom na relaciju ρ ako postoje.

Zadatak 2.3.5. Ispitaj relaciju $\emptyset$ na skupu $A = \{1, 2, 3\}$.

Zadatak 2.3.6. Neka je S neki skup. Ispitaj relaciju $\rho = \{(A, B) : A \subseteq B\} \subseteq \big(\mathscr{P}(S)\big)^2$.

RJEŠENJA

2.3.1. a) Refleksivnost:
Relacija I je refleksivna jer su u njoj svi jednaki parovi iz A, tj. $(1, 1)$, $(2, 2)$ i $(3, 3)$.

b) Irefleksivnost:
Relacija I nije irefleksivna jer sadrži par $(2, 2)$.

c) Simetričnost:
Relacija I je simetrična jer suprotni par svakog para iz I također je iz I.

d) Antisimetričnost:
Relacija I je antisimetrična jer u njoj nema simetričnih parova različitih elemenata, tj. ne postoje i (a, b) i (b, a) u I za neke različite a i b.

e) Tranzitivnost:
Relacija I je tranzitivna jer ne postoje u njoj parovi (a, b) i (b, c) za koje u I ne postoji i (a, c).

f) Linearnost:
Relacija I nije linearna jer za odabrane prirodne brojeve 1 i 3 iz A niti je par $(1, 3) \in \rho$ niti je par $(3, 1) \in \rho$.

2.3.2. U ρ su očito parovi prirodnih brojeva za koje vrijedi da je prvi broj djeljiv s drugim. U prvom koraku ispišimo neke parove iz ρ kako bismo ju lakše analizirali.

$$\rho = \{(1,1),(2,1),(3,1),(4,1),(5,1),\ldots,(2,2),(4,2),(6,2),(8,2),(10,2),\ldots,\\ (3,3),(6,3),(9,3),(12,3),(15,3),\ldots\}.$$

a) Refleksivnost:
Relacija ρ je refleksivna jer je svaki prirodni broj djeljiv sa samim sobom.

b) Irefleksivnost:
Relacija ρ nije irefleksivna jer je u njoj na primjer par $(3, 3)$.

c) Simetričnost:
Relacija ρ nije simetrična jer je u njoj par $(4, 1)$ (jer je 4 djeljiv s 1), a nema para $(1, 4)$ (jer 1 nije djeljiv s 4).

d) Antisimetričnost:
Relacija ρ je antisimetrična jer u njoj nema simetričnih parova, tj. ne postoje i (a, b) i (b, a) gdje su a i b različiti prirodni brojevi.

e) Tranzitivnost:
Relacija ρ je tranzitivna jer ako je a djeljiv s b i b je djeljiv sa c, onda mora biti i a djeljiv sa c.
a je djeljiv s b znači da postoji prirodni broj k sa svojstvom $a = kb$.
b je djeljiv sa c znači da postoji prirodni broj m sa svojstvom $b = mc$.
No, sada je $a = kb = kmc$, tj. postoji prirodan broj km koji potvrđuje djeljivost a sa c.

f) Linearnost:
Relacija ρ nije linearna jer za odabrane prirodne brojeve 19 i 6 niti je 19 djeljiv sa 6 niti je 6 djeljiv s 19. To jest, niti je $(19, 6) \in \rho$ niti je $(6, 19) \in \rho$.

Relacija ρ je refleksivna i tranzitivna pa je ρ relacija uređaja.

$\mathbb{N}$ nema minimuma jer u ρ ne postoji element koji je sa svima ostalima u paru i uvijek je prvi u paru jer svaki $n \in \mathbb{N}$ u paru je na drugom mjestu s elementom $2n$, tj. $\forall n \in \mathbb{N}\ (2n, n) \in \rho$.
Iz istog razloga nema niti minimalnih elemenata.

Maksimum je 1 jer u paru je sa svim prirodnim brojevima i on je uvijek u paru na drugom mjestu.
Jedini maksimalni element je 1. Svaki drugi prirodni broj bar jednom je prvi u paru, tj. "manji je" od nekog drugog prirodnog broja, tj. djeljiv je s bar jednim prirodnim brojem (na primjer s brojem 1).

2.3.3. a) Refleksivnost:
Relacija R je refleksivna jer su u njoj svi jednaki parovi iz $\mathbb{N}_4$, tj. $(1,1)$, $(2,2)$, $(3,3)$ i $(4,4)$.

b) Irefleksivnost:
Relacija R nije irefleksivna jer sadrži par $(1,1)$.

c) Simetričnost:
Relacija R je simetrična jer suprotni par svakog para iz R također je iz R.

d) Antisimetričnost:
Relacija R nije antisimetrična jer sadrži simetrične parove $(2,3)$ i $(3,2)$.

e) Tranzitivnost:
Relacija R je tranzitivna jer ne postoje u njoj parovi (a,b) i (b,c) za koje u R ne postoji i (a,c).

f) Linearnost:
Relacija R nije linearna jer za odabrane prirodne brojeve 1 i 3 iz $\mathbb{N}_4$ niti je par $(1,3) \in R$ niti je par $(3,1) \in R$.

Relacija R je refleksivna, simetrična i tranzitivna pa je R relacija ekvivalencije.

Klase ekvivalencije su:
$[1] = \{1\}$.
$[2] = \{2,3\}$.
$[3] = \{2,3\} = [2]$.
$[4] = \{4\}$.

$\mathbb{N}_4 |_R = \{[1],[2],[3],[4]\} = \{[1],[2],[4]\} = \{\{1\},\{2,3\},\{4\}\}$.

2.3.4. Odredimo prvo pobliže što se nalazi u R.

$$R = \{(0,0),(1,1),(2,2),(1,6),(6,1),(-1,4),(4,-1),(-1,-1),(-1,-6),\ldots\}$$

a) Refleksivnost:
Relacija R je refleksivna jer su u njoj svi jednaki parovi iz $\mathbb{Z}$, tj. $(1,1)$, $(2,2)$, $(3,3)$, $(-1,-1)$, ...

b) Irefleksivnost:
Relacija R nije irefleksivna jer sadrži i neke "jednake parove", npr. par $(1, 1)$.

c) Simetričnost:
Relacija R je simetrična jer ako a i b pri dijeljenju s 5 daju isti ostatak, onda i b i a pri dijeljenju s 5 daju isti ostatak.

d) Antisimetričnost:
Relacija R nije antisimetrična jer sadrži simetrične parove, npr. $(-1, -6)$ i $(-6, -1)$.

e) Tranzitivnost:
Relacija R je tranzitivna jer ako a i b pri dijeljenju s 5 daju isti ostatak i ako b i c pri dijeljenju s 5 daju isti ostatak, onda, naravno, i a i c pri dijeljenju s 5 daju isti ostatak.

f) Linearnost:
Relacija R nije linearna jer za odabrane prirodne brojeve 1 i 3 iz $\mathbb{Z}$ niti je par $(1, 3) \in R$ niti je par $(3, 1) \in R$.

Relacija R je refleksivna, simetrična i tranzitivna pa je R relacija ekvivalencije.
Klase ekvivalencije su:
$[1] = \{1, 6, 11, 16, 21, 26, \ldots, -4, -9, -14, -19, \ldots\}$,
$[2] = \{2, 7, 12, 17, 22, 27, \ldots, -3, -8, -13, -18, \ldots\}$,
$[3] = \{3, 8, 13, 18, 23, 28, \ldots, -2, -7, -12, -17, \ldots\}$,
$[4] = \{4, 9, 14, 19, 21, 26, \ldots, -1, -6, -11, -16, \ldots\}$,
$[5] = \{5, 10, 15, 20, 25, \ldots, 0, -5, -10, -15, -20, \ldots\}$,
$[6] = \{1, 6, 11, 16, 21, 26, \ldots, -4, -9, -14, -19, \ldots\} = [1]$,
$[7] = \{2, 7, 12, 17, 22, 27, \ldots, -3, -8, -13, -18, \ldots\} = [2]$,
$\ldots$

$\mathbb{Z} |_R = \{[1], [2], [3], [4], [5]\}$

2.3.5. a) Refleksivnost:
Relacija $\emptyset$ nije refleksivna jer u njoj nije $(1, 1)$.

b) Irefleksivnost:
Relacija $\emptyset$ je irefleksivna jer ne sadrži niti jedan par pa onda posebno ne sadrži niti par jednakih elemenata.

c) Simetričnost:
Relacija $\emptyset$ je simetrična jer simetričan par svakog para iz $\emptyset$ također je iz $\emptyset$ (nema niti jednog, pa je istina da ako u njoj postoji neki par, postoji i njemu simetrični).

d) Antisimetričnost:
Relacija $\emptyset$ je antisimetrična jer u njoj nema simetričnih parova različitih elemenata, tj. ne postoje i (a,b) i (b,a) u $\emptyset$ za neke različite a i b.

e) Tranzitivnost:
Relacija $\emptyset$ je tranzitivna jer ne postoje u njoj parovi (a,b) i (b,c) za koje u $\emptyset$ ne postoji i (a,c).

f) Linearnost:
Relacija $\emptyset$ nije linearna jer za odabrane prirodne brojeve 1 i 3 iz A niti je par $(1,3) \in \emptyset$ niti je par $(3,1) \in \emptyset$.

Relacija $\emptyset$ na skupu $A = \{1,2,3\}$ nije relacija ekvivalencije niti relacija uređaja.

2.3.6. Neka je npr. $S = \{k,m,n\}$.
Sada je $\mathscr{P}(S) = \big\{\emptyset, \{k\}, \{m\}, \{n\}, \{k,m\}, \{k,n\}, \{m,n\}, \{k,m,n\}\big\}$.

$$\begin{aligned}\rho = \Big\{ & (\emptyset,\emptyset), \big(\{k\},\{k\}\big), \big(\{m\},\{m\}\big), \big(\{n\},\{n\}\big), \big(\{k,m\},\{k,m\}\big), \big(\{k,n\},\{k,n\}\big),\\ & \big(\{m,n\},\{m,n\}\big), \big(\{k,m,n\}\},\{k,m,n\}\}\big), \big(\emptyset,\{k\}\big), \big(\emptyset,\{m\}\big), \big(\emptyset,\{n\}\big),\\ & \big(\emptyset,\{k,m\}\big), \big(\emptyset,\{k,n\}\big), \big(\emptyset,\{m,n\}\big), \big(\emptyset,\{k,m,n\}\big), \big(\{k\},\{k,m\}\big), \big(\{k\},\{k,n\}\big),\\ & \big(\{k\},\{k,m,n\}\big), \big(\{m\},\{k,m\}\big), \big(\{m\},\{m,n\}\big), \big(\{m\},\{k,m,n\}\big),\\ & \big(\{n\},\{m,n\}\big), \big(\{n\},\{k,n\}\big), \big(\{n\},\{k,m,n\}\big), \big(\{k,m\},\{k,m,n\}\big),\\ & \big(\{k,n\},\{k,m,n\}\big), \big(\{m,n\},\{k,m,n\}\big)\Big\}.\end{aligned}$$

Sada na osnovu ovog primjera pokušajmo zaključiti općenito.

a) Refleksivnost:
Relacija ρ je refleksivna jer svaki je skup podskup samog sebe.

b) Irefleksivnost:
Relacija ρ nije irefleksivna jer sadrži npr. par $(\emptyset,\emptyset)$.

c) Simetričnost:
Relacija ρ je simetrična samo ako je S prazan skup. Ako S ima bar jedan element, na primjer k, onda nije simetrična jer je u njoj par $\big(\emptyset,\{k\}\big)$, a nema para $\big(\{k\},\emptyset\big)$.

d) Antisimetričnost:
Relacija ρ je antisimetrična jer u njoj nema simetričnih parova različitih skupova jer nije moguće A je podskup od B i B je podskup od A ako A i B nisu jednaki.

e) Tranzitivnost:
Relacija ρ je tranzitivna jer ako je $A \subseteq B$ i $B \subseteq C$, onda je i $A \subseteq C$.

f) Linearnost:
Relacija ρ je linearna ako je S prazan skup ili ako S ima točno jedan element. Ako S ima dva različita elementa, npr. k ili m, onda nije linearna jer $\{k\}$ i $\{m\}$ nisu usporedivi, tj. niti je $\{k\}$ podskup od $\{m\}$ niti je $\{m\}$ podskup od $\{k\}$.

Relacija ρ je refleksivna, antisimetrična i tranzitivna pa je ρ relacija uređaja.

Minimum je $\emptyset$ jer u ρ je sa svima ostalima u paru i uvijek je prvi u paru.
Jedini minimalni element je $\emptyset$.
Maksimum je S jer u paru je sa svim ostalim skupovima i on je uvijek u paru na drugom mjestu.
Jedini maksimalni element je S.

2.4. Kardinalni brojevi

U potpoglavlju 2.3. u proizvoljni skup "uveli smo reda", tj. uočili smo kako elemente jednog skupa grupirati po nekom svojstvu (relacijom ekvivalencije) i kako ih po nekom svojstvu međusobno uspoređivati (relacijom uređaja). U ovom ćemo poglavlju sada u "svijet" ili klasu svih skupova uvesti reda i naučit ćemo skupove raspoređivati u klase (opet relacijom ekvivalencije). Imena klasa bit će brojevi. Naučit ćemo što je to broj 1, broj 2, itd. Upoznat ćemo i novi broj, $\mathcal{X}_0$.

Cilj je potpoglavlja 2.4. demonstrirati uobičajeni način uvođenja reda u prostor svih skupova, to jest pokazati kako se skupovi raspoređuju u klase i kako pri tome nastaju brojevi.

Čitatelj bi nakon potpoglavlja 2.4. trebao znati što su ekvipotentni skupovi i kardinalni brojevi, te bi trebao znati konstruirati bijekciju između dvaju zadanih skupova s ciljem dokazivanja ekvipotentnosti skupova.

Literatura za potpoglavlje 2.4. sljedeće su knjige:

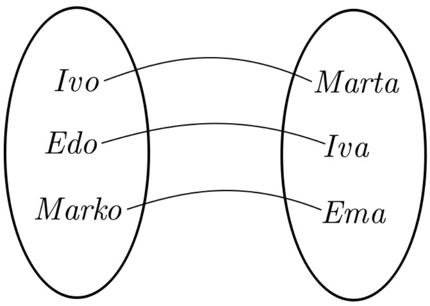
1. P. Papić. *Uvod u teoriju skupova*, HMD, Zagreb, 2000.

   (Za ovo poglavlje je zbog čestog pojavljivanja pojma "beskonačno" od velike pomoći knjiga.)

2. N. J. Vilenkin. *Priče o skupovima*, Školska knjiga, Zagreb, 1975.

3. M. Vuković. *Teorija skupova*, predavanja.
https://web.math.pmf.unizg.hr/nastava/ts/materijali/ts-skripta-2015.pdf (str. 19. – 25.)
(zadnji posjet stranici travanj 2022.)

Ponovimo: Ako imamo dva skupa, bijekcija između tih dvaju skupova jest pridruživanje u kojemu je svakom elementu prvog skupa pridružen točno jedan element drugog skupa tako da se i svakom elementu iz drugog skupa pridružio jedan element iz prvog skupa (obostrano jednoznačno preslikavanje). Bijekciju nije moguće uvijek izvesti (npr. ako je $A = \{a, c\}$, a skup $B = \{3, 4, 5\}$).



Slika 2.4.1: Primjer bijekcije.

Bijekcije imaju i inverznu funkciju koju označavamo ako je zadana bijekcija bila označena s f, s f^{-1}. Ako f preslikava neki x u y, onda je f^{-1} takva funkcija koja y preslika nazad u početni x. (Strogo govoreći, $f(x)$ je element kodomene, a $f^{-1}(y)$ je podskup domene.)

Ako bijekcija f preslikava elemente skupa A u skup B, a bijekcija g preslikava elemente tog skupa B u skup C, onda možemo odmah elemente skupa A prebaciti po tim pravilima u skup C. Takva funkcija, nazovimo ju h, koja napravi odmah preslikavanje iz A u C na isti način kako bi ih napravile f i g, zove se kompozicija funkcija f i g. Dakle, $h(x) = g(f(x))$.

U pokušaju da uvedemo neki red među same skupove, najveći je problem što skupova ima jako puno i što njihovi elementi mogu biti gotovo bilo što.

Kada bi netko pred nas stavio tri košarice s voćem u kojima su: u košarici A dvije jabuke, u košarici B dvije kruške i u košarici C tri jabuke te nas pitao koja su dva od ovih triju skupova najsličniji, što bismo odgovorili?

Uočili bismo povezanost košarica A i C po vrsti voća i povezanost košarica A i B po "brojnosti" elemenata.

Kada bismo dobili puno više košarica u kojima su različite vrste voća, povrća ili predmeta, a u nekima su i miješani sadržaji (npr. imamo i košaricu u kojoj su i bar jedna jabuka i bar jedna kruška), itd., i netko nam postavi zadatak da uvedemo reda među sve te košarice, kako bismo ih tada organizirali?

Pitanje organizacije ("sinteze") nalazi se u početku čovjekovog razumskog i racionalnog razmišljanja. Vjerujemo da je u početku čovjekovog odvajanja (podizanja) od ostalog životinjskog svijeta (po inteligenciji i ostalim sposobnostima) bila, osim inteligencije i fizičkih mogućnosti za korištenje oruđa i oružja, i mogućnost uočavanja da pojedini objekti u okolini imaju zajedničku karakteristiku (skup mačaka, skup pasa, skup drveća, ...). Ovaj se ljudski dar koristi i u počecima jezika. Ne možemo dati nekim objektima oko nas ime "stablo", dok nismo uočili zajedničku karakteristiku nekih objekata da izlaze iz zemlje jednim debelim dijelom koji se grana na tanje dijelove i iz kojih na kraju izlazi lišće ili plod itd. U ljudskoj glavi nastaje skup svih stabala na svijetu, odnosno ono što zovemo "stablo". (Ovo je prva znanost.)

Sadržaje košarica nećemo u općem slučaju moći uspoređivati po "vrsti" sadržaja. Morat ćemo se osloniti na neku drugu karakteristiku.

Dolazimo do posljednjeg koraka pokušaja sređivanja skupova. Kako ne postoji karakteristika (težina, boja, ...) koja je praktična, lako mjerljiva i odgovara čovjekovim potrebama, i po kojoj možemo uvijek usporediti ili klasificirati skupove, kao očita karakteristika za uvođenje reda pojavila se količina predmeta (u košarici).

(Ovdje treba razmisliti i pokušati ipak pronaći neku drugu karakteristiku po kojoj bi se usporedba i klasifikacija skupova mogla izvesti. Možemo, npr. podijeliti skupove u klasu onih u kojima je nešto za jelo i onih u kojima nije ništa za jelo ili slično.)

I tako smo došli do početka matematike: uzimanja količine ili brojnosti skupova kao osnovne karakteristike skupa elemenata.

No, odmah se nalazimo pred sljedećim problemom – kako se dogovoriti na koji način uvesti brojnost kao "najvažniju", bolje reći "najkorisniju" ili "najoperativniju" karakteristiku skupa?

"Brojnosti" je puno. Košarica može biti i prazna. Je li i to brojnost? Izgleda da opet posežemo za drevnim alatima jer je čovjeku, navodno, u prirodi postupak uspostavljanja bijekcije. Kažu da su, prije prebrojavanja, uzgajatelji ovaca ili koza pri puštanju ovaca na pašu, za svaku ovcu koja izlazi iz tora postavili kamen pored tora, a kada su se ovce vraćale, svaki bi kamen vratili, pomaknuli, pa su vidjeli jesu li sve ovce stigle s paše, tj. ima li ih onoliko koliko ih je i bilo. Drugi pokazatelj važnosti bijekcije nalazi se u načinu na koji mala djeca prebrojavaju stvari, a to je brojanje na prste ili uspostava bijekcije između prstiju na ruci i predmeta koje prebrojavamo.

Tako dolazimo do druge važne ideje u problemu sređivanju svega što je oko nas: dva će skupa imati istu količinu stvari ako se između tih skupova može uspostaviti bijekcija. (Važno je i ovdje razmisliti je li to jedini način za uspostavljanje pojma brojnosti i količine.)

Definicija 2.4.1. *Neka su A i B skupovi. Ako je moguće konstruirati (bar jednu) bijek-*

ciju sa skupa A na skup B, onda za skupove A i B kažemo da su ***bijektivni*** *ili* ***ekvipotentni*** *(ili rjeđe, ali jasnije,* ***jednakobrojni****).*
Kažemo da A i B imaju isti kardinalni broj. Činjenicu da se između A i B može uspostaviti bijekcija, pišemo $A \sim B$ ili $k(A) = k(B)$ (kardinalni broj od A jednak je kardinalnom broju od B).

Primjer 2.4.1. Skupovi $A = \{$Ivo, Edo, Marko$\}$ i $B = \{$Iva, Ena, Marta$\}$ su ekvipotentni. Jedna od bijekcija je $f : A \to B$, f(Ivo)=Marta, f(Edo)=Iva, f(Marko)=Ena.

Primjer 2.4.2. Skupovi $S = \{\beta\}$, $T = \{G\}$ su ekvipotentni. $f : S \to T$, $f(\beta) = G$ je očito bijekcija.
Iz ovog je primjera jasno da će svi skupovi koji imaju jedan element biti ekvipotentni sa skupom $S = \{\beta\}$. Bijekcija će uvijek element β preslikati u jedan jedini element nekog drugog jednočlanog skupa.

Stoga skupove organiziramo na sljedeći način:

- Svi skupovi s jednim elementom međusobno su jednakobrojni. Sve ćemo njih smjestiti u jedan prostor, jedan pretinac kojeg ćemo nazvati Jedan i označiti ga s 1 (kosa crta prema gore i onda okomita prema dolje). Tako smo dobili naš prvi broj.

- Sve skupove koji su ekvipotentni sa skupom $A = \{g, h\}$ smjestit ćemo u klasu koju ćemo zvati Dva, a Dva ćemo kraće pisati ovako: 2 (polukrug na koji se nastavljaju kosa i vodoravna crta).

- Sve skupove koji su ekvipotentni sa skupom $S = \{$palac, kažiprst, srednji prst$\}$ smjestit ćemo u klasu koju ćemo zvati Tri, a Tri ćemo pisati ovako: 3.

I tako dalje.

Točnije, u prostoru svih skupova, uvest ćemo relaciju "biti ekvipotentan s"

$$\rho = \{(A, B) : \text{ postoji bijekcija s } A \text{ u B}\}.$$

Sada je ρ relacija ekvivalencije jer je

- refleksivna (svaki je skup bijektivan samom sebi),

- simetrična (jer ako postoji bijektivno pridruživanje s A u B, onda je "suprotno" (inverzna funkcija bijekcije opet je bijekcija) bijektivno pridruživanje pridruživanje s B na A) i

- tranzitivna (kompozicija dviju bijekcija, one iz A u B i one iz B u C, opet je bijekcija, s A u C).

A ako je ρ relacija ekvivalencije, podijelit će sve skupove u klase.

U klasi $[\emptyset]$ bit će samo prazan skup. Tu ćemo klasu nazvati kratko: Nula. Nula ćemo kraće pisati: 0. (Uočimo kako je ova oznaka dosta neprikladna jer na isti način zovemo i jedno slovo abecede, tj. već smo nešto nazvali tim istim imenom.)

U klasi $[\{\beta\}]$ bit će svi oni skupovi koji su bijektivni s $\{\beta\}$. Tu ćemo klasu nazvati kratko: Jedan. Jedan ćemo kraće pisati: 1.

U klasi [{kažiprst, srednji prst}] bit će svi oni skupovi koji su bijektivni s {kažiprst, srednji prst}. Tu ćemo klasu nazvati kratko: Dva. Dva ćemo kraće pisati: 2.

U klasi $[\{A, B, C\}]$ bit će svi oni skupovi koji su bijektivni s $\{A, B, C\}$. Tu ćemo klasu nazvati kratko: Tri. Tri ćemo kraće pisati: 3.

U klasi $[\{0, 1, 2, 3\}]$ bit će svi oni skupovi koji su bijektivni s $\{0, 1, 2, 3\}$. Tu ćemo klasu nazvati kratko: Četiri. Četiri ćemo kraće pisati: 4.

I tako dalje.

U klasi $[\mathbb{N}]$ bit će svi oni skupovi koji imaju isti broj elemenata kao i skup prirodnih brojeva. Tu ćemo klasu nazvati kratko: $\aleph_0$ (čitamo Alef nula, gdje je Alef prvo slovo hebrejskog pisma).

U klasi $[\mathbb{R}]$ bit će svi oni skupovi koji imaju isti broj elemenata kao i skup realnih brojeva. Tu ćemo klasu nazvati kratko: c (malo c od engleske riječi "continuum", u smislu neprekidno jer je skup realnih brojeva neprekidan na pravcu).

I tako dalje.

Gore navedenim sređivanjem sve smo skupove raspodijelili na način na koji poštar razvrstava pisma u različite pretince kako bi sva došla na prava odredišta: za zadani skup, nađemo s kojim je on skupom ekvipotentan i onda ga smjestimo u pretinac u kojem su svi takvi skupovi. U pretincu 0 samo je prazan skup, a u svim ostalim pretincima ima beskonačno skupova.

Definicija 2.4.2. *Skup* $\mathbb{N}_n = \{1, 2, 3, 4, 5, \ldots, n\}$ *ćemo zvati* ***početni komad skupa prirodnih brojeva veličine*** n.

Što se sve nalazi u pretincu $\aleph_0$?

Primjer 2.4.3. Dokaži da brojeva većih od 10 "ima koliko i" prirodnih, tj. da vrijedi $\{11, 12, 13, 14, \ldots\} \sim \mathbb{N}$.

Rješenje. Očito treba uspostaviti bijekciju između $\{11, 12, 13, 14, \ldots\}$ i $\mathbb{N}$.
Zadan je skup

$$\{11, 12, 13, 14, \ldots\}$$

i zadan je skup

$$\{1, 2, 3, 4, 5, \ldots\}.$$

Pogledamo li te skupove, prva je ideja da 11 preslikamo u 1, 12 u 2, 13 u 3 i tako dalje. Tako će različiti brojevi prijeći u različite brojeve i svaki će prirodan broj, 1, 2, 3, 4, 5, ... biti “pogođen” prirodnim brojem koji je za 10 veći od njega. Funkcija je, dakle, injekcija i surjekcija pa je i bijekcija i uspostavili smo $1-1$ preslikavanje s $\{11, 12, 13, 14, \ldots\}$ na $\{1, 2, 3, 4, \ldots\}$.
Tražena bijekcija je $f(x) = x - 10$.
Zaključujemo da je prirodnih brojeva koji su veći od deset točno toliko koliko i svih prirodnih brojeva. Uočimo da smo istu konstrukciju mogli napraviti za bilo koji skup $\mathbb{N} \setminus \mathbb{N}_k$ kojeg dobijemo ako od skupa $\mathbb{N}$ prirodnih brojeva oduzmemo neki njegov početni komad veličine k.

Primjer 2.4.4. Dokaži da parnih brojeva “ima koliko i” prirodnih, tj. da vrijedi

$$\{2, 4, 6, 8, 10, \ldots\} \sim \mathbb{N} \qquad \text{(Galileov[3] paradoks)}$$

Rješenje. Očito treba uspostaviti bijekciju između $\{2, 4, 6, 8, 10, \ldots\}$ i $\mathbb{N}$.
Zadatak možemo riješiti i tako da uspostavimo bijekciju s $\mathbb{N}$ u $\{2, 4, 6, 8, 10, \ldots\}$.
Kako preslikati 1, 2, 3, 4, 5, ... u 2, 4, 6, 8, 10, ...
Rješenje se nameće samo.
Tražena bijekcija je $f(x) = 2x$. $f(3) = 6$, $f(100) = 200$, ... Svaki se prirodni broj preslika u dva puta veći broj. Takvo je preslikavanje injekcija jer ako su a i b različiti prirodni brojevi, onda su i $2a$ i $2b$ različiti. Takvo je preslikavanje i surjekcija jer svaki je parni broj x “pogođen” prirodnim brojem $x : 2$. Dakle parnih je brojeva točno onoliko koliko je i prirodnih.

Primjer 2.4.5. Dokaži da višekratnika broja 3 “ima koliko i” prirodnih brojeva, tj. da vrijedi

$$\{3, 6, 9, 12, 15, \ldots\} \sim \mathbb{N}.$$

Rješenje. Zadatak možemo riješiti tako da uspostavimo bijekciju s $\mathbb{N}$ u $\{3, 6, 9, 12, 15, \ldots\}$.
Kako preslikati 1, 2, 3, 4, 5, ... u 3, 6, 9, 12, 15, ...?
Tražena bijekcija je $f(x) = 3x$. $f(2) = 6$, $f(100) = 300$, ... Svaki se prirodni broj preslika u tri puta veći broj. Takvo je preslikavanje injekcija jer ako su a i b različiti prirodni brojevi, onda su i $3a$ i $3b$ različiti. Takvo je preslikavanje i surjekcija jer se u svaki višekratnik broja tri preslika trostruko manji broj. Dakle, višekratnika broja tri točno je koliko i prirodnih brojeva.

[3] Galileo Galilei (Pisa, 1564. – Arcetri, 1642.) – talijanski znanstvenik

Primjer 2.4.6. Dokaži da višekratnika broja 1000 "ima koliko i" prirodnih brojeva, tj. da vrijedi

$$\{1000, 2000, 3000, \ldots\} \sim \mathbb{N}.$$

Rješenje. Zadatak možemo riješiti tako da uspostavimo bijekciju s $\mathbb{N}$ u

$$\{1000, 2000, 3000, 4000, \ldots\}.$$

Tražena bijekcija je $f(x) = 1000x$. $f(2) = 2000$, $f(1000) = 1000000$, ...

U realnom životu, ako posjedujemo neke predmete i određeni dio predmeta nekom poklonimo, onda imamo manje predmeta nego što smo ih imali. No, kod beskonačnih skupova, kao što je skup svih prirodnih brojeva, ne vrijedi "$N - x < N$", gdje su N i x neki kardinalni brojevi. Ako od skupa prirodnih brojeva, vidjeli smo u primjeru 2.4.3, oduzmemo prvih deset prirodnih brojeva, ostaje nam isto toliko brojeva koliko smo i imali. Skupu $\mathbb{N}$ možemo oduzeti bilo koju konačnu količinu, 10, 100 ili 10^{100} prirodnih brojeva i preostali će skup ostati "toliki" koliki je i bio na početku, prije oduzimanja. Beskonačnost je "prevelika" da bi na nju utjecala bilo koja konačna veličina, koliko god to bilo veliko. Čak štoviše, iz primjera 2.4.4 vidimo kako skupu prirodnih brojeva možemo oduzeti i beskonačno, tj. "točno pola" članova, tj. "svaki drugi član" i ostat će nam ponovo toliko brojeva koliko smo imali na početku. U stvari, iz prethodnih primjera vidljivo je da je skupu $\mathbb{N}$ dovoljno u takvom oduzimanju ostaviti svaki treći ili svaki tisućiti ili svaki milijunti, itd. član i opet će ostati isto toliko brojeva koliko ih je i bilo.

Ista je situacija i s dodavanjem članova. Dodamo li skupu prirodnih brojeva još jedan član, "količina" će brojeva ostati ista, tj. točnije, ponovo dobivamo skup kardinalnosti $\mathcal{X}_0$. Dodamo li mu bilo koji konačan broj novih članova, količina će ostati $\mathcal{X}_0$. Dodamo li mu i još toliko članova koliko ima skup prirodnih brojeva, količina elemenata dobivenog skupa bit će $\mathcal{X}_0$.

Provjerimo to.

Primjer 2.4.7. Dokaži $\{0, 1, 2, 3, 4, 5, \ldots\} \sim \{1, 2, 3, 4, 5, \ldots\}$.

Rješenje. Očita bijekcija je $f(x) = x + 1$.

Primjer 2.4.8. Dokaži da je $\mathbb{N} \sim \mathbb{Z}$.

Rješenje. $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.
Članove skupa $\mathbb{N}$ poredali smo u niz. Kada bismo sada sve članove skupa cijelih brojeva uspjeli zapisati u jednom nizu u kojem su svi ti članovi nabrojani, tj. tako da svaki cijeli broj ima svoje konkretno mjesto u nizu, odmah bismo imali bijekciju.
$\mathbb{Z} = \{-1, -2, -3, -4, \ldots, 0, 1, 2, 3, 4, \ldots\}$ je loš pokušaj jer broj nula nije niti na kojem

konkretnom mjestu u tom nizu jer je prije nule nabrojano beskonačno puno brojeva.
Dobar je pokušaj $\{0, -1, 1, -2, 2, -3, 3, -4, 4, -5, \ldots\}$. Sada, koji god cijeli broj odaberemo, postoji mjesto u nizu na kojem je on. 1 je na trećem mjestu. 5 je na jedanaestom mjestu u nizu. -100 je na 200-tom mjestu u konstruiranom nizu. Prirodno se pojavila i bijekcija koja će svaki prirodni broj preslikati u broj svog mjesta u nizu. $f(1) = 3$, $f(5) = 11$, $f(-100) = 200$, $f(0) = 1$.
Još je možda prirodnija bijekcija inverzna prvoj, tj. ona koja broj mjesta pridruži cijelom broju koji je na tom mjestu.
Na prvom mjestu konstruiranog niza je 0, što zapisujemo s $f(1) = 0$.
Na drugom mjestu konstruiranog niza je -1, što zapisujemo s $f(2) = -1$.
Na 11. mjestu je broj 5, što zapisujemo s $f(11) = 5$.
Na 201. mjestu je 100. Pišemo $f(200) = -100$.
...
Dakle, $k(\mathbb{Z}) = k(\mathbb{N}) = \aleph_0$.

Daljnje jednostavne konstrukcije ovog tipa dane su u priči o hotelu s beskonačno puno soba u knjizi *Priča o skupovima*, navedenoj na početku ovog potpoglavlja.

Sada je jasno da će svaki onaj skup za kojeg sve njegove elemente možemo poredati u niz tako da svaki element tog skupa ima svoje mjestu u nizu, biti ili ekvipotentan s $\mathbb{N}$ ili ako je taj niz konačan, ekvipotentan s nekim početnim komadom od $\mathbb{N}$.

Definicija 2.4.3. *Za skup S kažemo da je* **konačan** *ako je ekvipotentan s nekim početnim komadom od $\mathbb{N}$.*

Primjer 2.4.9. $S = \{a, b, c\}$ je konačan jer vrijedi $\{a, b, c\} \sim \{1, 2, 3\}$.

Primjer 2.4.10. Skup svih slova abecede je konačan jer je ekvipotentan s $\mathbb{N}_{30}$.

Primjer 2.4.11. Skup svih cijelih brojeva koji pri dijeljenju s 5 daju ostatak 2, tj. skup

$$P = \{2, 7, 12, 17, 22, 27, 32, 37, \ldots, -3, -8, -13, -18, \ldots\}$$

nije konačan jer koji god n odabrali, ne možemo uspostaviti bijekciju s navedenog skupa P na $\{1, 2, 3, 4, 5, \ldots, n\}$. U toj bijekciji 2 moramo preslikati u neki od brojeva iz $\mathbb{N}_n$. U $\mathbb{N}_n$ je ostao $n - 1$ član u kojeg se niti jedan broj iz P nije preslikao. 7 moramo preslikati u neki od preostalih $n - 1$ brojeva iz $\mathbb{N}_n$. U $\mathbb{N}_n$ je nakon toga ostalo $n - 2$ članova u koje se niti jedan broj iz P nije preslikao. 12 moramo preslikati u neki od preostalih brojeva iz $\mathbb{N}_n$. U $\mathbb{N}_n$ je ostalo $n - 3$ članova u koje se niti jedan broj iz P nije preslikao. Odabirući dalje redom članove iz P doći ćemo i do n-tog člana koji će se preslikati u zadnji preostali nepokriveni član iz $\mathbb{N}_n$ tako da se sljedeći član iz P neće više moći preslikati u neki slobodni član iz početnog komada skupa $\mathbb{N}$.

Definicija 2.4.4. *Za skup S kažemo da je* **prebrojiv** *ako je ili konačan ili je ekvipotentan sa skupom prirodnih brojeva.*

Primjer 2.4.12. Dokaži da je $\mathbb{Q}$ prebrojiv.

Rješenje. Elemente skupa $\mathbb{Q}$ poredamo u niz na sljedeći način:

$$0, -1, 1, -2, -\frac{1}{2}, \frac{1}{2}, 2, -3, -\frac{3}{2}, -\frac{2}{3}, -\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, 3, -4, \ldots$$

tj. prvo navedemo nulu, pa sve racionalne brojeve koji u svom zapisu u brojniku i nazivniku sadrže samo jedinicu, zatim one koje nismo nabrojali, a sastoje se od jedinice i dvojke, zatim one koje nismo nabrojali, a sastoje se od jedinice, dvojke i trojke, zatim one koje nismo nabrojali, a sastoje se od jedinice, dvojke, trojke i četvorke, itd.
Bijekcija je sada jednostavna, samo treba čitati gornji niz:

$$f(1) = 0, \; f(2) = -1, \; f(3) = 1, \ldots$$

Zaključujemo da prirodnih brojeva ima "isto toliko koliko i" racionalnih.

Realnih brojeva nema koliko i prirodnih brojeva, tj. nemoguće je uspostaviti bijekciju s $\mathbb{N}$ u $\mathbb{R}$.
Postoji, dakle, više vrsta beskonačnosti. $\mathcal{X}_0$ je broj koji je manji od c.
Postoje i kardinalni brojevi koji su strogo veći od c.
Ne postoji najveći kardinalni broj.
Sve ove tvrdnje objašnjene su detaljnije i dokazane u gore navedenoj literaturi.

Kardinalne brojeve možemo i uspoređivati.

Definicija 2.4.5. *Neka su α i β dva kardinalna broja. Neka su A i B skupovi takvi da je $k(A) = \alpha$, $k(B) = \beta$. Reći ćemo da je kardinalni broj α manji ili jednak kardinalnom broju β i pisati to u obliku $\alpha \leq \beta$ ako postoji injekcija s A u B.*

Primjer 2.4.13. $3 \leq 4$ jer $3 = k(\{q, w, e\})$, $4 = k(\{a, s, d, f\})$, a injekcija je $f(q) = a$, $f(w) = s$, $f(e) = d$.

Primjer 2.4.14. Nije istina da je $4 \leq 2$ jer ne postoje skupovi A i B od kojih A ima 4 elementa, a B 2 elementa i postoji injekcija s A u B.

Definicija 2.4.6. *Neka su α i β dva kardinalna broja. Neka su A i B skupovi takvi da je $k(A) = \alpha$, $k(B) = \beta$. Reći ćemo da je kardinalni broj α manji od kardinalnog broju β i pisati to u obliku $\alpha < \beta$ ako postoji injekcija s A u B, ali ne postoji bijekcija s A u B.*

Kardinalne brojeve možemo i zbrajati i množiti.

Definicija 2.4.7. *Neka su α i β dva kardinalna broja. Neka su A i B disjunktni skupovi (nemaju zajedničkih elemenata) takvi da je $k(A) = \alpha$, $k(B) = \beta$. Sada je*

$$k(A) + k(B) = k(A \cup B),$$
$$k(A) \cdot k(B) = k(A \times B).$$

Primjer 2.4.15. Dokaži: $2 + 2 = 4$.

Rješenje. Neka je $2 = k(\{a, s\})$, $2 = k(\{d, f\})$, $4 = k(\{y, x, c, v\})$.

$$2 + 2 = k(\{a, s\} \cup \{d, f\}) = k(\{a, s, d, f\}) = k(\{y, x, c, v\}) = 4.$$

(Treću jednakost povlači npr. bijekcija $g(a) = y$, $g(s) = x$, $g(d) = c$, $g(f) = v$.)

ZADACI ZA VJEŽBU

Zadatak 2.4.1. Konstruiraj bijekciju sa skupa $A = \{a, s, d\}$ u skup $\{g, h, j\}$. Koliko bijekcija s A u B postoji?

Zadatak 2.4.2. Neka je $A = \{1, 2\}$. Koliko ima bijekcija sa skupa A u skup A?

Zadatak 2.4.3. Neka je $A = \{\alpha, \beta, \gamma\}$. Koliko ima bijekcija sa skupa A u skup A?

Zadatak 2.4.4. Odredi sve injekcije sa skupa $A = \{1, 2\}$ u skup $\{4, 5, 6\}$.

Zadatak 2.4.5. Odredi sve surjekcije sa skupa $A = \{1, 2, 3\}$ u skup $\{5, 6\}$.

Zadatak 2.4.6. Odredi neku bijekciju sa skupa $\mathbb{N}$ prirodnih brojeva u skup NP neparnih brojeva.

Zadatak 2.4.7. Odredi neku bijekciju sa skupa $\mathbb{N}$ prirodnih brojeva u skup $4\mathbb{N} - 2 = \{2, 6, 10, 14, 18, \ldots\}$.

Zadatak 2.4.8. Odredi neku bijekciju sa skupa NP neparnih prirodnih brojeva u skup $3\mathbb{N} = \{3, 6, 9, 12, 15, \ldots\}$.

Zadatak 2.4.9. Odredi neku bijekciju sa skupa $\mathbb{N}$ prirodnih brojeva u skup $-\mathbb{N}$ negativnih brojeva.

Zadatak 2.4.10. Odredi neku bijekciju sa skupa $\mathbb{Z} \backslash \mathbb{N}_8$ u skup $\mathbb{Z} \backslash \{-1, 0, 1\}$.

Rješenja

2.4.1. $f(a) = g$, $f(s) = h$, $f(d) = j$. Ovo kraće zapisujemo: $f = \begin{pmatrix} a & s & d \\ g & h & j \end{pmatrix}$.
Ostale bijekcije su:

$f_2 = \begin{pmatrix} a & s & d \\ g & j & h \end{pmatrix}$, $f_3 = \begin{pmatrix} a & s & d \\ h & g & j \end{pmatrix}$, $f_4 = \begin{pmatrix} a & s & d \\ h & j & g \end{pmatrix}$, $f_5 = \begin{pmatrix} a & s & d \\ j & g & h \end{pmatrix}$ i $f_6 = \begin{pmatrix} a & s & d \\ j & h & g \end{pmatrix}$.

2.4.2. $f_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$.

2.4.3. $f_1 = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha & \beta & \gamma \end{pmatrix}$, $f_2 = \begin{pmatrix} \alpha & \beta & \gamma \\ \alpha & \gamma & \beta \end{pmatrix}$, $f_3 = \begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \alpha & \gamma \end{pmatrix}$, $f_4 = \begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \gamma & \alpha \end{pmatrix}$, $f_5 = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \end{pmatrix}$ i

$f_5 = \begin{pmatrix} \alpha & \beta & \gamma \\ \gamma & \beta & \alpha \end{pmatrix}$.

2.4.4. $f_1 = \begin{pmatrix} 1 & 2 \\ 4 & 5 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 \\ 4 & 6 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 \\ 5 & 4 \end{pmatrix}$, $f_4 = \begin{pmatrix} 1 & 2 \\ 5 & 6 \end{pmatrix}$, $f_5 = \begin{pmatrix} 1 & 2 \\ 6 & 4 \end{pmatrix}$ i $f_6 = \begin{pmatrix} 1 & 2 \\ 6 & 5 \end{pmatrix}$.

2.4.5. $f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 5 & 6 \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 6 & 5 \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 5 & 6 & 6 \end{pmatrix}$, $f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 6 & 5 & 5 \end{pmatrix}$, $f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 6 & 5 & 6 \end{pmatrix}$ i

$f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 6 & 6 & 5 \end{pmatrix}$.

2.4.6. $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.
$\mathrm{NP} = \{1, 3, 5, 7, 9, \ldots\}$.
Jedna bijekcija je $f(x) = 2x - 1$.

2.4.7. $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.
$4\mathbb{N} - 2 = \{2, 6, 10, 14, 18, \ldots\}$.
Jedna bijekcija je $f(x) = 4x - 2$.

2.4.8. $\mathrm{NP} = \{1, 3, 5, 7, 9, \ldots\}$.
$3\mathbb{N} = \{3, 6, 9, 12, 15, \ldots\}$.
Jedna bijekcija je $f(x) = \frac{3}{2}(x + 1)$.

2.4.9. $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$.
$-\mathbb{N} = \{-1, -2, -3, -4, \ldots\}$.
Jedna bijekcija je $f(x) = -x$.

2.4.10. $\mathbb{Z} \backslash \mathbb{N}_8 = \{\ldots, -3, -2, -1, 0, 9, 10, 11, 12, \ldots\}$.
$\mathbb{Z} \backslash \{-1, 0, 1\} = \{\ldots, -3, -2, 2, 3, 4, 5, 6, \ldots\}$.

Jedna bijekcija f je

$$f(x) = x - 2 \text{ za } x < 1,$$
$$f(x) = x - 7 \text{ za } x > 8.$$

Ovo kraće pišemo na sljedeći način

$$f(x) = \begin{cases} x - 2; & x < 1 \\ x - 7; & x > 8 \end{cases}$$

gdje će, u ovisnosti o broju slučajeva, postojati i analogni broj redova te otvorenu vitičastu zagradu po dogovoru ne zatvaramo.

3

Teorija brojeva

Teorija brojeva (Carl Fridrich Gauss[1]: *"Matematika je kraljica znanosti, a teorija brojeva kraljica je matematike"*) je dio matematike u kojoj proučavamo samo cijele brojeve i funkcije s cijelim brojevima. No, većina gradiva ove cjeline bavit će se (a tako je najčešće i u preostaloj literaturi) prirodnim brojevima.

Teorija brojeva negdje se naziva i viša aritmetika.

Osnovni su joj dijelovi djeljivost, prosti brojevi, osnovni teorem aritmetike, kongruencije i diofantske jednadžbe.

3.1. Djeljivost. Prosti brojevi.

Cilj je potpoglavlja 3.1. izložiti osnovne rezultate o djeljivosti u $\mathbb{Z}$, prostim brojevima te o najvećoj zajedničkoj mjeri i najmanjem zajedničkom višekratniku. Dalje, čitatelj će biti upoznat s rezultatima Osnovnog teorema aritmetike.

Nakon ovog potpoglavlja čitatelj bi trebao, na osnovu rezultata Osnovnog teorema aritmetike, konstruirati rastav broja na proste faktore, izvesti postupak za traženje najveće zajedničke mjere i najmanjeg zajedničkog višekratnika te bi trebao znati upotrijebiti taj teorem u računanju s prirodnim brojevima.

Osnovna literatura za potpoglavlje 3.1. jest:

1. A. Baker, *A Concise Introduction to the Theory of Numbers*, Cambridge University Press, Cambridge, 1994.

[1]Carl Friedrich Gauss (1777. – 1855.) – njemački matematičar i astronom koji je dokazao osnovni teorem algebre

2. A. Dujella, *Uvod u teoriju brojeva* (skripta), PMF – Matematički odjel (poglavlja 1., 2. i 7.)
   Cijela skripta dostupna je na https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf (zadnji pristup travanj 2022.)

3. A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

4. I. Gucunski, P. Žuljević, V. Kolobarić, V. Crnjak, *Prosti brojevi*,
   https://www.fer.hr/_download/repository/Seminar_Prosti_brojevi.pdf
   (zadnji pristup travanj 2022.)

5. J. H. Silverman, *A Friendly Introduction to Number Theory*, Pearson, 1997. 4th Edition 2012.
   https://www.math.brown.edu/~jhs/frint.html (zadnji pristup travanj 2022.)

   (Ova je knjiga pisana jednostavnim engleskim jezikom i jednostavnih je rezultata pa će njena građa biti razumljiva i srednjoškolcu matematičaru.)

6. W. Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, January 23, 2017.
   Cijela knjiga dostupna je na https://wstein.org/ent/ent.pdf (zadnji pristup travanj 2022.)
   (Samo nam je prva cjelina zanimljiva, ostale su "prenapredne" za ovaj udžbenik.)

7. Z. Zorić, *Poučak o uzastopnom prebrojavanju*, Matka: časopis za mlade matematičare br. 5. 1993.
   https://natjecanja.math.hr/wp-content/uploads/2014/12/matka5-prebrojavanje.pdf (zadnji pristup travanj 2022.)

8. Na https://www.vedantu.com/maths/divisibility-rules-for-13 dana su četiri načina ispitivanja djeljivosti s 13. (zadnji pristup travanj 2022.)

9. https://en.wikipedia.org/wiki/Sieve_of_Eratosthenes (zadnji pristup travanj 2022.)
   (Na ovoj je stranici detaljnije objašnjeno Eratostenovo sito, ali na njemu su i poveznice za ostala sita za traženje prostih brojeva pomoću računala.)

Pojam djeljivosti najvažniji je pojam u cijeloj teoriji brojeva.

Definicija 3.1.1. *Kažemo da je cijeli broj a **djeljiv** prirodnim brojem b i pišemo $a \vdots b$ (ovo čitamo: a je djeljiv s b) ili pišemo $b \mid a$ (ovo čitamo b dijeli a) ako postoji neki treći cijeli broj k takav da je $a = k \cdot b$. Ako a nije djeljiv s b, tj. ako b ne dijeli a, pišemo $b \nmid a$.*
*Ako je prirodni broj a djeljiv prirodnim brojem b, za b kažemo da je **djelitelj** od a te kažemo da je a **višekratnik** od b.*

Često se u literaturi može naći definicija u kojoj su ili a i b oba cijeli ili prirodni brojevi. Za potrebe ove knjige dovoljna je definicija djeljivosti u kojoj je cijeli broj djeljiv prirodnim brojem.

Primjer 3.1.1.

a) -8 je djeljiv s 2 jer postoji cijeli broj -4 takav da je $-8 = -4 \cdot 2$.
Pišemo $-8 \vdots 2$, $2 \mid -8$.

b) 8 je djeljiv s 2 jer postoji cijeli broj 4 takav da je $8 = 4 \cdot 2$.
Pišemo $8 \vdots 2$, $2 \mid 8$.

c) 8 nije djeljiv s 3 jer ne postoji cijeli broj k za kojeg bi bilo $8 = k \cdot 3$.
Pišemo $3 \nmid 8$.

d) Nula je djeljiva sa svim cijelim brojevima, ali niti jedan cijeli broj nije djeljiv s nulom.
(Nema smisla pitati: Ako imamo 10 bombona i podijelimo ih na nula djece, koliko svako dijete dobije bombona, tj. nema smisla pitati za "svako dijete" ako smo rekli da je djece nula.)

Najčešće se definicija djeljivosti koristi samo za prirodne brojeve, tj. prirodni broj a djeljiv je prirodnim brojem b ako postoji prirodni broj k za koji je $a = k \cdot b$.

Istražimo na skupu prirodnih brojeva relaciju "biti djeljiv s". Istraga je lakša napišemo li točnije što u stvari želimo dokazati.

Ispitajmo relaciju $D = \{(a, b) : \ a \text{ je djeljiv s } b\} \subseteq \mathbb{N}^2$.

1. Refleksivnost: Budući da je svaki broj djeljiv sa samim sobom, očito je relacija D refleksivna.

2. Irefleksivnost: Budući da je D refleksivna na $\mathbb{N}$, naravno, nije irefleksivna (sadrži npr. par (1, 1)).

3. Simetričnost: 10 je djeljiv s 5, ali 5 nije djeljiv s 10 pa D nije simetrična.

4. Antisimetričnost: Ne postoje različiti prirodni brojevi a i b takvi da je $a \vdots b$ i u isto vrijeme $b \vdots a$. Stoga je D antisimetrična.
Strože, iz $a \vdots b$ slijedilo bi da postoji k takav da je $a = k \cdot b$. Iz $b \vdots a$ slijedi da postoji neki m takav da je $b = m \cdot a$. Ukupno je, dakle, $b = m \cdot a = m \cdot k \cdot b$, gdje su k i m neki prirodni brojevi. $b = m \cdot k \cdot b$ povlači $m \cdot k = 1$ pa mora biti $m = k = 1$, tj. a i b su jednaki.

5. Tranzitivnost: Ako je broj a djeljiv s b i b je djeljiv s c, onda je, naravno, i a djeljiv s c.

Opet, strože matematički dokazano: $a \vdots b$ i $b \vdots c$ povlači da postoje prirodni brojevi k i m takvi da je $a = k \cdot b$ i $b = m \cdot c$. No, onda je i $a = k \cdot b = k \cdot m \cdot c$, tj. $a = k \cdot m \cdot c$, tj. a je djeljiv s c jer postoji prirodni broj $k \cdot m$ sa svojstvom $a = k \cdot m \cdot c$.

6. Linearnost: Niti je 5 djeljiv s 3 niti je 3 s 5 pa relacija D nije linearna.

Definicija 3.1.2. *Za prirodni broj kažemo da je* **prost** *ako je djeljiv samo s jedan i sa samim sobom, a broj jedan nije prost. Ili, prirodni broj je prost ako ima točno dva različita djelitelja (djeljiv je sa samim sobom i s* 1*). Ako prirodni broj veći od jedan nije prost, kažemo da je* **složen***.*

Dakle, broj jedan nije niti prost niti složen.

Primjer 3.1.2.

a) 2 je prost broj jer je djeljiv samo s jedan i sa samim sobom.
b) 91 nije prost broj jer je djeljiv s 1, 7, 13 i 91.
c) 1 nije prost jer, po dogovoru (definiciji), nije prost.
d) -273.15 nije prost broj jer prosti mogu biti samo prirodni brojevi.

Prosti brojevi manji od 1000 su redom:
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997.

Postoji ukupno 4 prosta broja manja od 10, 25 prostih brojeva manjih od 100 i 168 prostih brojeva manjih od 1000.

Dalje navodimo nekoliko poznatih još nedokazanih tvrdnji o prostim brojevima. Čitatelja pozivamo da ih svakako pokuša provjeriti na računalu s početnih 100, 1000 ili više prirodnih brojeva.

1. Prosti brojevi koji se razlikuju za 2 zovu se **prosti brojevi blizanci**. Npr. 3 i 5 su prosti brojevi blizanci, kao i 857 i 859. Otvoren je problem u matematici postoji li beskonačno prostih brojeva blizanaca.

2. Goldbachova hipoteza kaže kako se svaki parni broj od 4 pa nadalje može napisati kao zbroj dvaju prostih brojeva.
   Npr. $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 5 + 5$, $12 = 5 + 7$, ...

3. Goldbachova hipoteza o neparnim brojevima: Svaki neparni broj veći od 5 je zbroj triju prostih brojeva.
   Npr. $7 = 2 + 2 + 3$, $9 = 3 + 3 + 3$, $11 = 2 + 2 + 7 = 3 + 3 + 5$, ...

4. Za svaki prirodni broj n, između n^2 i $(n + 1)^2$ postoji bar jedan prost broj.
   Ovdje bi bilo dobro napisati program koji će dati izračun broja prostih brojeva između n^2 i $(n + 1)^2$.
   Npr.

Tablica 3.1.1: Prosti brojevi u intervalu $[n^2, (n + 1)^2]$.

n	$[n^2, (n + 1)^2]$	prosti brojevi unutar $[n^2, (n + 1)^2]$
1	[1, 4]	2, 3
2	[4, 9]	5, 7
3	[9, 16]	11, 13
4	[16, 25]	17, 19, 23
5	[25, 36]	29, 31

Teorem 3.1.1. (Osnovni teorem aritmetike)
Svaki prirodni broj veći od 1 *može se na jedinstven način zapisati u obliku produkta prostih brojeva (produkt od jednog ili više članova). Pri tome dva zapisa smatramo jednakima ako se sastoje od istih prostih brojeva, a međusobno su jednaka ili se razlikuju po poretku čimbenika (faktora).*
Pišemo

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot p_4^{e_4} \cdot \ldots \cdot p_k^{e_k},$$

gdje broj e_x zovemo **kratnost** *prostog broja p_x, $x = 1, 2, \ldots, k$ u rastavu broja n na proste faktore.*

Primjer 3.1.3. $2 = 2$, $3 = 3$, $4 = 2 \cdot 2$, $5 = 5$, $6 = 2 \cdot 3$, $7 = 7$, $8 = 2 \cdot 2 \cdot 2$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5$, $11 = 11$, $12 = 2 \cdot 2 \cdot 3$, ...

Rastavimo brojeve 144, 100 i 35 na proste faktore i pogledajmo njihove eksponente pri tom razvoju.

$$\begin{aligned}
144 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2^4 \cdot 3^2 = 2^4 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 \ldots \\
100 &= 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13^0 \ldots \\
35 &= 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1 \cdot 11^0 \cdot 13^0 \ldots
\end{aligned}$$

Očito, po teoremu 3.1.1. svaki prirodni broj jedinstveno je određen beskonačnim nizom brojeva $(e_1, e_2, \ldots)$ koji su u stvari eksponenti prostih brojeva 2, 3, 5, 7, 11, 13, 17, ... u rastavu zadanog prirodnog broja na proste faktore. U zapisu ćemo prvo koristiti potencije najvećih prostih faktora, pa sve manjih, sve do 2.

Tako možemo pisati

$$\begin{aligned}144 &= 3^2 \cdot 2^4 = (2,4)_p,\\ 100 &= (2,0,2)_p,\\ 35 &= (1,1,0,0)_p.\end{aligned}$$

Za ovako zapisane brojeve kažemo da su zapisani u bazi prostih brojeva ili u bazi p ili u kanonskom zapisu.

U ovom zapisu brojevi se lako množe i, ako su djeljivi jedan s drugim, lako dijele.

$$\begin{aligned}144 \cdot 100 &= (2,4)_p \cdot (2,0,2)_p =\\ &= (0+2, 2+0, 4+2)_p =\\ &= \big(\text{samo zbrojimo elemente ``po znamenkama''}\big) =\\ &= (2,2,6)_p =\\ &= 14\,400.\end{aligned}$$

U ovom zapisu brojevi se lako i potenciraju.

$$\begin{aligned}144^7 &= 3^{2\cdot 7} \cdot 2^{4\cdot 7} = (14, 28)_p,\\ (2,0,2)_p^3 &= (6,0,6)_p.\end{aligned}$$

Uočimo sada dvije stvari koje će nam biti od velike koristi u razumijevanju nadolazeće teorije.

1. Ako su a i b prirodni brojevi rastavljeni na faktore kao u gornjem teoremu, tj. ako je

$$\begin{aligned}a &= p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot p_4^{e_4} \cdot \ldots \cdot p_k^{e_k} \quad \text{i}\\ b &= r_1^{f_1} \cdot r_2^{f_2} \cdot r_3^{f_3} \cdot r_4^{f_4} \cdot \ldots \cdot r_m^{f_m},\end{aligned}$$

   onda je a djeljiv s b ako a sadrži u svom rastavu sve proste brojeve koje ima i b (i možda još i neke druge) te su eksponenti tih prostih brojeva (kratnosti) koji se pojavljuju u a veći ili jednaki eksponentima (kratnostima) tih istih brojeva u b.

Na primjer, za $a = 2^3 \cdot 7^2 \cdot 11^5$, ako želimo da a bude djeljiv s b, onda prirodni broj b u rastavu na proste faktore smije sadržavati samo brojeve 2, 7 i 11 i to 2 s kratnošću manjom ili jednakom 3, 7 s kratnošću manjom ili jednakom 2 i 11 s kratnošću manjom ili jednakom 5. Pojavi li se u rastavu broja b na proste faktore bilo koji broj osim 2, 5 ili 11, a sigurno neće biti djeljiv s b.

2. Ako je prirodni broj a djeljiv prirodnim brojem b, tj. $a = k \cdot b$, onda je a djeljiv i s bilo kojim djeliteljem od b, tj. ako je $b = k_2 \cdot n$, onda je $a = k \cdot b = k \cdot k_2 \cdot n$.
   Jasno je: ako je 98 djeljiv s 14, a 14 je djeljiv sa 7, onda 98 djeljiv sa 7. (To smo već pokazali kada smo rekli da je relacija "biti djeljiv s" tranzitivna na $\mathbb{N}$.)

Teorem 3.1.2. *Postoji beskonačno puno prostih brojeva, tj. nema najvećeg prostog broja.*

Dokaz. (Euklidov) Pretpostavimo da postoji konačan broj prostih brojeva. Neka su to 2, 3, 5, ..., p, gdje je p najveći prosti broj.
Promotrimo broj $2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p + 1$. Taj je broj veći od p jer je umnožak svih prostih brojeva do p (zajedno s p).
Taj broj pri dijeljenju sa svakim prostim brojem od 2 do p daje ostatak 1, tj. nije djeljiv ni s jednim prostim brojem od 2 do p.
Taj broj nije djeljiv niti s nekim složenim brojem jer svaki je složeni broj po gore navedenom Osnovnom teoremu aritmetike moguće zapisati kao umnožak prostih brojeva, pa bi taj broj bio djeljiv ili s 2 ili s 3 ili s 5, ... ili s p. Nije djeljiv ni s jednim od njih jer ostatak pri dijeljenju uvijek je 1.
On je, dakle, ili prost ili je djeljiv s nekim drugim prostim brojem kojeg nismo naveli u nizu, što je nemoguće jer smo pretpostavili da su 2, 3, 5, ..., p svi prosti brojevi. $\square$

Kako istražiti je li zadani broj prost? Treba provjeriti je li djeljiv s nekim manjim brojem od njega ili ne. Ako nije djeljiv niti s jednim od njih, tj. ako je djeljiv samo s 1 i sa samim sobom, onda je prost.

Uočimo da je za provjeru je li broj prost dovoljno provjeravati brojeve koji su manji od drugog korijena od tog broja.

Uočimo dalje da je za provjeru je li broj prost dovoljno provjeravati samo proste brojeve manje od korijena od tog broja.

Razvijene su mnoge (računalne) taktike za provjeru je li broj prost ili ne. Najpoznatija su takozvana "sita" (Eratostenovo, Atkinovo, Sundaramovo, Legendreovo, Brunovo, Selbergovo).
Eratostenovo je sito najjednostavnije i najsporije gledajući računalno.

Eratostenovo sito pregledava niz prirodnih brojeva od početka do određenog broja i pronalazi sve proste brojeve na sljedeći način:

1. Prvi je broj 1. On nije prost pa ga prekrižimo.
2. Nakon toga prvi je neprekriženi broj 2. Njega zaokružimo i precrtamo sve njegove višekratnike.
3. Nakon toga prvi je neprekriženi broj 3. Njega zaokružimo i precrtamo sve njegove višekratnike.
4. Nakon toga prvi je neprekriženi broj 5. Njega zaokružimo i precrtamo sve njegove višekratnike.
5. Nakon toga prvi je neprekriženi broj 7. Njega zaokružimo i precrtamo sve njegove višekratnike.

   I tako dalje.

U prvom krugu križamo višekratnike od 2. Oni sigurno nisu prosti brojevi jer su svi djeljivi s 2. Isto vrijedi i za 3, 5, 7, ... U nizu će preostati samo oni brojevi koji nisu ničiji višekratnici, a to su prosti brojevi.

Sundaramovo sito počinje sa svim brojevima od 1 do n, a onda izbacuje sve brojeve oblika $i + j + 2 \cdot i \cdot j$, a preostale brojeve udvostruči i poveća za 1.

Atkinovo sito promatra ostatke pri dijeljenju sa 60 te nešto kompliciranijom teorijom rezultira bržim algoritmom.

Primjer 3.1.4. Napiši program za neka odabrana sita i usporedi vremena izvođenja (npr. za traženje svih prostih brojeva od 1 do zadanog n).

Primjer 3.1.5.

a) Koliko djelitelja ima broj 12?

   Rješenje. 6. To su 1, 2, 3, 4, 6 i 12.

b) Koliko djelitelja ima broj 15?

   Rješenje. 4. To su 1, 3, 5 i 15.

c) Koliko djelitelja ima broj 17?

   Rješenje. 2. To su 1 i 17.

Postavlja nam se pitanje kako odrediti broj djelitelja nekog broja.

Zapišimo djelitelje broja 12 u kanonskom obliku, po teoremu 3.1.1.

$$\begin{aligned} 1 &= 2^0 \cdot 3^0 \\ 2 &= 2^1 \cdot 3^0 \\ 3 &= 2^0 \cdot 3^1 \\ 4 &= 2^2 \cdot 3^0 \\ 6 &= 2^1 \cdot 3^1 \\ 12 &= 2^2 \cdot 3^1 \end{aligned}$$

Po razmišljanjima koja smo proveli nakon teorema 3.1.1., znamo da svi djelitelji broja 12 imaju sve baze kao i broj 12 (to su 2 i 3), ali s eksponentima koji se kreću od nule do eksponenta te iste baze u broju 12. Budući da je broj 12 jednak $2^2 \cdot 3^1$, njegovi djelitelji imat će u zapisu $2^x \cdot 3^y$, gdje x ide od 0 do 2, a y od 0 do 1. Ukupno, x može biti 0, 1 ili 2 (tri mogućnosti), a y može biti 0 ili 1 (2 mogućnosti). Po teoremu o uzastopnom prebrojavanju ([7.]) postoji $3 \cdot 2 = 6$ različitih djelitelja broja 12. To pišemo kao $d(12) = 6$.

Analogno, ako je n prirodan broj i $n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot p_4^{e_4} \cdot \ldots \cdot p_k^{e_k}$, onda broj djelitelja broja n računamo po formuli

$$d(n) = (e_1 + 1) \cdot (e_2 + 1) \cdot \ldots \cdot (e_k + 1).$$

Dakle, za broj djelitelja nekog broja nije važno koliko je taj broj velik, nego kolike su kratnosti na prostim brojevima na koje se taj broj rastavlja.

Primjer 3.1.6. Broj djelitelja broja $15 = 3^1 \cdot 5^1$ jednak je broju djelitelja broja $14 = 2^1 \cdot 7^1$ i jednak je broju djelitelja broja $143 = 11^1 \cdot 13^1$.

Riješimo sada, primjenom navedene teorije, problem pronalaženja največeg zajedničkog djelitelja i najmanjeg zajedničkog višekratnika.

Definicija 3.1.3. *Za zadane prirodne brojeve a_1, a_2, ..., a_k,* **najveći zajednički djelitelj** *brojeva a_1, a_2, ..., a_k je najveći prirodni broj s kojim su svi navedeni brojevi djeljivi. Najveći zajednički djelitelj brojeva (najveću zajedničku mjeru u nekim knjigama) označavat ćemo s $\mathrm{nzd}(a_1, a_2, \ldots, a_k)$.*

Primjer 3.1.7.

- Djelitelji broja 48 su 1, 2, 3, 4, 6, 8, 12, 16, 24 i 48.
- Djelitelji broja 120 su 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 25, 30, 40, 60 i 120.
- Djelitelji broja 60 su 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 i 60.

Zajednički djelitelji navedenih brojeva su 1, 2, 3, 4, 6 i 12.
Najveći zajednički djelitelj brojeva 48, 120 i 60 je broj 12.
Pišemo $\mathrm{nzd}(48, 120, 60) = 12$.

Kako za veće brojeve ili za više brojeva možemo najbrže naći najveći zajednički djelitelj?

Postupak 1:

Rastavimo ponovo zadane brojeve na proste faktore:

$$\begin{aligned} 48 &= 2^4 \cdot 3^1, \\ 120 &= 2^3 \cdot 3^1 \cdot 5^1, \\ 60 &= 2^2 \cdot 3^1 \cdot 5^1. \end{aligned}$$

Svaki broj s kojim su i 48 i 120 i 60 djeljivi smije u svom rastavu na proste faktore sadržavati samo one proste faktore koje sadrže i 48 i 120 i 60, a to su samo 2 i 3. Kratnosti brojeva 2 i 3 moraju biti ili manje ili jednake onima koje se nalaze u 48, 120 i 60, tj. kratnost od 2 smije biti najviše 2, kratnost od 3 najviše 1. Stoga je $\mathrm{nzd}(48, 120, 60) = 2^2 \cdot 3^1 = 12$.

Postupak 2:

$\mathrm{nzd}(a_1, a_2, \ldots, a_k)$, na osnovu prethodnog razmatranja, nalazimo sljedećim algoritmom: brojeve a_1, a_2, $\ldots$, a_k dijelit ćemo redom prostim brojevima s kojima su svi djeljivi, kao dolje u postupku, sve dok ne ostanu brojevi za koje ne postoji prosti broj s kojim su svi djeljivi. Umnožak prostih brojeva s kojima smo dijelili bit će traženi najveći zajednički djelitelj.

$$\begin{array}{rrr|l} 48, & 120, & 60 & 2 \\ 24, & 60, & 30 & 2 \\ 12, & 30, & 15 & 3 \\ 4, & 10, & 5 & - \text{ (sada više ne postoji prost broj s kojim su i 4 i 10 i 5 djeljivi)} \end{array}$$

$\mathrm{nzd}(48, 120, 60) = 2 \cdot 2 \cdot 3 = 12$.

Postupak 3: (Euklidov algoritam)

Ako su nam zadana samo dva prirodna broja a i b, $\mathrm{nzd}(a, b)$ možemo naći na sljedeći način:
Prvo cjelobrojno podijelimo a sa b. Dobivamo količnik q_1 i ostatak r_1.
Zatim dijelimo b s ostatkom r_1. Dobivamo količnik q_2 i ostatak r_2.
Zatim dijelimo r_1 s ostatkom r_2. Dobivamo količnik q_3 i ostatak r_3.

Zatim dijelimo r_2 s ostatkom r_3. Dobivamo količnik q_4 i ostatak r_4.
Dakle, neprestano dijelimo djelitelj iz prethodnog dijeljenja ostatkom iz prethodnog dijeljenja, sve dok ostatak ne bude nula. U dijeljenju u kojem je ostatak nula, djelitelj je najveći zajednički djelitelj kojeg smo tražili. Dokaz ispravnosti ovog postupka nalazi se u gore navedenoj knjizi *Uvod u teoriju brojeva*, na https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf, stranica 4.

Primjer 3.1.8.
$\mathrm{nzd}(120, 48) =?$
$120 : 48 = 2$ i ostatak 24.
$48 : 24 = 2$ i ostatak 0.
$\mathrm{nzd}(120, 48) = 24$ jer je djelitelj u zadnjem redu Euklidovog algoritma 24.

Na ovaj način možemo tražiti i najveći zajednički djelitelj dvaju polinoma.

Primjer 3.1.9. Napiši program za traženje najvećeg zajedničkog djelitelja dvaju prirodnih brojeva.

U gore navedenom postupku koristili smo se sljedećim teoremom:

Teorem 3.1.3. (Teorem o dijeljenju s ostatkom)
Za zadani cijeli broj a i prirodni broj b, postoji cijeli broj q i postoji prirodni broj $r \in \{0, 1, 2, \ldots, b-1\}$ sa svojstvom $a = q \cdot b + r$.

Broj r iz teorema 3.1.3. zovemo **ostatak** pri dijeljenju broja a brojem b. Dokaz teorema 3.1.3 čitatelj može naći u gore navedenoj knjizi *Uvod u teoriju brojeva*, na https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf, stranica 2.

Primjer 3.1.10.
Podijelimo cjelobrojno 16 s 5. $16 : 5 = 3$ i ostatak 1.
Podijelimo cjelobrojno -16 s 5. $-16 : 5 = -4$ i ostatak 4.
To pišemo kao $-16 : 5 = -4$
$\quad$ ost.: 4

Definicija 3.1.4. *Za zadane prirodne brojeve a_1, a_2, …, a_k,* **najmanji zajednički višekratnik** *brojeva a_1, a_2, …, a_k najmanji je prirodni broj koji je djeljiv sa svim navedenim brojevima. Najmanji zajednički višekratnik brojeva (najmanji zajednički nazivnik u nekim knjigama) označavat ćemo s $\mathrm{nzv}(a_1, a_2, \ldots, a_k)$.*

Primjer 3.1.11.

- Višekratnici broja 18 su 18, 36, 54, 72, 90, 108, … (ima ih beskonačno).

- Višekratnici broja 12 su 12, 24, 36, 48, 60, 72, 84, ...
- Višekratnici broja 9 su 9, 18, 27, 36, 45, ...

Zajednički višekratnici navedenih brojeva su 36, 72, 108, ...
Najmanji zajednički višekratnik brojeva 18, 12 i 9 je broj 36.
$\text{nzv}(18, 12, 9) = 36$.

Kako za veće brojeve ili za više brojeva najbrže naći najmanji zajednički višekratnik?

Postupak 1:

Rastavimo ponovno zadane brojeve na proste faktore:

$$\begin{aligned} 18 &= 2^1 \cdot 3^2, \\ 12 &= 2^2 \cdot 3^1, \\ 9 &= 3^2 \end{aligned}$$

Svaki broj koji je djeljiv s 18, 12 i 9 mora u svom rastavu na proste faktore (osim eventualno još nekih faktora) sadržavati sve one proste faktore koje sadrže i 18 i 12 i 9, a to su 2 i 3. Kratnosti brojeva 2 i 3 moraju u višekratniku biti ili veće ili jednake kratnostima brojeva 2 i 3 u 18, 12 i 9, tj. kratnost od 2 mora biti bar 2, kratnost od 3 također bar 2. Stoga je $\text{nzv}(18, 12, 9) = 2^2 \cdot 3^2 = 36$.

Postupak 2:

$\text{nzv}(a_1, a_2, \ldots, a_k)$, na osnovu prethodnog razmatranja, nalazimo sljedećim algoritmom: brojeve a_1, a_2, ..., a_k dijelit ćemo redom prostim brojevima kao dolje u postupku (ovaj puta dijelimo kad je bar jedan broj djeljiv tim prostim brojem, a brojeve koji nisu djeljivi samo prepišemo) sve dok u zadnjem redu ne budu same jedinice. Umnožak prostih brojeva s kojima smo dijelili bit će traženi najmanji zajednički višekratnik.

$$\begin{array}{ccc|l} 18, & 12, & 9 & 2 \\ 9, & 6, & 9 & 2 \\ 9, & 3, & 9 & 3 \\ 3, & 1, & 3 & 3 \\ 1, & 1, & 1 & - \text{ (sve jedinice u redu znak su da je postupak gotov)} \end{array}$$

$\text{nzv}(18, 12, 9) = 2 \cdot 2 \cdot 3 \cdot 3 = 36$.

Postupak 3:

nzv(a, b) možemo lako naći ako imamo izračunat nzd(a, b), po sljedećem teoremu.

Teorem 3.1.4. *Neka su a i b prirodni brojevi. Vrijedi* $a \cdot b = \text{nzd}(a, b) \cdot \text{nzv}(a, b)$.

Pokazat ćemo zašto je ova tvrdnja točna na primjeru brojeva $a = 18$ i $b = 24$. Ako napišemo a i b u obliku umnoška prostih faktora

$$
\begin{aligned}
18 &= 2^1 \cdot 3^2, \\
24 &= 2^3 \cdot 3^1.
\end{aligned}
$$

Umnožak $18 \cdot 24 = 2^{1+3} \cdot 3^{2+1} = 2^4 \cdot 3^3$.

$$
\begin{aligned}
\text{nzd}(18, 24) \cdot \text{nzv}(18, 24) &= 2^{\min\{1,3\}} \cdot 3^{\min\{2,1\}} \cdot 2^{\max\{1,3\}} \cdot 3^{\max\{2,1\}} = \\
&= 2^{\min\{1,3\}} \cdot 2^{\max\{1,3\}} \cdot 3^{\min\{2,1\}} \cdot 3^{\min\{2,1\}} = \\
&= 2^{1+3} \cdot 3^{1+2} = 2^4 \cdot 3^3,
\end{aligned}
$$

gdje je $\min\{a_1, a_2, \ldots, a_n\}$ najmanji od brojeva a_1, a_2, ..., a_n, a $\max\{a_1, a_2, \ldots, a_n\}$ najveći od brojeva a_1, a_2, ..., a_n, a a_1, a_2, ..., a_n neki su prirodni brojevi.

Ili općenito, isti je rezultat zbrojimo li dva eksponenta kao prvi plus drugi ili kao manji plus veći. Više vrsta dokaza ovog teorema nalaze se na https://math.stackexchange.com/questions/349858/easiest-and-most-complex-proof-of-gcd-a-b-times-operatornamelcm-a-b-a (posljednji pristup travanj 2021.)

Do kraja potpoglavlja pozabavit ćemo se zadacima koji su slični onima koje često možemo naći na matematičkim natjecanjima, a za čije se rješavanje koriste rezultati upravo izložene teorije.

Primjer 3.1.12. Odredi tri najveća troznamenkasta broja koja pri dijeljenju s 3, 5 i 7 daju ostatak 2.

Rješenje. Pronađimo prvo bar jedan broj koji pri dijeljenju s 3, 5 i 7 daje ostatak 2. Neka je n taj broj. Tada je

$$n = 3k + 2 = 5m + 2 = 7p + 2$$

za neke brojeve k, m i p (koji su prirodni brojevi ili nula).

$$
\begin{aligned}
n = 3k + 2 &= 5m + 2 = 7p + 2 \quad / - 2 \\
n - 2 = \quad 3k \quad &= \quad 5m \quad = 7p.
\end{aligned}
$$

$n - 2$ je, dakle, djeljiv s 3, 5 i 7.
$n - 2$ je zajednički višekratnik od 3, 5 i 7.
Jedan takav $n - 2$ je 105. Dalje su to 210, 315, ..., 735, 840, 945.
Odgovor: Tri najveća takva troznamenkasta broja su 737, 842 i 947.

Za dalje će nam u zadacima biti potrebna i pravila djeljivosti. Pogledajmo neka od tih pravila.

1. Prirodni broj n je djeljiv s 2 ako mu je zadnja znamenka 2, 4, 6, 8 ili 0.
2. Prirodni broj n je djeljiv s 3 ako mu je zbroj znamenaka djeljiv s 3.
3. Prirodni broj n je djeljiv s 3 ako je broj n bez zadnje znamenke zbrojen sa zadnjom znamenkom djeljiv s 3.
4. Prirodni broj n je djeljiv s 4 ako mu je dvoznamenkasti završetak djeljiv sa 4.
5. Prirodni broj n je djeljiv s 5 ako mu je zadnja znamenka 0 ili 5.
6. Prirodni broj n je djeljiv sa 6 ako je djeljiv s 2 i 3.
7. Prirodni broj n je djeljiv sa 7 ako je n bez zadnje znamenke minus 2 puta zadnja znamenka djeljiv sa 7.
8. Prirodni broj n je djeljiv sa 7 ako je n bez zadnje znamenke plus 5 puta zadnja znamenka djeljiv sa 7.
9. Prirodni broj n je djeljiv s 8 ako mu je troznamenkasti završetak djeljiv sa 8.
10. Prirodni broj n je djeljiv s 9 ako mu je zbroj znamenaka djeljiv s 9.
11. Prirodni broj n je djeljiv s 9 ako je broj n bez zadnje znamenke plus ta zadnja znamenka djeljiv s 9.
12. Prirodni broj n je djeljiv s 10 ako mu je zadnja znamenka 0.
13. Prirodni broj n je djeljiv s 11 ako mu je zbroj znamenaka na parnim mjestima minus zbroj znamenaka na neparnim mjestima djeljiv s 11.
14. Prirodni broj n je djeljiv s 12 ako je djeljiv s 3 i 4.

Neka je n složen broj i neka je

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot p_4^{e_4} \cdot \ldots \cdot p_k^{e_k}$$

rastav broja n na proste faktore. Bilo koji prirodni broj je djeljiv s n ako je djeljiv i s $p_1^{e_1}$ i s $p_2^{e_2}$ i s $p_3^{e_3}$ ... i s $p_k^{e_k}$.

Primjer 3.1.13. Broj je djeljiv s 36 ako je djeljiv s 4 i s 9. Broj je djeljiv s 50 ako je djeljiv s 2 i s 25.

Označimo s $[a_1 a_2 \ldots a_n]$ n-znamenkasti broj čije su znamenke redom a_1, a_2, ..., a_n, gdje je a_n znamenka jedinica.

Primjer 3.1.14. $[abc] = 100a + 10b + c$.

Primjer 3.1.15. Odredi sve četveroznamenkaste prirodne brojeve oblika $[abba]$ koji su djeljivi s 18.

Rješenje. Prva i zadnja znamenka moraju biti jednake, druga i treća moraju biti jednake. Također a ne smije biti nula (jer prva znamenka četveroznamenkastog broja nije nula). Broj je djeljiv s 18 ako i samo ako je djeljiv s 2 i s 9. To znači: dovoljno je naći one brojeve koji su djeljivi i s 2 i s 9 i pronaći ćemo sve one brojeve koji su djeljivi s 18.
$[abba]$ je djeljiv s 2 ako mu je zadnja znamenka 0, 2, 4, 6 ili 8.

1. Ako je $a = 2$, radi se o broju $[2bb2]$ čiji zbroj znamenaka dalje mora biti djeljiv s 9.
   $2 + b + b + 2$ ne može biti 9, ali može biti 18.
   $2 + b + b + 2$ je djeljiv s 9 samo ako je $b = 7$.
   $2 + b + b + 2$ ne može biti 27 kao niti bilo koji veći višekratnik broja 9 veći od 27.
   Rješenje je 2772.
2. Ako je $a = 4$, radi se o broju $[4bb4]$ čiji zbroj znamenaka dalje mora biti djeljiv s 9.
   $4 + b + b + 4$ ne može biti 9, ali može biti 18.
   $4 + b + b + 4$ ne može biti 27 kao niti bilo koji veći višekratnik broja 9 veći od 27.
   $4 + b + b + 4$ je djeljiv s 9 samo ako je $b = 5$.
   Rješenje je 4554.
3. Ako je $a = 6$, radi se o broju $[6bb6]$ čiji zbroj znamenaka dalje mora biti djeljiv s 9.
   Rješenje je 6336.
4. Ako je $a = 8$, radi se o broju $[8bb8]$ čiji zbroj znamenaka dalje mora biti djeljiv s 9.
   Rješenje je 8118.

Primjer 3.1.16. Odredi sve peteroznamenkaste prirodne brojeve oblika $[1a24a]$ koji su djeljivi s 11.

Rješenje. $1 - a + 2 - 4 + a = -1$.
Kako -1 nije djeljiv s 11, traženi broj ne postoji.

Primjer 3.1.17. Odredi sve brojeve oblika $[bbb]$ koji su djeljivi s 36.

Rješenje. Broj je djeljiv s 36 ako je djeljiv s 4 i 9.
Broj je djeljiv s 4 ako mu je dvoznamenkasti završetak djeljiv s 4.
Dakle, $[bb] = 0$ ili $[bb] = 44$ ili $[bb] = 88$.

1. Za $[bb] = 0$ zadani broj nije troznamenkasti.
2. Za $[bb] = 44$ zadani broj je 444 koji nije djeljiv s 9 jer mu je zbroj znamenaka 12.
3. Za $[bb] = 88$ zadani broj je 888 koji nije djeljiv s 9 jer mu je zbroj znamenaka 24.

Zaključak: Broj s traženim svojstvima ne postoji.

Zadaci za vježbu

Zadatak 3.1.1. Odaberi neki četveroznamenkasti broj. Koristeći samo džepno računalo, pronađi prva tri prosta broja veća od zadanog broja.

Uputa: Za odabrani četveroznamenkasti broj, ne treba gledati parne brojeve koji su veći od njega jer parni brojevi nisu prosti jer su djeljivi s 2. Treba preskočiti i one čiji je zbroj znamenaka djeljiv s 3 jer su oni djeljivi s 3. Treba preskočiti i one čija je zadnja znamenka nula ili 5 jer su oni djeljivi s 5 pa sigurno nisu prosti, itd. Džepnim računalom isprobamo je li promatrani broj djeljiv s nekim prostim brojem od 2 do korijena od promatranog broja. Ako nije djeljiv ni s jednim od tih brojeva, prost je. Važnost je ovog zadatka u tome što bi čitatelj trebao dobiti osjećaj za izgled prostih brojeva (za koje se, jer su četveroznamenkasti, ne vidi odmah s kojim su sve brojevima djeljivi) i djeljivost većih brojeva manjima.

Zadatak 3.1.2. Dokaži da postoje cijeli brojevi a i b za koje vrijedi $a \mid b$ i $b \mid a$ i $a \neq b$ (djeljivost nije antisimetrična, pa onda niti relacija uređaja na $\mathbb{Z}$).

Zadatak 3.1.3. Rastavi na proste faktore: 99, 8, 111, 288.

Zadatak 3.1.4. Svaki od brojeva iz prethodnog zadatka zapiši u bazi p prostih brojeva.

Zadatak 3.1.5. Svakom od brojeva iz prethodnog zadatka odredi broj njegovih djelitelja. Odaberi neki od njih pa i ispiši sve njegove djelitelje.

Zadatak 3.1.6. Odredi $\mathrm{nzd}(420, 132, 288)$ na sva tri u tekstu navedena načina.

Zadatak 3.1.7. Odredi $\mathrm{nzv}(420, 132, 288)$ na sva tri u tekstu navedena načina.

Zadatak 3.1.8. Euklidovim algoritmom odredi $\mathrm{nzd}(x^3 - 1, x^2 - 1)$.

Zadatak 3.1.9. Euklidovim algoritmom odredi $\mathrm{nzd}(x^5 + 1, x^3 + 1)$.

Zadatak 3.1.10. Odredi sve brojeve oblika $[xyx]$, $[aaaab]$ i $[aabb]$ djeljive s

a) 11,

b) 15,

c) 13 *(malo teži!)*.

Rješenja

3.1.2. Za cijele brojeve $a = 5$, $b = -5$ vrijede navedena svojstva.

3.1.3.
$$\begin{aligned} 99 &= 3 \cdot 3 \cdot 11 \\ 8 &= 2 \cdot 2 \cdot 2 \\ 111 &= 3 \cdot 37 \\ 288 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \end{aligned}$$

3.1.4.
$$\begin{aligned} 99 &= 3^2 \cdot 11^1 = (1, 0, 0, 2, 0)_p \\ 8 &= (3)_p \\ 111 &= (1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0)_p \\ 288 &= (2, 5)_p \end{aligned}$$

3.1.5.
$$\begin{aligned} d(99) &= 2 \cdot 3 = 6 \\ d(8) &= 4 \\ d(111) &= 2 \cdot 2 = 4 \\ d(288) &= 3 \cdot 6 = 18 \end{aligned}$$

$99 = 3^2 \cdot 11^1$.

Djelitelji broja 99 su

$$3^0 \cdot 11^0 = 1,\ 3^1 \cdot 11^0 = 3,\ 3^2 \cdot 11^0 = 9,\ 3^0 \cdot 11^1 = 11,\ 3^1 \cdot 11^1 = 33,\ 3^2 \cdot 11^1 = 99.$$

Dakle, ukupno 6 djelitelja, kao što smo i dobili gore računajući direktno po formuli.

3.1.6.

Postupak 1.

Rastavimo zadane brojeve na proste faktore:

$$\begin{aligned} 420 &= 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1, \\ 132 &= 2^2 \cdot 3^1 \cdot 11^1, \\ 288 &= 2^5 \cdot 3^2. \end{aligned}$$

$\text{nzd}(420, 132, 288) = 2^2 \cdot 3^1 = 12.$

Postupak 2.

$$\begin{array}{ccc|c} 420, & 132, & 288 & 2 \\ 210, & 66, & 144 & 2 \\ 105, & 33, & 72 & 3 \\ 35, & 11, & 24 & - \end{array}$$

$\text{nzd}(420, 132, 288) = 2 \cdot 2 \cdot 3 = 12.$

Postupak 3. (Euklidov algoritam) ne možemo provesti za tri prirodna broja. Provodi se samo za dva broja pa pokažimo nalaženje $\text{nzd}(420, 132)$ Euklidovim algoritmom.

$420 : 132 = 3$
ost.: 24

$132 : 24 = 5$
ost.: 12

$24 : 12 = 2$
ost.: 0

Kako je u zadnjem dijeljenju ostatak nula, traženi najveći zajednički djelitelj je djelitelj tog zadnjeg dijeljenja, a to je 12.

3.1.7.

Postupak 1.

Rastavimo zadane brojeve na proste faktore:

$$420 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1,$$
$$132 = 2^2 \cdot 3^1 \cdot 11^1,$$
$$288 = 2^5 \cdot 3^2.$$

$\text{nzv}(420, 132, 288) = 2^5 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 110880.$

Postupak 2.

$$\begin{array}{rrr|l} 420, & 132, & 288 & 2 \\ 210, & 66, & 144 & 2 \\ 105, & 33, & 72 & 2 \\ 105, & 33, & 36 & 2 \\ 105, & 33, & 18 & 2 \\ 105, & 33, & 9 & 3 \\ 35, & 11, & 3 & 3 \\ 35, & 11, & 1 & 5 \\ 7, & 11, & 1 & 7 \\ 1, & 11, & 1 & 11 \\ 1, & 1, & 1 & - \end{array}$$

$\mathrm{nzv}(420, 132, 288) = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$

Postupak 3. (Euklidov algoritam)

$a \cdot b = \mathrm{nzd}(a, b) \cdot \mathrm{nzv}(a, b)$ možemo upotrijebiti samo za dva prirodna broja pa pokažimo nalaženje $\mathrm{nzd}(420, 132)$.

$$\begin{aligned} 420 \cdot 132 &= \mathrm{nzd}(420, 132) \cdot \mathrm{nzv}(420, 132) \\ 420 \cdot 132 &= 12 \cdot \mathrm{nzv}\ (420, 132) \\ \mathrm{nzv}(420, 132) &= 420 \cdot 132 : 12 = 420 \cdot 11 = 4620. \end{aligned}$$

3.1.8.

$$\begin{array}{l} \big(\ \ x^3 \qquad -1\big) : \big(x^2 - 1\big) = x + \dfrac{x-1}{x^2-1} \\ \underline{-x^3 + x} \\ \qquad\quad x - 1 \end{array}$$

$$\begin{array}{l} \big(\ \ x^2 \qquad -1\big) : \big(x - 1\big) = x + 1 \\ \underline{-x^2 + x} \\ \qquad\quad x - 1 \\ \qquad\ \underline{-x + 1} \\ \qquad\qquad 0 \end{array}$$

$\mathrm{nzd}(x^3 - 1, x^2 - 1) = x - 1.$

3.1.9.

$$
\begin{array}{l}
\big(\;\; x^5 \qquad\quad +1\big) : \big(x^3+1\big) = x^2 + \dfrac{-x^2+1}{x^3+1} \\
\underline{\;-x^5 - x^2\;} \\
\qquad\quad -x^2+1
\end{array}
$$

$$
\begin{array}{l}
\big(\;\; x^3 \qquad +1\big) : \big(-x^2+1\big) = -x + \dfrac{x+1}{-x^2+1} \\
\underline{\;-x^3 + x\;} \\
\qquad\quad x+1
\end{array}
$$

$$
\begin{array}{l}
\big(-x^2 \qquad +1\big) : \big(x+1\big) = -x+1 \\
\underline{\;\;\; x^2 + x\;} \\
\qquad\quad x+1 \\
\qquad \underline{-x-1} \\
\qquad\qquad 0
\end{array}
$$

$\text{nzd}(x^5+1, x^3+1) = x+1.$

3.1.10. a) $[xyx]$ su troznamenkasti brojevi kojima su znamenka stotica i znamenka jedinica jednake.
Broj je djeljiv s 11 ako mu je zbroj znamenaka na parnim mjestima minus zbroj znamenaka na neparnim mjestima djeljiv s 11.
Mora, dakle, biti $x - y + x$ djeljiv s 11, tj. $2x - y$ djeljiv s 11.

- Za $2x - y = 0$ traženi brojevi su 121, 242, 363 i 484.
- Za $2x - y = 11$ traženi brojevi su 616, 737, 858 i 979.

Kako su x i y znamenke, tj. brojevi od 0 do 9, $2x - y$ ne može biti -11, -22, ... kao niti 22, 33, 44, ..., pa su sva rješenja dana gore.

$[aaaab]$ je djeljiv s 11 ako je $a - a + a - a + b$ djeljivo s 11, a to će biti ako je b djeljiv s 11.
Znamenka b mora, dakle, biti 0.
Svi brojevi $[aaaa0]$ su dakle djeljivi s 11 pa su sva rješenja: 11110, 22220, 33330, 44440, 55550, 66660, 77770, 88880 i 99990.

Četveroznamenkasti broj oblika $[aabb]$ je zbog $a + b - a - b = 0$ uvijek djeljiv s 11.

b) Broj je djeljiv s 15 ako je djeljiv s 3 i s 5.
Za $[xyx]$ mora biti $x + y + x$ djeljiv s 3 i mora biti zadnja znamenka x ili 0 ili 5.

No, x ne može biti 0 jer je to ujedno i prva znamenka pa broj neće biti troznamenkast. Mora znači biti $x = 5$.
$5 + y + 5$ mora biti djeljiv s 3 pa je y ili 2 ili 5 ili 8, a sva rješenja su 525, 555 i 585.

Broj $[aaaab]$ bit će djeljiv s 15 ako je $b = 0$ ili $b = 5$.

- Za $b = 0$ mora biti $4a$ djeljiv s 3, a to će biti za $a = 3$, $a = 6$ i $a = 9$. Rješenja su 33330, 66660 i 99990.
- Za $b = 5$, $4a + 5$ mora biti djeljiv s 3, a to će biti za $a = 1$, $a = 4$ i $a = 7$. Rješenja su 11115, 44445 i 77775.

Broj $[aabb]$ bit će djeljiv s 15 ako je $b = 0$ ili $b = 5$.

- Za $b = 0$ mora biti $2a$ djeljiv s 3, a to će biti za $a = 3$, $a = 6$ i $a = 9$. Rješenja su 3300, 6600 i 9900.
- Za $b = 5$, $2a + 10$ mora biti djeljiv s 3, a to će biti za $a = 1$, $a = 4$ i $a = 7$. Rješenja su 1155, 4455 i 7755.

c) Broj n je djeljiv s 13 ako je broj n bez zadnje znamenke, zbrojen s umnoškom zadnje znamenke i broja 4, djeljiv s 13.
Dakle, $[xyx]$ će biti djeljiv s 13 ako je $[xy] + 4x$ djeljiv s 13.

$[xy] + 4x = 10x + y + 4x = 14x + y = 13x + x + y$.
$13x$ je djeljiv s 13.
Dakle, da bi $[xyx]$ bio djeljiv s 13, mora biti i dovoljno je da je i $x + y$ djeljiv s 13.

Rješenje: 494, 585, 676, 767, 858, 949.

Istražimo djeljivost broja $[aaaab]$ s 13. Broj n je djeljiv s 13 ako mu je troznamenkasti završetak minus sljedeći troznamenkasti dio plus sljedeći troznamenkasti dio itd. (naizmjenično pozitivno i negativno) djeljiv s 13.
Na primjer, 1234567890 nije djeljiv s 13 jer $890 - 567 + 234 - 1 = 556$ nije djeljiv s 13.
U našem slučaju

$$[aab] - [aa] = 100a + 10a + b - 10a - a = 100a + b - a = 99a + b = 91a + 8a + b.$$

$91a$ je djeljiv s 13.

Dakle, da bi $[aaaab]$ bio djeljiv s 13, mora biti $8a + b$ djeljiv s 13.

- Za $a = 0$ broj $[aaaab]$ nije peteroznamenkasti.
- Za $a = 1$, $8 + b$ je djeljiv s 13 za $b = 5$. Rješenje je 11115.
- Za $a = 2$, $16 + b$ nije djeljiv s 13 ni za jedan $b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- Za $a = 3$, $24 + b$ je djeljiv s 13 za $b = 2$. Rješenje je 33332.
- Za $a = 4$, $32 + b$ je djeljiv s 13 za $b = 7$. Rješenje je 44447.
- Za $a = 5$, $40 + b$ nije djeljiv s 13 ni za jedan $b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- Za $a = 6$, $48 + b$ je djeljiv s 13 za $b = 4$. Rješenje je 66664.
- Za $a = 7$, $56 + b$ je djeljiv s 13 za $b = 9$. Rješenje je 77779.
- Za $a = 8$, $64 + b$ nije djeljiv s 13 ni za jedan $b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- Za $a = 9$, $72 + b$ je djeljiv s 13 za $b = 6$. Rješenje je 99996.

Istražimo djeljivost broja $[aabb]$ s 13. Broj n je djeljiv s 13 ako je n bez zadnjih dviju znamenki pomnožen s 4 minus dvoznamenkasti završetak djeljiv s 13.
Na primjer, 12345 nije djeljiv s 13 jer $4 \cdot 123 - 45$ nije djeljiv s 13.
U našem slučaju $4 \cdot [aa] - [bb] = 4 \cdot 11a - 11b = 11(4a - b)$.
$11x$ će biti djeljiv s 13 samo ako je x djeljiv s 13.

Dakle, da bi $[aabb]$ bio djeljiv s 13, mora biti $4a - b$ djeljiv s 13.

- Za $a = 0$ broj $[aabb]$ nije četveroznamenkasti.
- Za $a = 1$, $4 - b$ je djeljiv s 13 za $b = 4$. Rješenje je 1144.
- Za $a = 2$, $8 - b$ je djeljiv s 13 za $b = 8$. Rješenje je 2288.
- Za $a = 3$, $12 - b$ nije djeljiv s 13 ni za jedan $b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- Za $a = 4$, $16 - b$ je djeljiv s 13 za $b = 3$. Rješenje je 4433.
- Za $a = 5$, $20 - b$ je djeljiv s 13 za $b = 7$. Rješenje je 5577.
- Za $a = 6$, $24 - b$ nije djeljiv s 13 ni za jedan $b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
- Za $a = 7$, $28 - b$ je djeljiv s 13 za $b = 2$. Rješenje je 7722.
- Za $a = 8$, $32 - b$ je djeljiv s 13 za $b = 6$. Rješenje je 9966.
- Za $a = 9$, $36 - b$ nije djeljiv s 13 ni za jedan $b \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

3.2. Djeljivost u zadacima s matematičkih natjecanja

U zadacima s natjecanja često su na razne načine implementirani rezultati teorija brojeva, tj. najčešće djeljivosti. Slijedi desetak zadataka s različitim idejama u konstrukciji rješenja i primjenom (gdje god je to moguće) gore navedenih rezultata.

Literatura za potpoglavlje 3.2. jest:

1. K. Logarušić, *Teorija brojeva u zadatcima s natjecanja*, Diplomski rad. Zagreb, 2017.
   https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view (zadnji pristup travanj 2022.)

2. Zadaci s matematičkih natjecanja u Hrvatskoj dostupni su, zajedno s rješenjima na http://www.matematika.hr/natjecanja/domaca/2020/ (zadnji pristup travanj 2022.)

Zadaci s matematičkih natjecanja osnovnih i srednjih škola te matematičkih olimpijada često (možda i najčešće) pripadaju upravo području teorije brojeva.

Primjer 3.2.1. Odredi sve troznamenkaste brojeve koji pri dijeljenju s 3 daju ostatak 2, pri dijeljenju sa 7 ostatak 5 i pri dijeljenju s 8 ostatak 5.

Rješenje. Ako neki prirodni broj n pri dijeljenju s 3 daje ostatak 2, možemo ga napisati u obliku $n = 3k + 2$, $k \in \mathbb{N}_0$.
Ako neki prirodni broj n pri dijeljenju sa 7 daje ostatak 5, možemo ga napisati u obliku $n = 7m + 5$, $m \in \mathbb{N}_0$.
Ako neki broj n pri dijeljenju s 8 daje ostatak 5, možemo ga napisati u obliku $n = 8r + 5$, $r \in \mathbb{N}_0$.

Ako želimo da broj n zadovoljava sva tri uvjeta, mora biti

$$n = 3k + 2 = 7m + 5 = 8r + 5$$

za neke brojeve k, m i r koji su ili prirodni brojevi ili nula.

Sada nam je cilj cijeloj navedenoj višestrukoj jednakosti dodati ili oduzeti broj z za koji bi $n + z$ ili $n - z$ s lijeve strane bio višekratnika brojeva k, m i r.

1. Da bi $n+z$ bio višekratnik broja 3, moramo broju $3k+2$ dodati neki broj iz skupa $\{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, \ldots\}$.
2. Da bi $n+z$ bio višekratnik broja 7, moramo broju $7m+5$ dodati neki broj iz skupa $\{2, 9, 16, 23, 30, 37, 44, 51, 58, 65, 72, \ldots\}$.
3. Da bi $n+z$ bio višekratnik broja 8, moramo broju $8r+5$ dodati neki broj iz skupa $\{3, 11, 19, 27, 35, 43, 51, 59, 67, 75, 83, \ldots\}$.
4. Da bi $n + z$ bio djeljiv i s 3 i sa 7 i s 8, z mora biti broj koji se nalazi u svim trima skupovima. Detaljnijim (dužim) nabrajanjem brojeva u svim trima gotnjim

skupovima dobivamo da je najmanji takav broj 163.

$$\begin{aligned} n = &\ 3k+2 &= &\ 7m+5 &= 8r+5 \quad / + 163 \\ n+163 = &\ 3k+165 &= &\ 7m+168 &= 8r+168 \\ n+163 = &\ 3(k+55) &= &\ 7(m+24) &= 8(r+21). \end{aligned}$$

$n+163$ je djeljiv i s 3 i sa 7 i s 8.

Najmanji broj koji je djeljiv i s 3 i sa 7 i s 8 je 168, a dalje su to višekratnici broja 168: 336, 504, 672, 840, 1008, 1176, ...

- Za $n+163 = 168$ traženi broj n je 5, što nije rješenje jer tražimo troznamenkasti broj.
- Za $n+163 = 336$ traženi broj n je 173, što je prvo rješenje.
- Za $n+163 = 504$ traženi broj n je 341, što je rješenje.
- Za $n+163 = 672$ traženi broj n je 509, što je rješenje.
- Za $n+163 = 840$ traženi broj n je 677, što je rješenje.
- Za $n+163 = 1008$ traženi broj n je 845, što je rješenje.
- Za $n+163 = 1176$ traženi broj n je 1013, što nije rješenje jer smo prešli u četveroznamenkaste brojeve.

Jedina su rješenja, dakle: 173, 341, 509, 677, 845.

Drugi, i brži način rješavanja:

$$\begin{aligned} n = &\ 3k+2 &= 7m+5 &= 8r+5 \quad / - 5 \\ n-5 = &\ 3k-3 &= 7m &= 8r \\ n-5 = &\ 3(k-1) &= 7m &= 8r. \end{aligned}$$

$n-5$ je djeljiv i s 3 i sa 7 i s 8.
Najmanji prirodni broj koji je djeljiv i s 3 i sa 7 i s 8 je 168, a dalje su to višekratnici broja 168: 336, 504, 672, 840, 1008, 1176, ...

- Za $n-5 = 168$ traženi broj n je 173, što je prvo rješenje.
- Za $n-5 = 336$ traženi broj n je 341, što je rješenje.
- Za $n-5 = 504$ traženi broj n je 509, što je rješenje.
- Za $n-5 = 672$ traženi broj n je 677, što je rješenje.
- Za $n-5 = 840$ traženi broj n je 845, što je rješenje.

- Za $n-5=1008$ traženi broj n je 1113, što nije rješenje jer smo prešli u četveroznamenkaste brojeve.

Jedina su rješenja, dakle: 173, 341, 509, 677, 845.

Primjer 3.2.2. Dvoznamenkasti broj $[ab]$ je djeljiv s 3. Ako između a i b upišemo nulu i dobivenom broju dodamo dvostruku vrijednost znamenke desetica, dobit ćemo devet puta veći broj od početnog dvoznamenkastog broja. Odredi a i b.

Rješenje.

$$\begin{aligned}
[a0b]+2a &= 9\cdot[ab]\\
100a+b+2a &= 9\cdot(10a+b)\\
12a &= 8b \quad /:4\\
3a &= 2b.
\end{aligned}$$

a je, dakle, djeljiv s 2, a b s 3.
Za $a=2$ vrijedi $b=3$ pa je kandidat za rješenje broj 23. No, 23 nije djeljiv s 3 pa nije rješenje.
Za $a=4$ vrijedi $b=6$ pa je kandidat za rješenje broj 46. No, 46 nije djeljiv s 3 pa nije rješenje.
Za $a=6$ vrijedi $b=9$ pa je kandidat za rješenje broj 69. 69 je djeljiv s 3 pa je i jedino rješenje.

Primjer 3.2.3. Odredi a, b, c i d, znamenke dolje navedenih brojeva ako vrijedi:

$$\begin{array}{rcccc}
 & & a & b & c\\
+ & & & b & a\\
\hline
 & d & c & c & a
\end{array}$$

Rješenje. Zbog $c+a=a$ mora biti $c=0$.
Dalje mora biti $b=0$ ili $b=5$.
Kada bi bilo $b=0$, na mjestu stotica imali bismo $a=c$ i ne bi bilo prijenosa na mjesto tisućice. Stoga mora biti $b=5$.
$a=9$ i $d=1$.
Ukupno:

$$\begin{array}{rcccc}
 & & 9 & 5 & 0\\
+ & & & 5 & 9\\
\hline
 & 1 & 0 & 0 & 9
\end{array}$$

Primjer 3.2.4. Odredi sve one parove prirodnih brojeva a i b za koje vrijedi

1. a nije djeljiv s b i b nije djeljiv s a,

2. $\text{nzd}(a, b) = 24$ i
3. $\text{nzv}(a, b) = 504$.

Rješenje. $\text{nzd}(a, b) = 24$ znači $a = 24 \cdot x$ za neki prirodni broj x i $b = 24 \cdot y$ za neki prirodni broj y. Osim toga, x i y su relativno prosti, tj. najveći im je zajednički djelitelj 1 (da su djeljivi s npr. 2 onda bi bilo $\text{nzd}(a, b) = 48$).

$\text{nzv}(a, b) = 504$ znači da je 504 djeljiv i s a i s b.
504 je, dakle, djeljiv i s $24x$ i s $24y$.
$504 : 24$ je, dakle, djeljiv i s x i s y.
21 je djeljiv i s x i s y.

Moguće je:

a) $x = 3$, $y = 7$,
b) $x = 7$, $y = 3$.

U slučaju pod a), vrijedi $a = 72$, $b = 168$, što je jedno rješenje.
U slučaju pod b), vrijedi $a = 168$, $b = 72$, što je drugo rješenje.

Primjer 3.2.5. Odredi sve one parove prirodnih brojeva a i b za koje vrijedi:

$$\text{nzv}(a, b) - \text{nzd}(a, b) = 30.$$

Rješenje. Neka je $a = x \cdot \text{nzd}(a, b)$, $b = y \cdot \text{nzd}(a, b)$. ($x$ i y nemaju zajedničkog djelitelja osim broja 1).
Iz $a \cdot b = \text{nzv}(a, b) \cdot \text{nzd}(a, b)$ slijedi

$$\begin{aligned} x \cdot \text{nzd}(a, b) \cdot y \cdot \text{nzd}(a, b) &= \text{nzv}(a, b) \cdot \text{nzd}(a, b) \quad / : \text{nzd}(a, b) \\ x \cdot y \cdot \text{nzd}(a, b) &= \text{nzv}(a, b). \end{aligned}$$

Iz uvjeta zadatka

$$\text{nzv}(a, b) - \text{nzd}(a, b) = 30$$

slijedi

$$\begin{aligned} x \cdot y \cdot \text{nzd}(a, b) - \text{nzd}(a, b) = 30, \quad \text{tj.} \\ \text{nzd}(a, b) \cdot (x \cdot y - 1) = 30. \end{aligned}$$

Sada imamo sljedeće mogućnosti:

1. $\text{nzd}(a, b) = 1$, $x \cdot y - 1 = 30$. Iz toga slijedi da je $x \cdot y = 31$.
   Dakle, ili je $x = 1$, $y = 31$, tj. $a = 1$, $b = 31$ ili je $x = 31$, $y = 1$, tj. $a = 31$, $b = 1$.

2. $\text{nzd}(a, b) = 2$, $x \cdot y - 1 = 15$. Iz toga slijedi da je $x \cdot y = 16$.
   Dakle,

   ili je $x = 1$, $y = 16$, tj. $a = 2$, $b = 32$

   ili je $x = 2$, $y = 8$ (ovo nije moguće jer x i y moraju biti relativno prosti)

   ili je $x = 4$, $y = 4$ (ovo nije moguće jer x i y moraju biti relativno prosti)

   ili je $x = 8$, $y = 2$ (ovo nije moguće jer x i y moraju biti relativno prosti)

   ili je $x = 16$, $y = 1$, tj. $a = 32$, $b = 2$.

3. $\text{nzd}(a, b) = 3$, $x \cdot y - 1 = 10$. Iz toga slijedi da je $x \cdot y = 11$.
   Dakle,

   ili je $x = 1$, $y = 11$, tj. $a = 3$, $b = 33$

   ili je $x = 11$, $y = 1$, tj. $a = 33$, $b = 3$.

4. $\text{nzd}(a, b) = 5$, $x \cdot y - 1 = 6$. Iz toga slijedi da je $x \cdot y = 7$.
   Dakle,

   ili je $x = 1$, $y = 7$, tj. $a = 5$, $b = 35$

   ili je $x = 7$, $y = 1$, tj. $a = 35$, $b = 5$.

5. $\text{nzd}(a, b) = 6$, $x \cdot y - 1 = 5$. Iz toga slijedi da je $x \cdot y = 6$.
   Dakle,

   ili je $x = 1$, $y = 6$, tj. $a = 6$, $b = 36$

   ili je $x = 2$, $y = 3$, tj. $a = 12$, $b = 18$

   ili je $x = 3$, $y = 2$, tj. $a = 18$, $b = 12$

   ili je $x = 6$, $y = 1$, tj. $a = 36$, $b = 6$.

6. $\text{nzd}(a, b) = 10$, $x \cdot y - 1 = 3$. Iz toga slijedi da je $x \cdot y = 4$.
   Dakle,

   ili je $x = 1$, $y = 4$, tj. $a = 10$, $b = 40$

   ili je $x = 2$, $y = 2$ (ovo nije moguće jer x i y moraju biti relativno prosti)

   ili je $x = 4$, $y = 1$, tj. $a = 40$, $b = 10$.

7. $\text{nzd}(a, b) = 15$, $x \cdot y - 1 = 2$. Iz toga slijedi da je $x \cdot y = 3$.
   Dakle,

   ili je $x = 1$, $y = 3$, tj. $a = 15$, $b = 45$

   ili je $x = 3$, $y = 1$, tj. $a = 45$, $b = 15$.

8. $\text{nzd}(a, b) = 30$, $x \cdot y - 1 = 1$. Iz toga slijedi da je $x \cdot y = 2$.
   Dakle,

   ili je $x = 1$, $y = 2$, tj. $a = 30$, $b = 60$

   ili je $x = 2$, $y = 1$, tj. $a = 60$, $b = 30$.

Primjer 3.2.6. Zbroj znamenaka prirodnog broja x jednak je razlici $223 - x$. Odredi x.

Rješenje. Prirodni broj x ne može biti jednoznamenkasti jer bi $223 - x$ bio onda troznamenkasti.
Prirodni broj x ne može biti dvoznamenkasti jer bi $223 - x$ bio onda troznamenkasti.
Prirodni broj x ne može biti veći od 223 jer bi $223 - x$ bio manji od nule, a zbroj znamenaka ne može biti manji od nule.
Prirodni broj x mora, dakle, biti troznamenkasti.

Neka je $x = 100a + 10b + c$ za neke znamenke a, b i c.
Slijedi, iz uvjeta zadatka,

$$a + b + c = 223 - (100a + 10b + c),$$

odnosno

$$101a + 11b + 2c = 223.$$

Kako je $a > 0$ i $a < 3$ može biti samo $a = 1$ ili $a = 2$.

- Za $a = 1$: $101 + 11b + 2c$ je manji ili jednak od $101 + 99 + 18 = 218$ pa ne može biti 223.
- Za $a = 2$: $202 + 11b + 2c = 223$. Slijedi da je $11b + 2c = 21$, pa odatle da je $b = 1$ te $c = 5$.

Jedino je, dakle, rješenje $x = 215$.

Primjer 3.2.7. Koji su troznamenkasti brojevi pet puta veći od umnoška svojih znamenki?

Rješenje.

$$100a + 10b + c = 5 \cdot a \cdot b \cdot c$$

Broj s desne strane je višekratnik broja 5 pa i lijeva strana mora biti djeljiva s 5, pa je c, dakle, ili nula ili pet.
No, c ne može biti nula jer bi onda umnožak s desne strane bio nula pa broj $100a + b + c$ također mora biti nula, što ne može biti jer onda zadani broj ne bi bio troznamenkasti.
Dakle, c mora biti 5.

Slijedi

$$\begin{aligned} 100a + 10b + 5 &= 5 \cdot a \cdot b \cdot 5 \\ 100a + 10b + 5 &= 25 \cdot a \cdot b \quad / : 5 \\ 20a + 2b + 1 &= 5ab. \end{aligned}$$

Broj s desne strane je višekratnik broja 5 pa i lijeva strana mora biti djeljiva s 5, pa je $2 \cdot b + 1$ djeljiv s 5.
$2 \cdot b + 1$ je neparan broj, dakle, može biti ili 5 ili 15 (budući da je b znamenka, dakle, ne veća od 9, $2 \cdot b + 1$ ne može biti veći od 20).

a) $2 \cdot b + 1 = 5$ daje $b = 2$ što ne može biti jer mora biti $20a + 2b + 1 = 5ab$, a za $b = 2$ bi bilo $20a + 5 = 10a$.

b) $2 \cdot b + 1 = 15$ daje $b = 7$, što daje $20a + 2 \cdot 7 + 1 = 35a$, odnosno $a = 1$.

Konačno rješenje je 175, i zaista $175 = 5 \cdot 1 \cdot 7 \cdot 5$.

Primjer 3.2.8. Odredi prirodne brojeve x i y za koje vrijedi

1. 2014 je djeljiv s $x + y$ i
2. $(x + y)^{x+y}$ djeljiv je s $x^y \cdot y^x$.

Rješenje. Prije svega $2014 = 2 \cdot 19 \cdot 53$.
Slijedi da je 2014 djeljiv s (i samo s) 1, 2, 19, 53, 38, 106, 1007 i 2014.
Dakle, $x + y \in \{1, 2, 19, 53, 38, 106, 1007, 2014\}$.

Uvjet djeljivosti znači da postoji prirodni broj K za koji je

$$\frac{(x + y)^{x+y}}{x^y \cdot y^x} = K.$$

Slijedi

$$\begin{aligned} \frac{(x + y)^x \cdot (x + y)^y}{x^y \cdot y^x} &= K \\ \frac{(x + y)^x}{y^x} \cdot \frac{(x + y)^y}{x^y} &= K \\ \left(\frac{x}{y} + 1\right)^x \cdot \left(\frac{y}{x} + 1\right)^y &= K. \end{aligned}$$

Ovdje vidimo da će se u zagradama pojaviti ili cijeli brojevi, ako je $x = y$, ili razlomci (koji potencirani ili pomnoženi možda neće moći u umnošku dati cijeli broj K).
Stoga dolazimo na ideju da mora biti $x = y$, no to treba i dokazati.

Neka je $d = \text{nzd}(x, y)$. Neka je, dakle, $x = d \cdot a$, $y = d \cdot b$, pri čemu su a i b relativno prosti.

$$(x+y)^{x+y} \text{ djeljiv je s } x^y \cdot y^x.$$

Znači da je

$$d^{x+y} \cdot (a+b)^{x+y} \text{ djeljiv s } (da)^{db} \cdot (db)^{da} = d^{db} \cdot d^{da} \cdot a^{db} \cdot b^{da} = d^{x+y} \cdot a^y \cdot b^x,$$

tj.

$$(a+b)^{x+y} \text{ djeljiv je s } a^y \cdot b^x.$$

To znači da je $(a+b)^{x+y}$ djeljiv i s a^y i s b^x.
Budući da je $\text{nzd}(a, b) = 1$, slijedi da je i

$$\text{nzd}(a+b, a) = \text{nzd}(a+b, b) = 1.$$

Mora, dakle, biti $a = b = 1$ ako želimo da $(a+b)^{x+y}$ bude djeljiv i s a^y i s b^x.
A $a = b = 1$ znači $x = d \cdot a = d$, $y = d \cdot b = d$, tj. $x = y$.

$x + y \in \{1, 2, 19, 53, 38, 106, 1007 \text{ i } 2014\}$ i $x = y$ daje rješenja:

$$x_1 = y_1 = 1,$$
$$x_2 = y_2 = 19,$$
$$x_3 = y_3 = 53,$$
$$x_4 = y_4 = 1007.$$

Primjer 3.2.9. Prirodan broj n je paran, umnožak je triju prostih brojeva (među kojima može biti i jednakih) i zbroj svih djelitelja broja n jednak je $2n$. Odredi n.

Rješenje. $28 = 2 \cdot 2 \cdot 7$
$1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28.$
Postupak rješavanja u ovom je zadatku bolje prepustiti računalu.

(Ako je $n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot p_4^{e_4} \cdot \ldots \cdot p_k^{e_k}$ onda zbroj svih djelitelja broja n možemo izračunati formulom

$$S(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{e_k+1} - 1}{p_k - 1}.$$

Na primjer, kako je $28 = 2^2 \cdot 7$,

$$S(28) = \frac{2^3 - 1}{2 - 1} \cdot \frac{7^2 - 1}{7 - 1} = 7 \cdot 8 = 56.)$$

Primjer 3.2.10. Pokaži da je $2^1 + 2^2 + 2^3 + 2^4 + \ldots + 2^{2020}$ djeljiv s 3.

Rješenje.

$$\begin{aligned} 2^1 + 2^2 + 2^3 + 2^4 + \ldots + 2^{2020} &= 2^1 \cdot (1+2) + 2^3 \cdot (1+2) + 2^5 \cdot (1+2) + \ldots + \\ &\quad + 2^{2019} \cdot (1+2) \\ &= 3 \cdot (2^1 + 2^3 + \ldots + 2^{2019}). \end{aligned}$$

3.3. Kongruencije

Cilj je potpoglavlja 3.3. detaljno objasniti značenje kongruencija, dati pregled osnovnih svojstava kongruencija i poučiti čitatelja služiti se ovim alatom u zadacima vezanim uz dijeljenje te zadacima vezanima uz prirodne i cijele brojeve općenito.

Literatura za kongruencije:

1. A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

2. A. Dujella, *Uvod u teoriju brojeva* (skripta), PMF – Matematički odjel (str. 12. do 29.)
   Cijela skripta dostupna je na http://e.math.hr/zeta/utblink.pdf (zadnji pristup travanj 2022.)

3. I. Ilišević, *Kongruencije*, Osječki matematički list 1, No. 2, (2001); 103–108

Početak teorije kongruencija nalazi se u knjizi Disquisitiones Arithmeticae iz 1801. godine čiji je autor Carl Friedrich Gauss. Gauss je za kongruencije uveo oznaku “ $\equiv$ ” koju koristimo i danas.

Po teoremu o dijeljenju s ostatkom, ako podijelimo cijeli broj a prirodnim brojem b, dobivamo rezultat q i ostatak r, $r \in \{0, 1, 2, \ldots, b-1\}$.

Primjer 3.3.1.
$6 : 5 = 1$ i ostatak je 1.
$-6 : 5 = -2$ i ostatak je 4.
$-9 : 5 = -2$ i ostatak je 1.

Vidimo kako brojevi 6 i -9 pri dijeljenju s 5 daju isti ostatak, 1.
Koliko ima takvih brojeva koji pri dijeljenju s 5 daju ostatak 1? To su svi brojevi iz skupa

$$\{\ldots, -14, -9, -4, 1, 6, 11, 16, 21, 26, 31, 36, \ldots\},$$

tj. ima ih beskonačno i oblika su $5k + 1$, $k \in \mathbb{Z}$.

Definicija 3.3.1. *Ako cijeli brojevi a i b pri dijeljenju brojem n daju isti ostatak, kažemo da su a i b “kongruentni modulo n” i pišemo*

$$a \equiv b \pmod{n}.$$

Ako za brojeve a i b to ne vrijedi, pišemo $a \not\equiv b \pmod{n}$.
Ponekad, ako i a i b i c imaju isti ostatak pri dijeljenju s n, pišemo

$$a \equiv b \equiv c \pmod{n}.$$

U izrazu $a \equiv b \pmod{n}$, a ćemo zvati lijeva strana kongruencije, b desna strana kongruencije, a broj n ćemo zvati modul.

Zanimljivo je da kada napišemo $a \equiv b \pmod{n}$, mi samo znamo da a i b pri dijeljenju s n daju isti ostatak, a ne znamo o kojem je ostatku je riječ, tj. sama garancija, odnosno "certifikat" kongruencije u izrazu se ne navodi.

U nekim knjigama kongruencija se definira na sljedeći način: $a \equiv b$ ako i samo ako je $a - b$ djeljiv s n. Ta je definicija ekvivalentna našoj jer ako a i b daju isti ostatak x pri dijeljenju s n, onda vrijedi $a = k \cdot n + x$, $b = m \cdot n + x$, pa je

$$a - b = k \cdot n - m \cdot n = (k - m) \cdot n,$$

tj. $a - b$ je djeljiv s n.

Obrnuto, ako je $a - b$ djeljiv s n, onda možemo pisati $a - b = kn$, tj. $a = kn + b$. Ako je x ostatak pri dijeljenju broja b brojem n, tj. $b = pn + x$, $x \in \{0, 1, 2, \ldots, n - 1\}$, onda je

$$a = kn + b = kn + pn + x = (k + p) \cdot n + x, \quad x \in \{0, 1, 2, \ldots, n - 1\},$$

tj. x je ostatak pri dijeljenju broja a brojem n.

Primjer 3.3.2.

a) $2 \equiv -5 \pmod{7}$ jer $2 - (-5)$ je djeljivo sa 7.
Također, na drugi način: Od broja 2 do broja -5, može se doći koracima veličine 7, hodajući lijevo ili desno.

b) $0 \equiv 2 \pmod{1}$ jer 0 i 2 pri dijeljenju s 1 daju ostatak: 0.
Također, na drugi način: Od broja 0 do broja 2, može se doći koracima veličine 1.

Primjer 3.3.3. Odredi neke x za koje je $23 \equiv x \pmod{7}$.

Rješenje. 23 pri dijeljenju sa 7 daje ostatak 2, pa su rješenje svi brojevi koji pri dijeljenju sa 7 daju ostatak 2, tj. svi brojevi oblika $7k + 2$, tj. brojevi iz skupa

$$\{\ldots, -12, -5, 2, 9, 16, \ldots\}.$$

Također, na drugi način: U koje sve brojeve stižemo krećući se od broja 23 koracima veličine 7? $23 + 7 = 30$, $30 + 7 = 37$, $\ldots$, $23 - 7 = 16$, $\ldots$

Primjer 3.3.4. Odredi neke x za koje je $23 \equiv 7 \pmod{x}$.

Rješenje. 23 i 7 pri dijeljenju s x daju isti ostatak.
Odmah se nudi kao rješenje $x = 1$ jer vrijedi $a \equiv b \pmod{1}$ za sve cijele brojeve a i b.
Kako su 7 i 23 neparni, pri dijeljenju s 2 dat će ostatak 1. Drugo je rješenje $x = 2$.
Treće rješenje je $x = 4$ jer 23 i 7 pri dijeljenju s 4 daju isti ostatak, 3.
Četvrto rješenje je $x = 8$ jer 23 i 7 pri dijeljenju s 8 daju isti ostatak, 7.
Za sve brojeve x veće od 7, vrijedi da 7 pri dijeljenju s njima daje ostatak 7. Budući da je $23 - 7 = 16$, slijedi da 23 pri dijeljenju sa 16 daje ostatak 7. Peto je rješenje 16.
Za sve brojeve veće od 23, vrijedi da 7 pri dijeljenju s njima daje rezultat 0 i ostatak 7, a 23 pri dijeljenju s njima daje također rezultat 0 i ostatak 23.

Dakle, osim 1, 2, 4, 8 i 16 ova jednadžba više nema rješenja.

Svojstva kongruencija:

1. Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, onda je i

a) $a + c \equiv b + d \pmod{n}$ (kongruencije smijemo zbrajati),

b) $a - c \equiv b - d \pmod{n}$ (kongruencije smijemo oduzimati) i

c) $a \cdot c \equiv b \cdot d \pmod{n}$ (kongruencije smijemo množiti).

Primjer 3.3.5. Kako je

$$9 \equiv 4 \pmod{5}$$
$$7 \equiv -3 \pmod{5},$$

slijedi:

a) $9 + 7 \equiv 4 - 3 \pmod{5}$, tj. $16 \equiv 1 \pmod{5}$,

b) $9 - 7 \equiv 4 - (-3) \pmod{5}$, tj. $2 \equiv 7 \pmod{5}$ i

c) $9 \cdot 7 \equiv 4 \cdot (-3) \pmod{5}$, tj. $63 \equiv -12 \pmod{5}$.

2. Ako je $a \equiv b \pmod{n}$, onda je i

a) $a + k \cdot n \equiv b + m \cdot n \pmod{n}$ za bilo koje cijele brojeve k i m
(lijevoj i desnoj strani kongruencije možemo oduzeti ili zbrojiti modul koliko god želimo puta),

b) $k \cdot a \equiv k \cdot b \pmod{n}$ za svaki cijeli broj k
(kongruencije smijemo množiti cijelim brojem),

c) $k \cdot a \equiv k \cdot b \pmod{k \cdot n}$ za svaki cijeli broj k
(kongruencije smijemo množiti cijelim brojem tako da s istim brojem pomnožimo i modul) i

d) $a^m \equiv b^m \pmod{n}$ za svaki prirodni broj k
(kongruencije smijemo potencirati prirodnim brojem).

Primjer 3.3.6. Kako je $7 \equiv -3 \pmod{5}$, slijedi:

a) $7 + 4 \cdot 5 \equiv -3 - 2 \cdot 5 \pmod{5}$, tj. $27 \equiv -13 \pmod{5}$,

b) $3 \cdot 7 \equiv 3 \cdot (-3) \pmod{5}$, tj. $21 \equiv -9 \pmod{5}$,

c) $9 \cdot 7 \equiv 9 \cdot (-3) \pmod{9 \cdot 5}$, tj. $63 \equiv -27 \pmod{45}$ (ostatak je u oba slučaja 18) i

d) $7^3 \equiv (-3)^3 \pmod{5}$, tj. $343 \equiv -27 \pmod{5}$.

3. a) Ako je $ak \equiv bk \pmod{n}$ i $\text{nzd}(k, n) = 1$, onda je i $a \equiv b \pmod{n}$.
(Kongruenciju smijemo podijeliti s brojem koji je s modulom relativno prost.)

b) Ako je $ak \equiv bk \pmod{nk}$, onda je i $a \equiv b \pmod{n}$.
(Kongruenciju smijemo podijeliti nekim brojem tako da podijelimo i lijevu stranu kongruencije i desnu stranu kongruencije i modul tim brojem, ako su, naravno, svi navedeni brojevi djeljivi tim brojem.)

c) Ako je $a \equiv b \pmod{n}$, onda je i $a \equiv b \pmod{d}$, gdje je d bilo koji djelitelj od n.

Primjer 3.3.7.

a) Kako je $21 \equiv 33 \pmod{4}$, slijedi da je (dijeljenjem s 3) $7 \equiv 11 \pmod{4}$,

b) Kako je $21 \equiv 33 \pmod{12}$, slijedi da je (dijeljenjem s 3) $7 \equiv 11 \pmod{4}$,

c) Kako je $21 \equiv 33 \pmod{12}$, slijedi da je

$$\begin{aligned} 21 &\equiv 33 \pmod{12}, \\ 21 &\equiv 33 \pmod{6}, \\ 21 &\equiv 33 \pmod{4}, \\ 21 &\equiv 33 \pmod{3}, \\ 21 &\equiv 33 \pmod{2} \quad \text{i} \\ 21 &\equiv 33 \pmod{1}. \end{aligned}$$

Sada čitatelja pozivamo da, prije nego što prijeđe na čitanje nadolazećih primjera i zadataka, konstruira što više primjera kongruencija te da na tim primjerima isproba sva navedena pravila.

Primjer 3.3.8. Odredi ostatak pri dijeljenju broja 7^{12345} s 4.

Rješenje.

$7 \equiv 7 \pmod 4$ (Jer, trivijalno, broj 7 daje ostatak pri dijeljenju s 4 kao i broj 7.)

$7 \equiv 7 \pmod 4$ / Oduzmimo $1 \cdot 4$ desnoj strani, po pravilu 2 a). (To pišemo kao -4 D. S.)

$7 \equiv 3 \pmod 4$ / Pomnožimo lijevu stranu i desnu stranu kongruencije sa 7 ($\cdot$ 7 L.S., D. S.)

$7^2 \equiv 21 \pmod 4$ / $-5 \cdot 4$ D. S.

$7^2 \equiv 1 \pmod 4$

Kad s desne strane u ovakvim zadacima dobijemo broj 1 ili broj -1, gotovi smo s velikim dijelom posla jer se 1 i -1 vrlo lako potenciraju i kongruenciju možemo potencirati bilo kojim prirodnim eksponentom.

$$
\begin{aligned}
12345 : 2 &= 6172 \text{ i ostatak je 1.} \\
7^2 &\equiv 1 \pmod 4 \quad /\ ^{6172} \\
7^{12344} &\equiv 1 \pmod 4 \quad / \cdot 7 \ \text{ L.S., D. S.} \quad \text{ili kratko: } / \cdot 7 \\
7^{12345} &\equiv 7 \pmod 4 \quad / -4 \ \text{ D.S.} \\
7^{12345} &\equiv 3 \pmod 4
\end{aligned}
$$

Ostatak pri dijeljenju broja 7^{12345} s 4 je 3.

Primjer 3.3.9. Odredi zadnje dvije znamenke broja 2^{2222}.

Rješenje. Prvo treba uočiti kako su zadnje dvije znamenke broja (dvoznamenkasti završetak broja) ostatak pri dijeljenju tog broja sa 100.
Stoga ispitujemo koji dvoznamenkasti broj x ima svojstvo

$$2^{2222} \equiv x \pmod{100}.$$

$$
\begin{aligned}
2^1 &\equiv 2 \pmod{100} \\
2^2 &\equiv 4 \pmod{100} \\
2^3 &\equiv 8 \pmod{100} \\
2^4 &\equiv 16 \pmod{100} \\
2^5 &\equiv 32 \pmod{100} \\
2^6 &\equiv 64 \pmod{100} \\
2^7 &\equiv 28 \pmod{100} \\
2^8 &\equiv 56 \pmod{100} \\
&\dots
\end{aligned}
$$

Uočavamo da na desnoj strani nikada nećemo dobiti niti 1 niti -1 jer su potencije broja 2 su parni brojevi i ne mogu završavati s 01 kao niti s 99.
Možemo stoga istražiti djeljivost s 50 umjesto sa 100 (i na kraju pomnožiti sva tri broja kongruencije s 2 po pravilu 2 c) pa ćemo opet dobiti u zagradi mod 100, odnosno zadnje dvije znamenke).
No, potencije broja dva niti pri dijeljenju s 50 ne mogu dati ostatak 1 kao niti 49.

I sljedeći isti takav korak: ako ne gledamo djeljivost s 50 nego s 25, i na kraju pomnožimo sva tri broja kongruencije s 4 po pravilu 2 c), opet ćemo dobiti na kraju mod 100, odnosno zadnje dvije znamenke. Pogledajmo kakav ostatak daje 2^{2220} pri dijeljenju s 25.
Sada s lijeve strane redom potenciramo broj 2, a s desne čekamo 01 ili 24.

$$\begin{aligned}
2^1 &\equiv 2 \pmod{25}\\
2^2 &\equiv 4 \pmod{25}\\
2^3 &\equiv 8 \pmod{25}\\
2^4 &\equiv 16 \pmod{25}\\
2^5 &\equiv 7 \pmod{25}\\
2^6 &\equiv 14 \pmod{25}\\
2^7 &\equiv 3 \pmod{25}\\
2^8 &\equiv 6 \pmod{25}\\
2^9 &\equiv 12 \pmod{25}\\
2^{10} &\equiv 24 \pmod{25}
\end{aligned}$$

Broj 24 na desnoj strani sada nam odgovara jer oduzimanjem modula dobivamo -1.

$$\begin{aligned}
2^{10} &\equiv 24 \pmod{25} && / - 25 \ \text{D.S.}\\
2^{10} &\equiv -1 \pmod{25} && /^{222}\\
2^{2220} &\equiv 1 \pmod{25} && / \cdot 2^2 = 4 \ \text{L.S, D.S. i modul}\\
2^{2222} &\equiv 4 \pmod{100}
\end{aligned}$$

Dakle: Broj 2^{2222} završava s 04.

Primjer 3.3.10. Odredi ostatak pri dijeljenju broja $22 \cdot 33^{44} - 55^{66} \cdot 77^{88}$ s 9.

Rješenje. Prvo ćemo odrediti ostatak pri dijeljenju broja 33^{44} s 9 i taj broj pomnožiti s 22. Zatim ćemo pronaći ostatak pri dijeljenju broja 55^{66} s 9 i 77^{88} s 9 i ta dva broja pomnožiti. Na kraju ćemo naći razliku dobivenih rezultata, sve po pravilima 1 b), 1 c) i 2 c).

A.

$$\begin{aligned} 33 &\equiv 6 \pmod 9 && /^{2} \\ 33^2 &\equiv 36 \pmod 9 \\ 33^2 &\equiv 0 \pmod 9 && /^{22} \\ 33^{44} &\equiv 0 \pmod 9 && / \cdot 22 \\ 22 \cdot 33^{44} &\equiv 0 \pmod 9. \end{aligned}$$

B.

$$\begin{aligned} 55 &\equiv 1 \pmod 9 && /^{66} \\ 55^{66} &\equiv 1 \pmod 9 \end{aligned}$$

C.

$$\begin{aligned} 77 &\equiv 5 \pmod 9 && /^{2}\ (1) \\ 77^2 &\equiv 25 \pmod 9 && / -2\cdot 9 \quad \text{D.S.} \\ 77^2 &\equiv 7 \pmod 9 && / \cdot \ \text{red } (1) \\ 77^3 &\equiv 35 \pmod 9 && / -4\cdot 9 \quad \text{D.S.} \\ 77^3 &\equiv -1 \pmod 9 && /^{29} \\ 77^{87} &\equiv -1 \pmod 9 && / \cdot \ \text{red } (1) \\ 77^{88} &\equiv -5 \pmod 9 && / +9 \quad \text{D.S.} \\ 77^{88} &\equiv 4 \pmod 9. \end{aligned}$$

B. i C. $\quad 55^{66} \cdot 77^{88} \equiv 1 \cdot 4 \pmod 9$

A. i B. i C.:

$$\begin{aligned} 22 \cdot 33^{44} - 55^{66} \cdot 77^{88} &\equiv 0 - 4 \pmod 9 \\ 22 \cdot 33^{44} - 55^{66} \cdot 77^{88} &\equiv -4 \pmod 9 && / +9 \qquad \text{D.S.} \\ 22 \cdot 33^{44} - 55^{66} \cdot 77^{88} &\equiv 5 \pmod 9. \end{aligned}$$

Ostatak pri dijeljenju broja $22 \cdot 33^{44} - 55^{66} \cdot 77^{88}$ s 9 je 5.

Primjer 3.3.11. Odredi ostatak pri dijeljenju broja 1234^{4321} s 18.

Rješenje 1. 1234 na bilo koju potenciju neće pri dijeljenju s 18 dati ostatak 1 kao niti ostatak 17 pri dijeljenju s 18 jer su i djelitelj i djeljenik parni pa i ostatak mora biti paran broj.
Stoga možemo na početku rastaviti broj 1234. $1234 = 2 \cdot 617$.

A. Nađimo ostatak pri dijeljenju broja 2^{4321} s 18.
Opet su i 2 i 18 parni pa ostatak pri dijeljenju neke potencije broja 2 sa 18 nikada neće biti 1 niti 17.

Stoga moramo 18 rastaviti na $18 = 2 \cdot 9$.
Pronaći ćemo ostatak pri dijeljenju 2^{4320} s 9, a onda ćemo obje strane kongruencije i modul pomnožiti s 2 po pravilu 2 c).

$$\begin{aligned} 2^3 &\equiv -1 \pmod 9 && /^{1440} \\ 2^{4320} &\equiv 1 \pmod 9 && / \cdot 2 \\ 2^{4321} &\equiv 2 \pmod{18}. \end{aligned}$$

B. Nađimo ostatak pri dijeljenju broja 617^{4321} s 18.

$$\begin{aligned} 617 &\equiv 5 \pmod{18} && /^{2} \quad (1) \\ 617^2 &\equiv 7 \pmod{18} && / \cdot \text{ red } (1) \\ 617^3 &\equiv 35 \pmod{18} && / - 2 \cdot 18 \ \text{ D.S.} \\ 617^3 &\equiv -1 \pmod{18} && /^{1440} \\ 617^{4320} &\equiv 1 \pmod{18} && / \cdot \text{ red } (1) \\ 617^{4321} &\equiv 5 \pmod{18}. \end{aligned}$$

A. i B.:

$$\begin{aligned} 2^{4321} \cdot 617^{4321} &\equiv 2 \cdot 5 \pmod{18} \\ 1234^{4321} &\equiv 10 \pmod{18}. \end{aligned}$$

Rješenje 2.

$$\begin{aligned} 1234 &\equiv 10 \pmod{18} && /^{4321} \\ 1234^{4321} &\equiv 10^{4321} \pmod{18}. \end{aligned}$$

Stoga treba u stvari naći koliki je ostatak pri djeljenju broja 10^{4321} s 18.
$10 = 2 \cdot 5$ pa treba naći ostatak pri dijeljenju broja 2^{4321} s 18 i ostatak pri dijeljenju broja 5^{4321} s 18 i te brojeve pomnožiti. Rješenje je $2 \cdot 5 = 10$.

Rješenje 3. (i najjednostavnije rješenje)

$1234 \equiv 10 \pmod{18}$, tj. 1234^x daje pri dijeljenju s 18 isti ostatak kao i 10^x za svaki $x \in \mathbb{N}$.

$$\begin{aligned} 10 &\equiv 10 \pmod{18} && / \cdot 10 \\ 10^2 &\equiv 100 \pmod{18} && / - 5 \cdot 18 \qquad \text{D.S.} \\ 10^2 &\equiv 10 \pmod{18}. \end{aligned}$$

Vidimo da se množenjem početne kongruencije s 10 lijeva strana se poveća 10 puta, a desna ostaje i dalje deset. Zaključujemo kako svaka potencija broja 10 pri dijeljenju s 18 daje ostatak 10.

$$1234^{4321} \equiv 10^{4321} \equiv 10 \pmod{18}.$$

Zadaci za vježbu

Zadatak 3.3.1. Ako 9^{40} završava s 01, odredi dvoznamenkasti završetak broja 9^{37}.

Zadatak 3.3.2. Dokaži da jednadžba $x^2 - 3y = 5$ nema cjelobrojnih rješenja.

Zadatak 3.3.3. Odredi ostatak pri dijeljenju broja $2^{123} + 3^{123} + 23^{123}$ s 11.

Zadatak 3.3.4. Odredi zadnje tri znamenke broja 234^{987}.

Zadatak 3.3.5. Riješi jednadžbu $8x \equiv 6 \pmod{14}$.

Rješenja

3.3.1. $9^{40} \equiv 1 \pmod{100}$. Ovaj red ne možemo podijeliti s 9 kako bismo dobili 9^{39} jer 1 nije djeljiv s 9. Stoga desnoj strani treba prvo dodati višekratnik od 100 tako da zbroj bude djeljiv s 9.

$$\begin{aligned}
9^{40} &\equiv 1 \pmod{100} && / +800 \text{ D.S.}\\
9^{40} &\equiv 801 \pmod{100} && / : 9\\
9^{39} &\equiv 89 \pmod{100} && / +100 \text{ D.S.}\\
9^{39} &\equiv 189 \pmod{100} && / : 9\\
9^{38} &\equiv 21 \pmod{100} && / +600 \text{ D.S.}\\
9^{37} &\equiv 621 \pmod{100} && / : 9\\
9^{37} &\equiv 69 \pmod{100}.
\end{aligned}$$

Zadnje dvije znamenke broja 9^{37} su 69.

3.3.2. Jednadžba kaže da x^2 umanjen za neki broj oblika $3y$ daje broj 5.
Ako je $x = 3k$ za neki $k \in \mathbb{Z}$, onda je

$$x^2 \equiv (3k)^2 \equiv 0 \pmod{3}.$$

Ako je $x = 3k + 1$ za neki $k \in \mathbb{Z}$, onda je

$$x^2 \equiv (3k+1)^2 \equiv 9k^2 + 6k + 1 \equiv 1 \pmod{3}.$$

Ako je $x = 3k + 2$ za neki $k \in \mathbb{Z}$, onda je

$$x^2 \equiv (3k+2)^2 \equiv 9k^2 + 12k + 4 \equiv 1 \pmod 3.$$

x^2 je, dakle, ili djeljiv s 3 ili pri dijeljenju s tri daje ostatak 1.
Tj. ili je $x^2 \equiv 0 \pmod 3$ ili je $x^2 \equiv 1 \pmod 3$. U oba slučaja, ako kongruenciji zbrojimo ili oduzmemo višekratnik od 3 (tj. ako oduzmemo broj $3y$), $x^2 - 3y$ je ili kongruentan s 0 ili s 1 (mod 3),a $5 \equiv 2 \pmod 3$. Stoga navedena jednadžba nema rješenje.

3.3.3. Prvo ćemo odrediti ostatak pri dijeljenju broja 2^{123} s 11. Zatim ćemo pronaći ostatak pri dijeljenju broja 3^{123} s 11 te ostatak pri dijeljenju broja 23^{123} s 11. Na kraju ćemo naći zbroj dobivenih rezultata.

A.

$$\begin{aligned}
2 &\equiv 2 \pmod{11} && /^{2}\\
2^2 &\equiv 4 \pmod{11} && / \cdot 2\\
2^3 &\equiv 8 \pmod{11} && / \cdot 2\\
2^4 &\equiv 5 \pmod{11} && / \cdot 2\\
2^5 &\equiv 10 \pmod{11} && / -11 \text{ D.S.}\\
2^5 &\equiv -1 \pmod{11} && /^{24}\\
2^{120} &\equiv 1 \pmod{11} && / \cdot 2^3\\
2^{123} &\equiv 8 \pmod{11}
\end{aligned}$$

B.

$$\begin{aligned}
3 &\equiv 3 \pmod{11} && /^{2}\\
3^2 &\equiv 9 \pmod{11} && / \cdot 3\\
3^3 &\equiv 5 \pmod{11} && / \cdot 3\\
3^4 &\equiv 4 \pmod{11} && / \cdot 3\\
3^5 &\equiv 1 \pmod{11} && /^{24}\\
3^{120} &\equiv 1 \pmod{11} && / \cdot 3^3\\
3^{123} &\equiv 5 \pmod{11}
\end{aligned}$$

C.

$$\begin{aligned}
23 &\equiv 1 \pmod{11} && /^{123}\\
23^{123} &\equiv 1 \pmod{11}
\end{aligned}$$

$$2^{123} + 3^{123} + 23^{123} \equiv 8 + 5 + 1 \equiv 14 \equiv 3 \pmod{11}$$

Ostatak pri dijeljenju broja $2^{123} + 3^{123} + 23^{123}$ brojem 11 je 3.

3.3.4. $234 = 2 \cdot 117$

A. Odredimo zadnje tri znamenke broja 2^{987}.
Budući da je $987 = 512 + 256 + 128 + 64 + 16 + 8 + 2 + 1$, računamo zadnje tri znamenke potencija od 2^1 do 2^{512}.

$$\begin{aligned}
2 &\equiv 2 \pmod{1000} && /^{2}\\
2^2 &\equiv 4 \pmod{1000} && /^{2}\\
2^4 &\equiv 16 \pmod{1000} && /^{2}\\
2^8 &\equiv 256 \pmod{1000} && /^{2}\\
2^{16} &\equiv 536 \pmod{1000} && /^{2}\\
2^{32} &\equiv 296 \pmod{1000} && /^{2}\\
2^{64} &\equiv 616 \pmod{1000} && /^{2}\\
2^{128} &\equiv 456 \pmod{1000} && /^{2}\\
2^{256} &\equiv 936 \pmod{1000} && /^{2}\\
2^{512} &\equiv 096 \pmod{1000}
\end{aligned}$$

$$\begin{aligned}
2^{987} &\equiv 2^{512} \cdot 2^{256} \cdot 2^{128} \cdot 2^{64} \cdot 2^{16} \cdot 2^{8} \cdot 2^{2} \cdot 2^{1} \equiv\\
&\equiv 096 \cdot 936 \cdot 456 \cdot 616 \cdot 536 \cdot 256 \cdot 004 \cdot 002 \equiv 528 \pmod{1000}
\end{aligned}$$

B. Odredimo zadnje tri znamenke broja 117^{987}.

$$\begin{aligned}
117^1 &\equiv 117 \pmod{1000} && /^{7}\\
117^7 &\equiv 973 \pmod{1000} && / -1000 \text{ D.S.}\\
117^7 &\equiv -27 \pmod{1000} && /^{9}\\
117^{63} &\equiv -987 \pmod{1000} && / +1000 \text{ D.S.}\\
117^{63} &\equiv 13 \pmod{1000} && /^{2}\\
117^{126} &\equiv 169 \pmod{1000} && /^{2}\\
117^{252} &\equiv 561 \pmod{1000} && /^{3}\\
117^{756} &\equiv 481 \pmod{1000}.
\end{aligned}$$

Dalje,

$$\begin{aligned}
117^7 &\equiv -27 \pmod{1000} && /^{6}\\
117^{42} &\equiv 489 \pmod{1000} && /^{9}
\end{aligned}$$

Budući da je $987 = 756 + 126 + 63 + 6 \cdot 7$, slijedi da je

$$\begin{aligned}
117^{987} &\equiv 117^{756} \cdot 117^{126} \cdot 117^{63} \cdot 117^{42} \pmod{1000}\\
117^{987} &\equiv 481 \cdot 169 \cdot 13 \cdot 489 \pmod{1000}\\
117^{987} &\equiv 173 \pmod{1000}
\end{aligned}$$

A. i B.:

$$\begin{aligned}
234^{987} &= 2^{987} \cdot 117^{987} \\
234^{987} &\equiv 2^{987} \cdot 117^{987} \pmod{1000} \\
234^{987} &\equiv 528 \cdot 173 \pmod{1000} \\
234^{987} &\equiv 344 \pmod{1000}
\end{aligned}$$

3.3.5.

$$\begin{aligned}
8x &\equiv 6 \pmod{14} \qquad / :2 \ \text{ L. S. i D. S. i modul} \\
4x &\equiv 3 \pmod{7}
\end{aligned}$$

Sada nam je cilj s lijeve strane dobiti čisti x, bez koeficijenta.

$$\begin{aligned}
4x &\equiv 3 \pmod{7} \ \ / \cdot 2 \qquad \text{L. S. i D. S.} \\
8x &\equiv 6 \pmod{7} \\
7x + x &\equiv 6 \pmod{7} \ \ / - 7x \qquad \text{L. S.} \\
x &\equiv 6 \pmod{7} \\
x &= 7k + 6, \ \ k \in \mathbb{Z}.
\end{aligned}$$

3.4. Eulerov teorem i mali Fermatov teorem

Eulerov teorem i mali Fermatov teorem dodatak su prethodnom potpoglavlju, a cilj im je u ovom tekstu čitatelju pokazati kako može jednostavnije na desnoj strani kongruencije dobiti broj 1.

Nakon potpoglavlja 3.4. čitatelj će u rješavanju zadataka vezanih uz djeljivost i kongruencije znati primjenjivati Eulerovu funkciju i Eulerov teorem.

Osnovna literatura za potpoglavlje 3.4. jest:

1. A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.
2. A. Dujella, *Uvod u teoriju brojeva* (skripta), PMF – Matematički odjel (str. 16. do 18.)
   Cijela skripta dostupna je na `http://e.math.hr/zeta/utblink.pdf` (zadnji pristup travanj 2022.)

3. M. Jukić Bokun, A. Behin, *Eulerova funkcija*, math.e Hrvatski matematički elektronički časopis (Vol. 31. No. 1 2017.)
http://e.math.hr/Vol31/Bokun (zadnji pristup travanj 2022.)

Primjer 3.4.1. Brojevi koji su manji od 7 i sa 7 su relativno prosti su 1, 2, 3, 4, 5 i 6. Dakle, ukupno ih postoji 6. To pišemo kao $\varphi(7) = 6$.
Brojevi koji su manji od 12 i s 12 su relativno prosti su 1, 5, 7 i 11. Dakle, ukupno postoji 4 broja koji su manji od 12 i s 12 su relativno prosti. To pišemo kao $\varphi(12) = 4$.

Definicija 3.4.1. *Neka je n prirodan broj. Broj brojeva koji su manji od n i s njim su relativno prosti označavamo s $\varphi(n)$. Po dogovoru uzimamo $\varphi(1) = 1$.*
Funkciju φ zovemo ***Eulerova funkcija****.*

Pogledajmo prvih nekoliko vrijednosti funkcije φ.

Tablica 3.4.1: Tablica početnih vrijednosti za φ.

n	1	2	3	4	5	6
$\varphi(n)$	1	1	2	2	4	2

Primjer 3.4.2. Nadopuni gornju tablicu do $n = 15$.

Rješenje.

Tablica 3.4.2: Nadopunjena tablica 3.4.1

n	7	8	9	10	11	12	13	14	15
$\varphi(n)$	6	4	6	4	10	4	12	6	8

Teorem 3.4.1. *Neka je $n \in \mathbb{N}$ i neka je $n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot p_4^{e_4} \cdot \ldots \cdot p_k^{e_k}$ rastav broja n na proste faktore.Tada je*

$$\varphi(n) = p_1^{e_1-1} \cdot (p_1 - 1) \cdot p_2^{e_2-1} \cdot (p_2 - 1) \cdot p_3^{e_3-1} \cdot (p_3 - 1) \cdot p_4^{e_4-1} \cdot (p_4 - 1) \cdot \ldots \cdot p_k^{e_k-1} \cdot (p_k - 1).$$

Jednostavan i postepen dokaz ovog teorema dan je na http://e.math.hr/Vol31/Bokun (zadnji pristup travanj 2022.)

Primjer 3.4.3. Izračunaj $\varphi(100)$, $\varphi(144)$, $\varphi(1000)$.

Rješenje.

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = 2^1 \cdot (2 - 1) \cdot 5^1 \cdot (5 - 1) = 2 \cdot 1 \cdot 5 \cdot 4 = 40.$$
$$\varphi(144) = \varphi(2^4 \cdot 3^2) = 2^3 \cdot (2 - 1) \cdot 3^1 \cdot (3 - 1) = 8 \cdot 1 \cdot 3 \cdot 2 = 48.$$
$$\varphi(1000) = \varphi(2^3 \cdot 5^3) = 2^2 \cdot (2 - 1) \cdot 5^2 \cdot (5 - 1) = 4 \cdot 1 \cdot 25 \cdot 4 = 400.$$

Teorem 3.4.2. (Eulerov teorem o kongruencijama)
Neka su a i p prirodni brojevi koji su relativno prosti. Vrijedi

$$a^{\varphi(p)} \equiv 1 \pmod{p}.$$

Posebno, ako je p prost broj (tada su a i p relativno prosti i $\varphi(p) = p - 1$), vrijedi

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ova se tvrdnja zove mali Fermatov teorem.

Dokaze ovih teorema čitatelj također može naći na http://e.math.hr/Vol31/Bokun (zadnji pristup travanj 2022.)

Primjer 3.4.4.

a) Budući da su 3, 9 i 21 relativno prosti sa 100, slijedi

$$3^{40} \equiv 1 \pmod{100}$$
$$9^{40} \equiv 1 \pmod{100}$$
$$21^{40} \equiv 1 \pmod{100},$$

što u stvari znači da 3^{40}, 7^{40} i 9^{40} završavaju s 01.
Uočimo da 40 nije najmanji eksponent s tim svojstvom, tj. već je:

$$3^{20} \equiv 1 \pmod{100}$$
$$9^{10} \equiv 1 \pmod{100}$$
$$21^{5} \equiv 1 \pmod{100}.$$

To znači da ponekad postoji i manji eksponent uz koji je baza a kongruentna s 01 (mod p), ali $\varphi(n)$ uvijek možemo koristiti.

b) Iako je $7^{40} \equiv 1 \pmod{100}$, "već je" $7^4 \equiv 1 \pmod{100}$, a onda je i

$$7^8 \equiv 1 \pmod{100},\ 7^{12} \equiv 1 \pmod{100}, \ldots$$

c) $4^{\varphi(6)} \equiv 1 \pmod{6}$, tj. $4^2 \equiv 1 \pmod{6}$ naravno, nije istina, jer 4^2 i 6 su parni brojevi, pa i ostatak pri dijeljenju dva parna broja mora biti paran, tj. ne može biti 1. Greška je u tome što Eulerov teorem možemo upotrijebiti samo ako su a i n relativno prosti, a mi smo ga koristili za $a = 4$ i $b = 6$.

Zadaci za vježbu

Zadatak 3.4.1. Odredi zadnju znamenku broja 17^{171717}.

Zadatak 3.4.2. Odredi zadnje dvije znamenke broja 9^{99999}.

Zadatak 3.4.3. Odredi ostatak pri dijeljenju broja $5 \cdot 2^{1000} + 4 \cdot 3^{1000} + 3 \cdot 4^{1000}$ sa 7.

Rješenja

3.4.1. Kako su 17 i 10 relativno prosti i budući da je $\varphi(10) = 4$, slijedi da je

$$\begin{aligned} 17^4 &\equiv 1 \pmod{10} && /^{42929} \text{ (Jer } 171717 : 4 = 42929\text{, i ostatak je 1.)} \\ 17^{171716} &\equiv 1 \pmod{10} && / \cdot 17 \\ 17^{171717} &\equiv 17 \pmod{10} && / -10 \text{ D.S} \\ 17^{171717} &\equiv 7 \pmod{10} \end{aligned}$$

Zadnja znamenka broja 17^{171717} je 7.

3.4.2. Kako su 9 i 100 relativno prosti i budući da je $\varphi(100) = 40$, slijedi da je

$$\begin{aligned} 9^{40} &\equiv 1 \pmod{100} && /^{2499} \\ 9^{99960} &\equiv 1 \pmod{100}. \end{aligned}$$

Do 99999 nedostaje nam još 39. Odredimo zadnje dvije znamenke broja 9^{39}.

$$\begin{aligned} 9^{40} &\equiv 1 \pmod{100} && / +800 \text{ D.S} \\ 9^{40} &\equiv 801 \pmod{100} && / : 9 \\ 9^{39} &\equiv 89 \pmod{100} \end{aligned}$$

$$9^{99999} = 9^{99960} \cdot 9^{39} \equiv 1 \cdot 89 \pmod{100}.$$

Zadnje dvije znamenke broja 9^{99999} su 89.

3.4.3. A.

$$2^{\varphi(7)} \equiv 1 \pmod 7$$
$$2^6 \equiv 1 \pmod 7$$

No, znamo da je već $2^3 = 8 \equiv 1 \pmod 7$.

$$\begin{aligned} 2^3 &\equiv 1 \pmod 7 && /^{333} \\ 2^{999} &\equiv 1 \pmod 7 && / \cdot 2 \\ 2^{1000} &\equiv 2 \pmod 7 && / \cdot 5 \\ 5 \cdot 2^{1000} &\equiv 10 \pmod 7 && / -7 \text{ D. S.} \\ 5 \cdot 2^{1000} &\equiv 3 \pmod 7 \end{aligned}$$

B.

$$\begin{aligned} 3^{\varphi(7)} &\equiv 1 \pmod 7 \\ 3^6 &\equiv 1 \pmod 7 && /^{166} \\ 3^{996} &\equiv 1 \pmod 7 && / \cdot 3^4 \\ 3^{1000} &\equiv 81 \pmod 7 && / -77 \text{ D. S.} \\ 3^{1000} &\equiv 4 \pmod 7 && / \cdot 4 \\ 4 \cdot 3^{1000} &\equiv 16 \pmod 7 && / -14 \text{ D. S.} \\ 4 \cdot 3^{1000} &\equiv 2 \pmod 7 \end{aligned}$$

C.

$$4^{\varphi(7)} \equiv 1 \pmod 7$$
$$4^6 \equiv 1 \pmod 7$$

No, znamo da je već $4^3 = 64 \equiv 1 \pmod 7$.

$$\begin{aligned} 4^3 &\equiv 1 \pmod 7 && /^{333} \\ 4^{999} &\equiv 1 \pmod 7 && / \cdot 4 \\ 4^{1000} &\equiv 4 \pmod 7 && / \cdot 3 \\ 3 \cdot 4^{1000} &\equiv 12 \pmod 7 && / -7 \text{ D. S.} \\ 3 \cdot 4^{1000} &\equiv 5 \pmod 7 \end{aligned}$$

A. i B. i C.:

$$\begin{aligned} 5 \cdot 2^{1000} + 4 \cdot 3^{1000} + 3 \cdot 4^{1000} &\equiv 3 + 2 + 5 \pmod 7 \\ 5 \cdot 2^{1000} + 4 \cdot 3^{1000} + 3 \cdot 4^{1000} &\equiv 10 \pmod 7 && / -7 \text{ D. S.} \\ 5 \cdot 2^{1000} + 4 \cdot 3^{1000} + 3 \cdot 4^{1000} &\equiv 3 \pmod 7 \end{aligned}$$

Broj $5 \cdot 2^{1000} + 4 \cdot 3^{1000} + 3 \cdot 4^{1000}$ pri dijeljenju sa 7 daje ostatak 3.

3.5. Diofantske jednadžbe

Ciljevi su potpoglavlja 3.5. pokazati najvažnije primjere diofantskih jednadžbi, pokazati kako se rješavaju neke nelinearne diofantske jednadžbe i dati dva načina za rješavanje linearne diofantske jednadžbe s dvjema nepoznanicama.

Nakon ovog potpoglavlja čitatelj bi trebao znati osnove diofantskih jednadžbi i riješiti linearnu diofantsku jednadžbu i neke vrste nelinearnih diofantskih jednadžbi.

Osnovna literatura za potpoglavlje 3.5. jest:

1. K. Burazin, *Nelinearne diofantske jednadžbe*, http://www.mathos.unios.hr/~kburazin/papers/diofantske.pdf (zadnji pristup travanj 2022.)

2. A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

3. A. Dujella, *Uvod u teoriju brojeva* (skripta). PMF – Matematički odjel (str. 75. do 86.)
   Cijela skripta dostupna je na http://e.math.hr/zeta/utblink.pdf (zadnji pristup travanj 2022.)

4. Mladi nadareni matematičari Marin Getaldić, *Diofantske jednadžbe*, https://mnm.hr/wp-content/uploads/2015/10/Diofantske_jednad_be__online_predavanje.pdf (zadnji pristup travanj 2022.)

5. N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, Cambridge, 1998.

6. V. Wagner, *Djeljivost. Diofantske jednadžbe*, https://natjecanja.math.hr/wp-content/uploads/2017/03/N-djeljivost-Vanja.pdf (zadnji pristup travanj 2022.)

Nelinearne diofantske jednadžbe

Diofantska jednadžba je jednadžba kod koje za rješenja tražimo samo cijele brojeve.

Ne postoji algoritam niti čak uputstvo koje bi bilo pomoć u rješavanje nelinearnih diofantskih jednadžbi općenito. Postoji puno ideja koje možemo isprobati za zadanu nelinearnu diofantsku jednadžbu. Ali, koliko god metoda, ideja ili algoritama imali, opet će postojati nelinearna diofantska jednadžba koja se niti jednim od tih algoritama neće moći riješiti. Više o povijesti diofantskih jednadžbi čitatelj može naći u gore navedenoj literaturi.

Primjer 3.5.1. Odredi prirodne brojeve x i y za koje vrijedi

$$x \cdot y - 6x = 13.$$

Rješenje. Na ovoj jednadžbi demonstrirat ćemo metodu rastavljanja na faktore u kojoj se na lijevoj strani jednadžbe treba "namjestiti" umnožak nekih dvaju izraza, a na desnoj neki cijeli broj koji se onda također faktorizira na onoliko faktora koliko ih ima na lijevoj strani.

$$\begin{aligned} xy - 6x &= 13 \\ x(y-6) &= 13 \end{aligned}$$

Desna strana, broj 13, može se rastaviti kao $1 \cdot 13$.

Imamo, dakle, dva slučaja:
A. $x = 1$ i $y - 6 = 13$ i B. $x = 13$, $y - 6 = 1$
Prvo je rješenje $x = 1$, $y = 19$, a drugo $x = 13$, $y = 7$.

Primjer 3.5.2. Riješi diofantsku jednadžbu

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{14}.$$

Rješenje. Na ovoj jednadžbi demonstrirat ćemo metodu dijeljenja u kojoj se jedna od nepoznanica izrazi pomoću svega ostalog u obliku razlomka. Tada, budući da nepoznanica mora biti cijeli broj, i razlomak na desnoj strani mora biti cijeli broj.

$$\begin{aligned} \frac{1}{x} + \frac{1}{y} &= \frac{1}{14} \quad / \cdot 14xy \\ 14x + 14y &= xy \\ 14x &= y(x-14) \quad / : (x-14) \\ y &= \frac{14x}{x-14} \\ y &= \frac{14(x-14)+196}{x-14} \\ y &= 14 + \frac{196}{x-14} \end{aligned}$$

Ovo je sada ključni red cijelog zadatka jer y s lijeve strane mora biti cijeli broj, 14 s desne strane je cijeli broj pa onda i razlomak $\frac{196}{x-14}$ također mora biti cijeli broj. Kako je $196 = 2 \cdot 2 \cdot 7 \cdot 7$, $x - 14$ mora biti neki od sljedećih brojeva: -1, 1, -2, 2, -4, 4, -7, 7,

$-14,\ 14,\ -28,\ 28,\ -49,\ 49,\ -98,\ 98,\ -196,\ 196.$
Rješenja su, dakle:

$$x - 14 = -1,\ y = 14 - 196, \quad \text{tj.} \quad x = 13,\ y = -182,\ \text{itd.}$$

Sva su rješenja dana izrazom

$$\begin{aligned}(x, y) \in \{&(13, -182), (15, 210), (12, -84), (16, 112), (10, -35), (18, 63), (7, -14),\\ &(21, 42), (28, 28), (-182, 13), (210, 15), (-84, 12), (112, 16), (-35, 10), (63, 18),\\ &(-14, 7), (42, 21)\}.\end{aligned}$$

Pitagorine trojke

Primjer 3.5.3. Riješi diofantsku jednadžbu

$$a^2 + b^2 = c^2, \quad a, b, c \in \mathbb{N}.$$

Definicija 3.5.1. *Uređenu trojku (a, b, c) prirodnih brojeva za koje vrijedi*

$$a^2 + b^2 = c^2$$

zovemo **Pitagorina trojka**. *Ako brojevi a, b i c nemaju zajedničkog djelitelja, trojku (a, b, c) tada zovemo* **temeljna Pitagorina trojka**.
Ako je (a, b, c) Pitagorina trojka, onda je i (ka, kb, kc) također Pitagorina trojka za svaki prirodni broj k. Dakle, jasno je da je svaka Pitagorina trojka ili temeljna ili temeljna pomnožena nekim prirodnim brojem.

Jednadžbu $a^2 + b^2 = c^2$, gdje su a, b i c nepoznanice, promatramo kao diofantsku jednadžbu s trima nepoznanicama.

Jednadžba je općenito riješena, tj. rješenja su dana u parametarskom obliku.

Neka su m i n neparni relativno prosti prirodni brojevi i $m > n$. Tada je trojka brojeva (a, b, c) zadana s

$$\begin{aligned} a &= mn,\\ b &= \frac{m^2 - n^2}{2},\\ c &= \frac{m^2 + n^2}{2} \end{aligned}$$

temeljna Pitagorina trojka. Također je temeljna Pitagorina trojka i (b, a, c).

I obrnuto, svaka temeljna Pitagorina trojka može se napisati gornjim izrazima za a, b i c za neke m i n (uz eventualnu zamjenu brojeva a i b ako je zadani a paran).

Pogledajmo neka od manjih rješenja.

Tablica 3.5.1: Početne vrijednosti Pitagorinih trojki za odabrane m i n.

m	3		5		5		7		7	
n	1		1		3		1		3	
a	3	4	5	12	15	8	7	24	21	20
b	4	3	12	5	8	15	24	7	20	21
c	5	5	13	13	17	17	25	25	29	29

Primjer 3.5.4. Napiši program koji će odrediti sve Pitagorine trojke čije su stranice manje od 1000.

Primjer 3.5.5. Napiši računalni program koji će određivati sve one Pitagorine trojke čije su katete susjedni prirodni brojevi.

Veliki Fermatov teorem

Primjer 3.5.6. Neka je n prirodni broj veći od 2. Riješi diofantsku jednadžbu

$$a^n + b^n = c^n, \quad a, b, c \in \mathbb{N}.$$

Fermatov[2] teorem tvrdi da ne postoje prirodni brojevi a, b i c za koje vrijedi

$$a^n + b^n = c^n \qquad \text{ako je } n > 2.$$

1995. godine to je i dokazano.
Za $n = 2$ rješenja je beskonačno i to su Pitagorine trojke.

Bealova hipoteza

Primjer 3.5.7. Riješi diofantsku jednadžbu

$$A^x + B^y = C^z, \qquad A, B, C, x, y, z \in \mathbb{N}, \quad x, y, z \geq 3,$$

A, B i C su relativno prosti.

[2] Pierre Fermat, (1601.– 1665.) – francuski odvjetnik i matematičar

Daniel Andrew "Andy" Beal[3] postavio je 1993. slavnu Bealovu hipotezu kao proširenje Fermatovog velikog teorema u kojoj kaže:

Jednadžba $A^x + B^y = C^z$ nema rješenja ako su eksponenti x, y i z prirodni brojevi svi veći od 3 i ako su A, B i C prirodni brojevi koji su relativno prosti (nemaju zajedničkog djelitelja većeg od 1).

Ako zanemarimo uvjet: A, B i C moraju biti relativno prosti, dobivamo beskonačno puno rješenja.
Npr.

$2^x + 2^x = 2^{x+1}$ za bilo koji prirodni broj x (A, B i C su djeljivi s 2 pa nisu relativno prosti),

$3^3 + 6^3 = 3^5$, (A, B i C su djeljivi s 3 pa nisu relativno prosti),

$7^6 + 7^7 = 98^3$, (A, B i C su djeljivi sa 7 pa nisu relativno prosti),

$162^3 + 27^4 = 9^7$, (A, B i C su djeljivi s 9 pa nisu relativno prosti),

$19^4 + 38^3 = 57^3$, (A, B i C su djeljivi s 19 pa nisu relativno prosti).

Ako zanemarimo uvjet: x, y i z su veći ili jednaki 3, Bealova jednadžba također ima beskonačno puno rješenja.
Npr. $3^2 + 4^2 = 5^2$, $2^3 + 1^5 = 3^2$, $1^1 + 1^1 = 2^1$, ...

Smatramo kako Bealova pretpostavka nije lako dokaziva, kao niti lako oboriva. Prije svega, poopćenje je Fermatova teorema za koji znamo koliko dugo je trebalo matematičarima da ga dokažu kao i koliko duboke matematičke tvrdnje su u tu svrhu morali upotrijebiti. Dalje, računalom se Bealova pretpostavka vrlo jednostavno postavlja pa bi netko i računalom "vjerojatno" već našao takvu šestorku A, B, C, x, y, z kada bi postojala (među računalom dohvatljivim brojevima).

Primjer 3.5.8. Izradi računalni program koji će provjeriti Bealovu hipotezu do određenog velikog broja (npr. 1 000 000). Ispiši trojke (A, B, C) koje zadovoljavaju Bealovu jednadžbu, ali A, B i C nisu relativno prosti brojevi.

Linearna diofantska jednadžba

Definicija 3.5.2. *Linearna diofantska jednadžba je jednadžba oblika*

$$a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_nx_n = b,$$

[3]Daniel Andrew "Andy" Beal, (1952. g. −) - američki bankar, poduzetnik i investitor

gdje su x_1, x_2, ..., x_n nepoznanice, a a_1, a_2, ..., a_n, b su cijeli brojevi. Rješenje zadane jednadžbe je svaka n-torka $(x_1, x_2, \ldots, x_n)$ cijelih brojeva koja zadovoljava zadanu jednadžbu.

Najpoznatija je linearna diofantska jednadžba s dvjema nepoznanicama,

$$ax + by = c.$$

Primjer 3.5.9. Odredi rješenja jednadžbe

$$2x + 3y = 5.$$

Rješenje. Očito je $(1, 1)$ jedno od rješenja zadane diofantske jednadžbe.
Neka su od rješenja i $(-2, 3)$, $(-5, 5)$, $(7, -3)$.
Sva rješenja zadane jednadžbe dana su izrazom $(1 + 3t, 1 - 2t)$, $t \in \mathbb{Z}$.
Pogledajmo prvih nekoliko rješenja za manje t.

Tablica 3.5.2: Tablica početnih vrijednosti rješenja zadane jednadžbe.

t	0	1	-1	2	-2	3	-3	4	-4	5
x	1	4	-2	7	-5	10	-8	13	-11	16
y	1	-1	3	-3	5	-5	7	-7	9	-9

Teorem 3.5.1. *Diofantska jednadžba*

$$a_1x_1 + a_2x_2 + a_3x_3 + \ldots + a_nx_n = b$$

ima rješenje ako i samo ako je b djeljiv s najvećim zajedničkim djeliteljem brojeva a_1, a_2, ..., a_n.

Dokaz ovog teorema je jednostavan i može se naći u većini knjiga gore navedene literature.

Primjer 3.5.10. Riješi jednadžbu

$$3x - 12y = 4.$$

Rješenje. Odmah je očito da kolike god x i y uzeli, lijeva će strana biti djeljiva s 3, a desna ne, pa jednadžba nema rješenja.

Teorem 3.5.2. *Ako je (x_0, y_0) jedno rješenje diofantske jednadžbe $ax + by = c$, onda su sva rješenja dana izrazom*

$$(x, y) = \left(x_0 + \frac{b}{d} \cdot t,\ y_0 - \frac{a}{d} \cdot t\right), \quad t \in \mathbb{Z},$$

gdje je d najveći zajednički djelitelj brojeva a i b.
Rješenje (x_0, y_0) zovemo partikularno rješenje *diofantske jednadžbe $ax + by = c$.*

Dokaz ovog teorema također se može naći u knjigama gore navedene literature.

Uočimo, dakle, da linearna diofantska jednadžba s dvjema nepoznanicama ili nema niti jednog rješenja ili ih ima beskonačno različitih.

Metodu iz teorema 3.5.2. praktično je koristiti ako znamo već jedno rješenje zadane linearne diofantske jednadžbe s dvjema nepoznanicama.

Primjer 3.5.11. Riješi linearnu diofantsku jednadžbu

$$4x - 9y = 2.$$

Rješenje. Bilo bi dobro kada bismo mogli pogoditi bar jedno rješenje zadane jednadžbe. Tada bi nam gornja formula dala sva ostala rješenja. Koji višekratnici od 4 i 9 se razlikuju za 2? To je lako. $2 \cdot 9$ i $4 \cdot 4$ se razlikuju za 2.

$$(x_0, y_0) = (-4, -2), \text{ pa je}$$
$$(x, y) = \left(x_0 + \frac{b}{d} \cdot t,\ y_0 - \frac{a}{d} \cdot t\right) = \left(-4 + \frac{-9}{1} \cdot t,\ -2 - \frac{4}{1} \cdot t\right) = (-4 - 9t, -2 - 4t)$$

Pogledajmo prvih nekoliko rješenja za manje t.

Tablica 3.5.3: Tablica početnih vrijednosti rješenja zadane jednadžbe.

t	0	1	-1	2	-2	3	-3	4	-4
x	-4	-13	5	-22	14	-31	23	-40	32
y	-2	-6	2	-10	6	-14	10	-18	14

Drugi najpoznatiji način rješavanja linearne diofantske jednadžbe s dvjema nepoznanicama je rješavanje Eulerovom metodom. Kod rješavanja tom metodom nije potrebno, kao gore, poznavati neko početno rješenje (x_0, y_0), nego odmah dobijemo konačan parametarski oblik rješenja za x i y.

Primjer 3.5.12. Riješimo Eulerovom metodom diofantsku jednadžbu

$$4x - 9y = 2.$$

Rješenje. Prvo nepoznanicu ispred koje je koeficijent s manjom apsolutnom vrijednošću (manji od brojeva 4 i 9 je 4) izlučimo s lijeve strane.

$$4x - 9y = 2$$
$$x = \frac{2}{4} + \frac{9}{4}y = \frac{1}{2} + \frac{9}{4}y$$

Sada u desnoj strani izlučimo cijeli dio broja kod obaju pribrojnika.

$$x = \frac{1}{2} + \frac{9}{4}y = 0 + \frac{1}{2} + 2y + \frac{1}{4}y.$$

$\frac{9}{4}y$ možemo napisati kao $2y + \frac{1}{4}y$ (to smo i napravili), ali i kao $3y - \frac{3}{4}y$. Bolje je uzeti onaj rastav kod kojega dobiveni razlomak ima manji brojnik (zato smo uzeli rastav s $\frac{1}{4}y$, a ne s $-\frac{3}{4}y$).

Kako x mora biti cijeli broj (rješavamo diofantsku jednadžbu, sjetimo se), tada i $0 + \frac{1}{2} + 2y + \frac{1}{4}y$ mora biti cijeli broj. 0 i 2 već jesu cijeli brojevi pa mora biti i $\frac{1}{2} + \frac{1}{4}y$. Zapišimo to.

$$\frac{1}{2} + \frac{1}{4}y = t$$

Sada množenjem s 4, budući da i y i t moraju biti cijeli brojevi, opet dobivamo diofantsku jednadžbu, ali, budući da smo izlučili cijeli dio iz dobivenih razlomaka, dobivamo jednadžbu s manjim koeficijentima nego na početku. Dosadašnji postupak (izlučiti iz mješovitog broja cijeli dio i kreirati novu diofantsku jednadžbu) ponavljat ćemo sve dok se u dobivenoj diofantskoj jednadžbi ne pojavi koeficijent 1 ili koeficijent -1. Tada ćemo pripadnu nepoznanicu izraziti pomoću ostaloga u jednadžbi i postupak je gotov.

$$\begin{aligned} \frac{1}{2} + \frac{1}{4}y &= t \ \ / \cdot 4 \\ 2 + y &= 4t \\ y &= 4t - 2 \end{aligned}$$

Sada smo izrazili y pomoću t i postupak je gotov. Preostalo je u gornjem izrazu za

$$x = \frac{1}{2} + \frac{9}{4}y$$

umjesto y uvrstiti $4t - 2$.

$$x = \frac{1}{2} + \frac{9}{4}y = \frac{1}{2} + \frac{9}{4} \cdot (4t - 2) = 9t - 4$$

Dakle, $(x, y) = (9t - 4, 4t - 2)$.

Pogledajmo prvih nekoliko rješenja za manje t.

$t = 0$ daje rješenje $(x, y) = (-4, -2)$.

$t = 1$ daje rješenje $(x, y) = (5, 2)$.

$t = -1$ daje rješenje $(x, y) = (-13, -6)$.

I tako dalje.

Primjer 3.5.13. Riješimo Eulerovom metodom diofantsku jednadžbu

$$13x - 9y = 2.$$

Rješenje. Prvo y (jer manji od brojeva 13 i 9 je 9) izlučimo s lijeve strane.

$$\begin{aligned} 13x - 9y &= 2 \\ y &= -\frac{2}{9} + \frac{13}{9}x \end{aligned}$$

Sada u desnoj strani izlučimo cijeli dio broja kod obaju pribrojnika.

$$y = -\frac{2}{9} + \frac{13}{9}x = -\frac{2}{9} + x + \frac{4}{9}x$$

Kako y mora biti cijeli broj, zamijenimo razlomke desne strane s t.

$$\begin{aligned} -\frac{2}{9} + \frac{4}{9}x &= t \ \ / \cdot 9 \\ -2 + 4x &= 9t \\ 4x - 9t &= 2. \end{aligned}$$

Kako nismo dobili diofantsku jednadžbu u kojoj je s lijeve strane bar jedan koeficijent ili 1 ili -1, treba još jednom napraviti korak Eulerovog algoritma.

$$\begin{aligned} 4x - 9t &= 2 \\ 4x &= 9t + 2 \ \ / : 4 \\ x &= \frac{9}{4}t + \frac{2}{4} = 2t + \frac{1}{4}t + \frac{1}{2} \end{aligned}$$

Budući da x mora biti cijeli broj, tada i $\frac{1}{4}t + \frac{1}{2}$ mora biti cijeli broj. Stoga vrijedi:

$$\begin{aligned} \frac{1}{4}t + \frac{1}{2} &= u \ \ / \cdot 4 \\ t + 2 &= 4u \\ t - 4u &= -2 \end{aligned}$$

Dobivena diofantska jednadžba ima koeficijent 1 uz t pa smo gotovi s postupkom, a preostalo je izraziti t pomoću u, pa x i y pomoću u.

$$\begin{aligned} t - 4u &= -2 \\ t &= 4u - 2 \\ x &= \frac{9}{4}t + \frac{2}{4} = \frac{9}{4} \cdot (4u - 2) + \frac{2}{4} = 9u - 4 \\ y &= -\frac{2}{9} + \frac{13}{9}x = -\frac{2}{9} + \frac{13}{9} \cdot (9u - 4) = 13u - 6. \end{aligned}$$

Pogledajmo prvih nekoliko rješenja za manje u.

$u = 0$ daje rješenje $(x, y) = (-4, -6)$.

$u = 1$ daje rješenje $(x, y) = (5, 7)$.

$u = -1$ daje rješenje $(x, y) = (-13, -19)$.

I tako dalje.

ZADACI ZA VJEŽBU

Zadatak 3.5.1. Riješi diofantsku jednadžbu:

$$2x^2 + xy - 3y^2 = 17.$$

Zadatak 3.5.2. Odredi sve dvoznamenkaste brojeve koji su tri puta veći od umnoška svojih znamenki.

Zadatak 3.5.3. Riješi linearnu diofantsku jednadžbu

$$15x + 18y + 6z = 44.$$

Zadatak 3.5.4. Riješi linearnu diofantsku jednadžbu

$$5x + 6y = 44.$$

Zadatak 3.5.5. Eulerovom metodom riješi diofantsku jednadžbu

$$21x - 17y = 15.$$

RJEŠENJA

3.5.1.

$$\begin{aligned} 2x^2 + xy - 3y^2 &= 17 \\ 2x^2 + 3xy - 2xy - 3y^2 &= 17 \\ x(2x + 3y) - y(2x + 3y) &= 17 \\ (2x + 3y)(x - y) &= 17 \end{aligned}$$

Desna strana, broj 17, može se rastaviti kao $1 \cdot 17$.

Imamo, dakle, dva slučaja:

A.
$$\begin{aligned} 2x + 3y &= 1 \\ x - y &= 17 \end{aligned}$$

Uvrstimo li iz druge jednadžbe $x = y + 17$ u prvu jednadžbu, dobivamo rješenja

$$\begin{aligned} x &= 10.4 \\ y &= -6.6 \end{aligned}$$

što nisu cijeli brojevi pa ovo rješenje ne uzimamo u obzir kao konačno rješenje.

B.
$$\begin{aligned} 2x + 3y &= 17 \\ x - y &= 1 \end{aligned}$$

Uvrstimo li iz druge jednadžbe $x = y + 1$ u prvu jednadžbu, dobivamo rješenja

$$\begin{aligned} x &= 4 \\ y &= 3 \end{aligned}$$

3.5.2. Označimo znamenke dvoznamenkastog broja s a i b.
Tada vrijedi

$$\begin{aligned} 10a + b &= 3ab \\ 10a &= 3ab - b \\ 10a &= b(3a - 1) \\ b &= \frac{10a}{3a - 1}. \end{aligned}$$

Kako je a znamenka desetica, prva znamenka dvoznamenkastog broja, a može biti neki od brojeva od 1 do 9. Provjerom svih tih brojeva dobivamo dva rješenja:

$$\begin{aligned} &a = 1,\ b = 5,\ 15 = 3 \cdot 1 \cdot 5 \quad \text{i} \\ &a = 2,\ b = 4,\ 24 = 3 \cdot 2 \cdot 4. \end{aligned}$$

3.5.3. Kako 44 nije djeljiv s nzd(15, 18, 6) = 3, navedena jednadžba nema rješenja. Drugim riječima, lijeva je strana za sve uvrštene x, y i z djeljiva s 3 pa nikada neće iznositi 44.

3.5.4. Bilo bi dobro kada bismo mogli pogoditi bar jedno rješenje zadane jednadžbe. Pitamo se koji višekratnici od 5 i 6 zbrojeni daju 44? To je lako. $5 \cdot 4 + 6 \cdot 4 = 44$.

$$\begin{aligned} &(x_0,\ y_0) = (4,\ 4) \\ &(x,\ y) = \left(x_0 + \frac{b}{d} \cdot t,\ y_0 - \frac{a}{d} \cdot t\right) = \left(4 + \frac{6}{1} \cdot t,\ 4 - \frac{5}{1} \cdot t\right) = (4 + 6t,\ 4 - 5t) \end{aligned}$$

Pogledajmo prvih nekoliko rješenja za manje t.

$t = 0$ daje rješenje $(x,\ y) = (4,\ 4)$.

$t = 1$ daje rješenje $(x,\ y) = (10,\ -1)$.

$t = -1$ daje rješenje $(x,\ y) = (-2,\ 9)$.

I tako dalje.

3.5.5.

$$\begin{aligned} 21x - 17y &= 15 \\ y &= -\frac{15}{17} + \frac{21}{17}x \end{aligned}$$

Sada u desnoj strani izlučimo cijeli dio broja kod obaju pribrojnika.

$$y = -\frac{15}{17} + \frac{21}{17}x = -\frac{15}{17} + x + \frac{4}{17}x$$

Kako y mora biti cijeli broj, zamijenimo razlomke desne strane s t.

$$\begin{aligned} -\frac{15}{17} + \frac{4}{17}x &= t \quad / \cdot 17 \\ -15 + 4x &= 17t \\ 4x - 17t &= 15 \end{aligned}$$

Kako nismo dobili diofantsku jednadžbu u kojoj je s lijeve strane bar jedan koeficijent ili 1 ili -1, treba još jednom napraviti korak Eulerovog algoritma.

$$\begin{aligned} 4x - 17t &= 15 \\ 4x &= 17t + 15 \quad / : 4 \\ x &= \frac{17}{4}t + \frac{15}{4} = 4t + \frac{1}{4}t + 4 - \frac{1}{4} \end{aligned}$$

Budući da x mora biti cijeli broj, tada i $\frac{1}{4}t - \frac{1}{4}$ mora biti cijeli broj. Stoga vrijedi:

$$\begin{aligned} \frac{1}{4}t - \frac{1}{4} &= u \quad / \cdot 4 \\ t - 1 &= 4u \\ t - 4u &= 1 \end{aligned}$$

Dobivena diofantska jednadžba ima koeficijent 1 uz t pa smo gotovi s postupkom, a preostalo je izraziti t pomoću u, pa x i y pomoću t.

$$\begin{aligned} t - 4u &= 1 \\ t &= 4u + 1 \\ x &= \frac{17}{4}t + \frac{15}{4} = \frac{17}{4} \cdot (4u + 1) + \frac{15}{4} = 17u + 8 \\ y &= -\frac{15}{17} + \frac{21}{17}x = -\frac{15}{17} + \frac{21}{17} \cdot (17u + 8) = 21u + 9. \end{aligned}$$

Pogledajmo prvih nekoliko rješenja za manje u.

$u = 0$ daje rješenje $(x, y) = (8, 9)$.

$u = 1$ daje rješenje $(x, y) = (25, 30)$.

$u = -1$ daje rješenje $(x, y) = (-9, -12)$.

4

Logički zadaci kombinatorne i diskretne matematike

Osnovni je zadatak poglavlja 4 ponuditi čitatelju skup odabranih zadataka u kojima će se moći upotrijebiti kombiniranja i logičko razmišljanje prvo u rješavanju navedenog konkretnog problema, a onda i u konstrukciji algoritma za rješavanje cijele te vrste problema računalom. U mnogima od problema (npr. sudoku ili problem rasvjete) važno je i brzo zapažanje, tj. traženje zgodnog mjesta za dalji nastavak kreiranja rješenja, kao i razmišljanje "nekoliko koraka unaprijed" (na primjer kod šaha koji slijedi).

4.1. Primirje na šahovskoj ploči

Literatura za ovo potpoglavlje jest:

1. V. Kovač, I. Madjerčić, *Matematičke igre na šahovskoj ploči*, Matematičko-fizički list, god. 65. (2014./2015.), br. 4./260., 229.–236.
   (Ovaj članak odlično ilustrira sve one igre kod kojih treba razmišljati nekoliko poteza unaprijed i odrediti pobjedničku strategiju, tj. poteze koji nas vode do pobjede u igri.)
2. T. Rudec, *Primirje na šahovskoj ploči*, Matematičko fizički list (1332–1552) 233 (2008), 1; 25–28.
   (Ovaj članak bavi se potpuno istim zadacima kao i cijelo ovo potpoglavlje. Čitatelju predlažemo prvo obraditi cjelinu 4.1., a onda ju utvrditi rješavanjem zadataka iz ovog članka.)
3. K. Vincetić, D. Brajković, M. Pilj, *Matematički zadatci na šahovskoj ploči*, Osječki matematički list 18 (2018), 81–103.
   (Ovaj članak nije vezan direktno uz ovo poglavlje po načinu razmišljanja, ali nudi izvrsne primjere zadataka koji povezuju matematiku i šah.)

Prije obrade navedenih zadataka nastavnika pozivamo da sa studentima svakako ponovi pravila pomicanja figura u šahu. Također, kao zanimljivu vježbu, studentima se može zadati zadatak definicije šaha, tj. kako opisati točno, po mogućnosti u jednoj što jednostavnijoj rečenici, cilj igre šah.

Primjer 4.1.1. Na šahovsku ploču veličine 3×3 postavi tri topa tako da se ne napadaju.

Rješenje. Kako top može napasti samo onu figuru koja je u njegovom redu i stupcu, potrebno je paziti samo na jedno, a to je da ne postavimo neka dva topa u isti red ili isti stupac. Topove označimo slovom T. Postoji šest različitih rješenja:

T		
	T	
		T

Rješenje A

		T
	T	
T		

Rješenje B

T		
		T
	T	

Rješenje C

		T
T		
	T	

Rješenje D

	T	
		T
T		

Rješenje E

	T	
T		
		T

Rješenje F

Slika 4.1.1: Šest različitih rješenja za tri topa na šahovskom polju 3×3.

Prvo i drugo rješenje smatrat ćemo jednim te istim rješenjem jer se drugo dobije rotacijom šahovske ploče za 90 stupnjeva u smjeru kazaljke na satu. Isto vrijedi i za rješenja C, D, E i F – sva su jednaka "do na rotaciju ploče".
Stoga smatramo da postoje točno dva različita rješenja "do na rotaciju ploče", npr. A i C.

Primjer 4.1.2. Na šahovsku ploču 4×4 postavi, da se ne napadaju, 4 kraljice.

Rješenje. Kraljica napada sva polja u svom redu, stupcu i na obje dijagonale. Označimo redove i stupce ploče 4×4 slovima i brojevima. Kraljicu označimo s Q.

	1	2	3	4
A				
B				
C				
D				

Slika 4.1.2: 4×4 prazna šahovska ploča.

Postavimo li prvu kraljicu na polje A1, kao na slici 4.1.3, u drugi red kraljica može ići samo na B3 ili B4 (4 kraljice moraju imati svaka svoj red i svaka svoj stupac, inače će napasti jedna drugu), no ako kraljicu stavimo na B3, ona će napasti i C2 i C4 pa u treći red kraljicu nećemo imati gdje staviti.

Ako u drugi red kraljicu stavimo na B4, u treći red moramo treću postaviti na C2 i onda nemamo gdje postaviti četvrtu kraljicu jer su sva mjesta u redu D napadnuta.

Stoga prva kraljica ne može ići na A1.

	1	2	3	4
A	Q	–	–	–
B	–	–		
C	–		–	
D	–			–

Slika 4.1.3: Polja koja napada kraljica postavljena na A1.

Pokušamo li prvu kraljicu postaviti na A2, dobivamo redom mogućnosti za drugu, treću i četvrtu koja daju sljedeće rješenje:

	1	2	3	4
A		Q		
B				Q
C	Q			
D			Q	

Slika 4.1.4: Rješenje.

Osnom simetrijom dobivamo i rješenje:

	1	2	3	4
A			Q	
B	Q			
C				Q
D		Q		

Slika 4.1.5: Drugo rješenje koje je osna simetrija prvog s obzirom na pravac koji sadrži dužinu između stupca 2 i stupca 3.

Također, kao i kod topova, smatramo da su ova dva rješenja jednaka te ovaj zadatak ima, dakle, samo jedno rješenje.

Primjer 4.1.3. Na šahovsku ploču zadanih dimenzija postavi, da se ne napadaju, zadane figure. Pronađi sva različita rješenja.

a) 3×3, 3 kraljice

b) 3×3, 4 lovca

c) 3×3, 4 kralja

d) 3×3, 5 skakača

e) 4×4, 2 lovca i 6 skakača

f) 4×4, 2 topa, 2 lovca i 2 skakača

g) 4×4, 6 lovaca

h) 4×4, 6 skakača i 2 kralja

i) 5×5, 5 kraljica

j) 5×5, 1 kraljica, 2 topa, 2 lovca i 2 skakača

k) 6×6, 6 kraljica

Rješenje. Čitatelja pozivamo da pokuša pronaći još poneko rješenje različito od ovdje danih.

a) Ne postoji takav smještaj, tj. zadatak a) nema rješenja.

b)

L	L	L
	L	

L	L	
L	L	

Slika 4.1.6: Rješenje za 4 lovca na šahovskom polju 3×3.

c)

K		K
K		K

Slika 4.1.7: Rješenje za 4 kralja na šahovskom polju 3×3.

d)

S		S
	S	
S		S

	S	
S	S	S
	S	

Slika 4.1.8: 2 različita rješenja za 5 skakača na šahovskom polju 3×3.

e)

S			S
L			S
S			L
S			S

S			S
L			L
S			S
S			S

Slika 4.1.9: 2 različita rješenja za 2 lovca i 6 skakača na šahovskom polju 4×4.

f)

	L	S	
			T
T			
	S	L	

	T		
		T	
L			S
S			L

Slika 4.1.10: 2 različita rješenja za 2 topa, 2 lovca i 2 skakača na šahovskom polju 4×4.

g)

L	L	L	L
	L	L	

L	L	L	
L	L	L	

L	L		L
			L
L			
		L	

Slika 4.1.11: 3 različita rješenja za 6 lovaca na šahovskom polju 4×4.

h)

K		S	S
			S
S			
S	S		K

Slika 4.1.12: Rješenje za 6 skakača i 2 kralja na šahovskom polju 4×4.

i) Lakše je nego što se čini jer se samo treba dosjetiti prepisati situaciju s četirima kraljicama na 4×4, a onda dodati i petu u peti stupac i peti red na jedino preostalo mjesto. Ipak, postoji još jedno rješenje koje ovdje ne navodimo (a u kojem niti jedna kraljica nije u kutu).

	Q			
			Q	
Q				
		Q		
				Q

Slika 4.1.13: Rješenje za 5 kraljica na šahovskom polju 5×5.

j) Ovo je vjerojatno najteži od postavljenih zadataka ove vrste. Postoji više rješenja.

Q				
		L	S	
				T
	T			
		S	L	

	Q			
			L	S
T				
		T		
			S	L

		Q		
				T
	T			
S			L	
L			S	

Slika 4.1.14: Tri različita rješenja za 1 kraljicu, 2 topa, 2 lovca i 2 skakača na šahovskom polju 5×5.

k)

			Q		
Q					
				Q	
	Q				
					Q
		Q			

Slika 4.1.15: Rješenje za 6 kraljica na šahovskom polju 6×6.

Zanimljivo je da je ovo jedino rješenje za 6 kraljica na ploči 6×6, dok na ploči 5×5 postoje dva različita smještaja 5 kraljica.

Na ploču veličine $n \times n$, $n > 3$, uvijek je moguće smjestiti n kraljica tako da se ne napadaju, na bar jedan način. (No, teško je naći konkretna rješenja čak i računalom za veće n zbog velikog broja kombinacija koje se moraju uzeti u obzir).

Evo i ostalih brojeva smještaja do $n = 10$.

Tablica 4.1.1: Tablica broja rješenja za smještaj n kraljica na šahovskom polju $n \times n$.

n	1	2	3	4	5	6	7	8	9	10
Broj osnovnih rješenja	1	0	0	1	2	1	6	12	46	92

Zadaci za vježbu

Zadatak 4.1.1. Napravi program na računalu koji će pronaći sva gore tražena rješenja. Za početak, napravi program koji će za svaku vrstu figure i njen smještaj na šahovskoj ploči, ispisati sva polja koja ta figura s danog polja napada.

Svi ovi problemi smještaja figura na šahovsku ploču uglavnom se ne mogu riješiti polinomijalnim algoritmima, nego u slučaju manjih dimenzija ploče, primjenjujemo razne "brute force" algoritme koji jednostavno isprobavaju sve mogućnosti smještaja. To je izvedivo ako je šahovska ploča dimenzija 4×4 ili slično, no za veće šahovske ploče (već za 6×6 ili više) i veći broj figura ne postoje brzi algoritmi, nego treba uzeti u obzir heurističke metode. Pri tome možemo ograničiti broj rješenja (npr. čim program nađe bar jedno rješenje, neka stane s računanjem i problem smatra riješenim) ili se ograničiti samo na neka polja itd. Jedna je od uspješnijih heurističkih ideja je prvo postaviti kraljice, koliko god ih je zadano, a onda (jer će te kraljice zauzeti velik dio polja) u preostala polja smjestiti ostale figure (počevši opet s topovima itd., te za sami kraj ostaviti kraljeve). Globalno, zanimljiv je i težak sljedeći osnovni problem.

Zadatak 4.1.2. Na zadanu šahovsku ploču veličine $n \times n$ postavi q kraljica, t topova, s skakača, l lovaca i k kraljeva tako da niti jedna od zadanih figura ne može uzeti neku od sljedećih u sljedećih m poteza, bez obzira koje figure povlače te poteze.

4.2. Rekurzivne logičke zagonetke

Ove vrste zagonetki lijep su dokaz da se, koliko god računala bila razvijena, neće svi problemi moći riješiti na njima; ovaj puta ne zbog hardverskih nego zbog softverskih zapreka.

Rekurzivne logičke zagonetke su naprimjer "zaokruži A, B ili C" pitanja koje možemo rješavati bez ikakvog konkretnog znanja (ne moramo npr. znati zemljopis ili matematiku itd. kao u uobičajenim pitanjima takvog tipa koje je čitatelj do sada vidio).

Literatura za ovo potpoglavlje jest:

1. T. Rudec, *Zaokruži točan odgovor*, Matka (1330–1047) 17 (2009), 67; 165–169.

U sljedećim testovima samo je jedan od ponuđenih odgovora točan. Zaokruži slovo ispred točnog odgovora.

Primjer 4.2.1. TEST 1.

1. Točan odgovor na ovo pitanje sigurno nije odgovor pod
   a) b   b) b   c) c

2. Točan odgovor na prvo pitanje je odgovor pod
   a) b   b) c   c) a

Rješenje. Odgovor na prvo pitanje sigurno nije b) b jer ako zaokružimo b, tvrdimo da točan odgovor nije pod b (a zaokružili smo ga). Iz istog razloga, odgovor na prvo pitanje sigurno nije c) c. Kako je u svakom pitanju točno jedan odgovor točan, i odgovor na prvo pitanje sigurno nije b) niti c), mora biti a).
Sada, kada znamo da je odgovor na prvo pitanje a), jasno je da je odgovor na drugo pitanje c) a.

Primjer 4.2.2. TEST 2.

1. Ukupan broj točnih odgovora pod b) ovog testa je
   a) paran broj   b) neparan broj   c) nula

2. Točni odgovori na ovo i na prethodno pitanje su uz
   a) jednako slovo   b) različito slovo

3. Savršeni rješavač koji čitajući test odmah i rješava pitanje koje čita i sva prethodno pročitana pitanja, do ovog trenutka već je zaokružio točne odgovore na
   a) nula pitanja   b) paran broj pitanja   c) neparan broj pitanja

4. Dan u tjednu u kojem je ovaj test prvi puta uveden u ovu knjigu je
   a) srijeda   b) četvrtak   c) petak.

Rješenje. Test možemo rješavati na sljedeći način:

Prvo: Odgovor na prvo pitanje sigurno nije c) nula jer 1. c) bi značio da je ukupan broj odgovora pod b) nula, a to bi značilo da je odgovor na drugo pitanje sigurno a) (jer ne smije biti niti jednog odgovora pod b)). No, to bi, zbog 2. a), značilo da su točni odgovori na pitanja 1. i 2. uz isto slovo. No, c i a nisu isto slovo.

Dalje, točan odgovor na prvo pitanje nije niti b) neparan broj jer da je b) neparan broj točan odgovor, onda odgovor na drugo pitanje ne smije biti a) jednako slovo jer a) i b) nisu jednaki. No, odgovor na drugo pitanje u slučaju 1. b) ne smije biti niti b) različito slovo jer su b) i b) jednaki.

Jasno je da mora onda odgovor na prvo pitanje biti 1. a). To je sigurno.
Nakon toga odgovor na drugo pitanje može biti i a) jednako slovo i b) različito slovo.

Dakle, savršeni rješavač do čitanja trećeg pitanja riješit će točno jedno pitanje. Stoga je odgovor na treće pitanje c) neparan broj pitanja.
Sada je sigurno 1. a) i 3. c). U prvom smo pitanju izjavili da je ukupan broj točnih odgovora pod b) ovog testa: a) paran broj. Kako je najmanji paran broj 2, slijedi da točni odgovori na 2. pitanje i na 4. pitanje moraju biti pod b).
Konačno je rješenje 1. a), 2. b), 3. c), 4. b).

Zadaci za vježbu

Zadatak 4.2.1. TEST 3.

1. Ukupan broj točnih odgovora pod a) ovog testa je
   a) 1 b) 2 c) 3

2. Točan odgovor na prethodno pitanje je pod
   a) c b) a c) b

Zadatak 4.2.2. TEST 4.

1. Broj točnih odgovora pod a) plus broj točnih odgovora pod b) ovog testa je
   a) 4 b) 3 c) 2

2. Broj točnih odgovora pod a) plus broj točnih odgovora pod c) ovog testa je
   a) 1 b) 2 c) 3

3. I bez pročitanog 4. pitanja znamo kako odgovor na drugo pitanje nije odgovor pod
   a) b b) c c) a

4. Točan odgovor na drugo pitanje je odgovor pod
   a) a b) b c) c

Zadatak 4.2.3. TEST 5.

1. Točan odgovor na 2. pitanje je odgovor pod
   a) a b) b c) c

2. Točan odgovor na 3. pitanje je odgovor pod
   a) a b) c c) b

3. Točan odgovor na 4. pitanje je odgovor pod
   a) b b) a c) c

4. U ovom je testu najviše točnih odgovora pod
   a) c b) b c) a

Zadatak 4.2.4. TEST 6.

1. Zbroj svih rješenja koja se nalaze uz točne odgovore pod 1) je
   1) 2 2) 1 3) 4

2. Zbroj svih rješenja koja se nalaze uz točne odgovore pod 2) je
   1) 3 2) 2 3) 1

3. Zbroj brojeva odgovora čije je rješenje broj 2 je
   1) 0 2) 2 3) 3

Zadatak 4.2.5. TEST 7.

1. Točan odgovor na treće pitanje je odgovor pod
   a) c b) a c) b

2. Točan odgovor na prvo pitanje je odgovor pod
   a) ni a ni b b) ni a ni c c) ni b ni c

3. Točan odgovor na drugo pitanje je odgovor pod
   a) b b) c c) a

RJEŠENJA

4.2.1. Konačno rješenje je 1. a) (jer ukupan broj točnih odgovora pod a) ne može biti 3 kad imamo samo dva pitanja, a ni 2 jer smo tada već zaokružili jedan b) , 2. b).

4.2.2. Ukupno imamo devet mogućnosti za rješenja prvog i drugog pitanja:

1. a), 2. a) – ovo znači da je jedan odgovor pod a), tri pod b) i nula je odgovora c). No, to je nemoguće jer smo već zaokružili dva odgovora a).

1. a), 2. b) – ovo znači da imamo dva odgovora pod a), dva pod b) i nula je odgovora c).

1. a), 2. c) – ovo znači da imamo tri odgovora pod a), jedan pod b) i nula je odgovora c). No, to je nemoguće jer smo već zaokružili jedan odgovor c).

1. b), 2. a) – ovo znači da imamo nula odgovora pod a), tri pod b) i jedan je odgovor c). No, to je nemoguće jer smo već zaokružili odgovor a) drugom pitanju.

1. b), 2. b) – ovo znači da imamo jedan odgovor pod a), dva pod b) i jedan odgovor c).

1. b), 2. c) – ovo znači da imamo dva odgovora pod a), jedan pod b) i jedan pod c).

1. c), 2. a) – ovo nije moguće jer ukupno imamo četiri pitanja.

1. c), 2. b) – ovo znači da imamo nula odgovora pod a), dva pod b) i dva odgovora c).

1. c), 2. c) – ovo znači da imamo jedan odgovor pod a), jedan odgovor pod b) i dva odgovora pod c).

Znači, moguće su kombinacije:

1. a), 2. b)

1. b), 2. b)

1. b), 2. c)

1. c), 2. b)

1. c), 2. c)

Svakako, dakle, odgovor na drugo pitanje nije a), a to onda znači da je odgovor na 3. pitanje c). (To smo mogli zaključiti i na druge načine.)
Budući da imamo jedan točan odgovor c), ne dolazi u obzir kombinacija 1. a), 2. b).
Kako su odgovori na pitanja 2. i 4. jednaki, rješenje je jedno od sljedećih:

1. b), 2. b), 3. c), 4. b)

1. b), 2. c), 3. c), 4. c)

1. c), 2. b), 3. c), 4. b)

1. c), 2. c), 3. c), 4. c).

Zbog tekstova 1. i 2. zadatka jedino moguće rješenje je 1. c), 2. b), 3. c), 4. b).

4.2.3. Iz pretpostavke 1. a) odmah slijedi 2. a), 3. a) i 4. b), a 4. b) kaže da je u testu najviše točnih odgovora b), što nije točno ako smo tri puta odabrali a).
Istom argumentacijom iz pretpostavke 1. b) dobivamo nemoguću situaciju, tj. kao konačno rješenje dobivamo 1. c), 2 c), 3. b), 4. a).

4.2.4. 1. pitanje: 3) sigurno nije točno jer zbroj rješenja uz 1) sigurno nije 4 kad su moguća rješenja uz 1) brojevi 2, 3 i 0, a kombinacijom tih triju brojeva ne možemo nikako dobiti 4. Iz istog razloga točan odgovor na prvo pitanje ne može biti 2) 1.
Dakle, mora biti 1) 2.
Kako odgovor na 1. pitanje mora biti 1) 2, odgovor na drugo pitanje ne može biti 1) 3 jer u trećem pitanju piše 2) 2.
Također, odgovor na drugo pitanje ne može biti 3) 1.
Slijedi da odgovor na 2. pitanje mora biti 2) 2.
Iz odgovora na prva dva pitanja odmah slijedi da je odgovor na 3. pitanje 3) 3.
Ukupno, rješenje testa je
1. 1), 2. 2), 3. 3)

4.2.5. Počnimo od prvog pitanja.

Ako je točan odgovor a) c, slijedi da je točan odgovor na treće pitanje odgovor pod c) a, što znači da je odgovor na drugo pitanje odgovor pod a) ni a ni b, što znači da točan odgovor na prvo pitanje nije ni a ni b, a to nije točno ako smo pretpostavili da je točan odgovor na prvo pitanje a).

Analogno, točan odgovor na prvo pitanje nije ni c) b.

Dakle, konačno rješenje je dakle 1. b), 2. b), 3. a).

4.3. Rasvjeta

Logička zagonetka rasvjeta (engleski *Light up* – osvijetli, japanski *Bijutsukan* – umjetnička galerija) ponegdje se zove i Akari. Jedna je od mnogobrojnih novih zagonetki u kojima treba nešto upisati u prazne kvadratiće i također je jedan od "proizvoda" za čiju je popularizaciju zaslužna japanska izdavačka kuća Nikoli.

Literatura za ovo potpoglavlje jest:

1. B. McPhail, *Light Up is NP–complete*, http://mountainvistasoft.com/docs/lightup-is-np-complete.pdf (zadnji

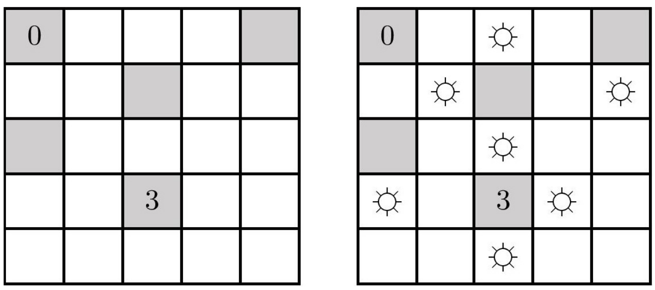
pristup travanj 2022.)
(U članku autor je prvo dokazao da je problem zagonetke rasvjete NP–težak, a zatim i da je NP–potpun. Ovo je važan podatak koji nam govori da se niti uz pomoć računala neće lako, u nekom razumnom vremenu, riješiti veći i teži primjerci ove zagonetke.)

2. https://www.brainbashers.com/lightuphelp.asp (zadnji pristup travanj 2022.)
(Ova je stranica zanimljiva po tome što čitatelja uči poučavanju rješavanju zagonetki rasvjeta. Premda je na engleskom jeziku zbog jednostavnosti je dobar izbor za učenje strategije rješavanja. No, još je važnija kao neprestani izvor novih zagonetki rasvjeta (Daily Light–Up) s odabirom težine.)

3. https://en.wikipedia.org/wiki/Light_Up_(puzzle) (zadnji pristup travanj 2022.)
(Ovo je Wikipedijina stranica s najvažnijim podacima o ovoj zagonetki.)

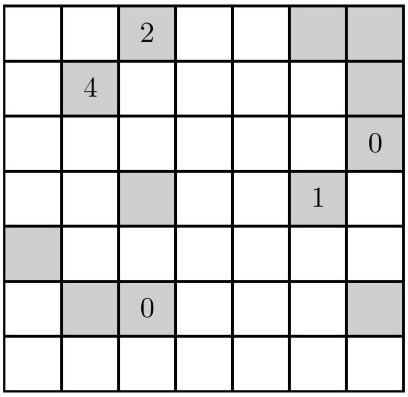
Pravila: U neka polja pravokutne, najčešće kvadratne mreže koja predstavlja hodnike zgrade s pogledom iz ptičje perspektive, treba upisati žarulje. Svaka će žarulja osvijetliti red i stupac u kojem se nalazi, do prepreke, tj. zida. Ne smije se dogoditi da dvije žarulje svijetle jedna u drugu. Na kraju, zagonetka je riješena kada su sva bijela polja zadane križaljke osvijetljena bar jednom žaruljom. Broj u crnom polju govori nam koliko se oko tog polja nalazi žarulja (na poljima lijevo, desno, gore i dolje, tj. broj se ne odnosi na dijagonalna polja). Žarulje upisujemo u bijela polja dok crna polja označavaju zid.

Primjer 4.3.1. Na slici 4.3.1 dana je logička zagonetka rasvjeta i njeno rješenje. Sva su polja križaljke osvijetljena, ne postoje dvije žarulje koje bi svijetlile jedna u drugu, a oko polja s brojevima zaista se nalazi onoliko žarulja koliki je broj koji je upisan u polju.



Slika 4.3.1: Zadana logička zagonetka rasvjeta i njeno rješenje.

Primjer 4.3.2. Riješi zadanu zagonetku rasvjeta.

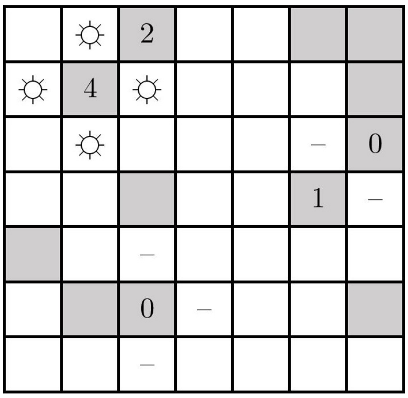


Slika 4.3.2: Zadana logička zagonetka rasvjeta.

Rješenje.

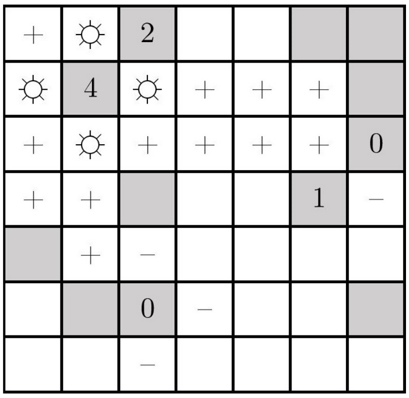
1. Na gornjoj slici oko dva polja s brojem nula sigurno ne idu žarulje pa u ta polja, kako bismo si pomogli u rješavanju, upišimo znak minus (−).

2. Oko polja s brojem 4 upišimo žarulje.



Slika 4.3.3: Prvi i drugi korak u rješavanju zadane logičke zagonetke rasvjeta.

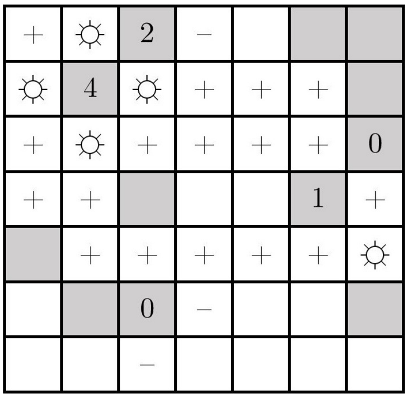
3. Sva obasjana polja označimo znakom plus (+). Znak plus u nekom polju označit će nam da je to polje osvijetljeno i da u to polje ne smijemo postaviti žarulju kako ne bi dvije žarulje svijetlile jedna u drugu.



Slika 4.3.4: Treći korak u rješavanju zadane logičke zagonetke rasvjeta.

4. U dva od tri polja oko polja s brojem 2 dolaze dvije žarulje. Dvije smo već upisali, pa u treće polje sigurno ne dolazi žarulja. Označimo ga znakom minus (−).

5. U polje desno od polja u kojem je zadan broj 1 ne smije doći žarulja. No, i to polje na kraju mora biti osvijetljeno pa ispod toga (jedino iz tog polja možemo polje s minusom osvijetliti) postavljamo žarulju te s plus označimo sva polja koja ona obasja.

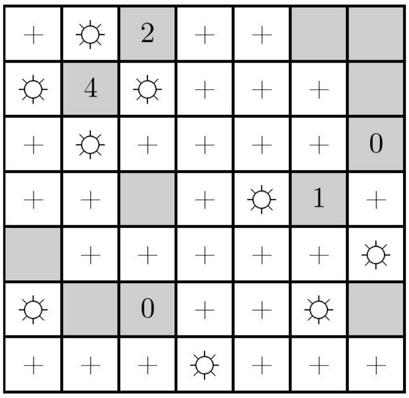


Slika 4.3.5: Četvrti i peti korak u rješavanju zadane logičke zagonetke rasvjeta.

6. Kako oko polja s brojem 1 mora doći žarulja, stavljamo ju lijevo od tog polja, na jedino moguće mjesto. Odmah polja koja ona obasjava označavamo znakom plus.

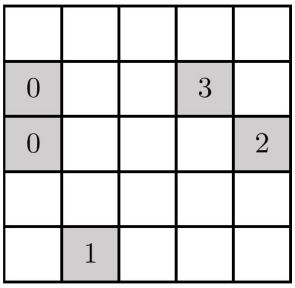
7. Polje desno od polja s brojem 2 i dalje sadrži minus (−). Jedino polje s kojega ga možemo obasjati najniže je polje tog stupca pa tu postavljamo žarulju i odmah znakom plus označavamo sva polja koja ta žarulja obasjava.

8. Preostala su dva prazna polja u koja jednostavno postavimo žarulje te dobivamo konačno rješenje.



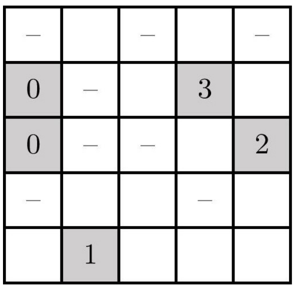
Slika 4.3.6: Konačno rješenje zadane logičke zagonetke rasvjeta.

Primjer 4.3.3. Riješi zadanu zagonetku rasvjeta.



Slika 4.3.7: Zadana logička zagonetka rasvjeta.

Rješenje. Premda je manja od prethodne, ova je zagonetka nešto teža od nje.
Prvo oko dva polja s brojem nula postavimo minuse ($-$) koji će nam značiti da u ta polja sigurno ne upisujemo žarulju. Drugo, u polja koja su dijagonalna, s obzirom na polje s brojem 3, ne smije doći žarulja. Ta bi žarulja obasjala dva polja oko polja s brojem 3 i onda ne bismo mogli postaviti žarulje u ta dva polja, a onda ne bismo mogli postaviti niti tri žarulje oko toga polja. Stoga polja koja dijagonalno dodiruju polje s brojem 3, također označavamo znakom minus. Isto vrijedi za polje s brojem 2.



Slika 4.3.8: Prvi korak u rješavanju zadane logičke zagonetke rasvjeta.

Polje desno od broja 3 mora osvijetliti neka od žarulja. To polje može osvijetliti ili žarulja koja bi bila u krajnjem gornjem desnom kutu križaljke ili u polju ispod njega. U krajnjem gornjem desnom kutu već je minus. Dakle, mora ići desno od broja 3 kako bi se osvijetlilo to mjesto.

Dalje, polje lijevo od polja s brojem 1 mora osvijetliti neka od žarulja. Kako je iznad tog polja minus, u polje lijevo od polja s brojem 1, moramo upisati žarulju. Odmah u ostala polja oko polja s brojem 1 postavljamo znak minus. Polja koja su obasjana označimo znakom plus (+).

−		−		+
0	−		3	☼
0	−	−		2
+	−		−	
☼	1	−		

Slika 4.3.9: Drugi korak u rješavanju zadane logičke zagonetke rasvjeta.

Sljedeći potez nešto je teže uočiti. Ispod polja s upisanim brojem 3 mora ići žarulja. Ako u to polje ne ide žarulja, onda mora ići u polja lijevo, desno i iznad polja s upisanim brojem 3 te ispod polja s upisanim brojem 2, kao na slici dolje. Sada na toj slici označimo znakom + (plus) sva osvijetljena polja. Vidimo kako drugo polje u trećem redu nije osvjetljeno (u njemu je minus) i kako ne postoji mjesto u zagonetki u koje bismo mogli upisati žarulju koja bi ga obasjala.

+	+	+	☼	+
0	+	☼	3	☼
0	−	+		2
+	+	+	+	☼
☼	1	+		

Slika 4.3.10: Pogrešna pretpostavka o položaju žarulja oko polja s brojem 3.

Stoga u polje ispod polja s brojem 3, moramo upisati žarulju. Označimo odmah i sva polja koja su osvijetljena do sada postavljenim žaruljama znakom +. Sada u polje ispod polja s brojem 2 sigurno ne ide žarulja jer smo već upisali dvije oko tog polja.

−		−		+
0	−		3	☼
0	+	+	☼	2
+	−		+	−
☼	1	−	+	

Slika 4.3.11: Treći korak u rješavanju zadane logičke zagonetke rasvjeta.

Na kraju, ako postavimo oko polja s brojem 3 treću, zadnju neupisanu žarulju, iznad tog polja, onda će biti nemoguće obasjati drugo polje u drugom redu (odmah desno od polja s upisanom nulom). Stoga iznad polja s brojem 3 ne ide žarulja, nego lijevo od broja 3. Sada na kraju samo još postavimo dvije žarulje koje će obasjati neosvijetljena polja.

+	☼	+	+	+
0	+	☼	3	☼
0	+	+	☼	2
+	+	+	+	+
☼	1	+	+	☼

Slika 4.3.12: Konačno rješenje zadane logičke zagonetke rasvjeta.

ZADACI ZA VJEŽBU

Zadatak 4.3.1. Napravi računalni program za pomoć u rješavanju logičke zagonetke rasvjeta. Egzaktni brzi, odnosno polinomijalni algoritam ne možemo očekivati jer je dokazano kako je problem zagonetke rasvjeta NP–težak. Umjesto toga možemo kreirati program koji se temelji na nekim jednostavnijim i brzim konkretnim idejama (nije teško kreirati heuristički algoritam s nekoliko brzih i jednostavnih ideja za koji se često ispostavi da će riješiti većinu zagonetki Rasvjeta koje su na gore navedenim internetskim stranicama okarakterizirane težinom "lako" ("easy") ili "srednje" ("medium")). Takav program neće možda riješiti cijelu zagonetku, ali će nam dati početnu pomoć u rješavanju.

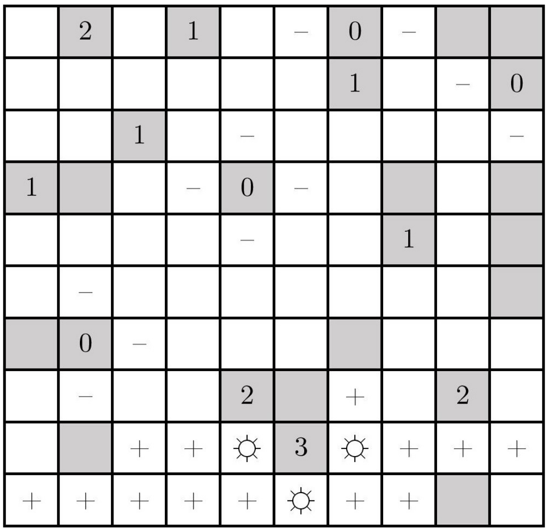
Zadatak 4.3.2. Riješi zagonetku rasvjeta:

	2		1			0			
						1			0
		1							
1				0					
							1		
	0								
				2				2	
					3				

Slika 4.3.13: Zadana logička zagonetka rasvjeta.

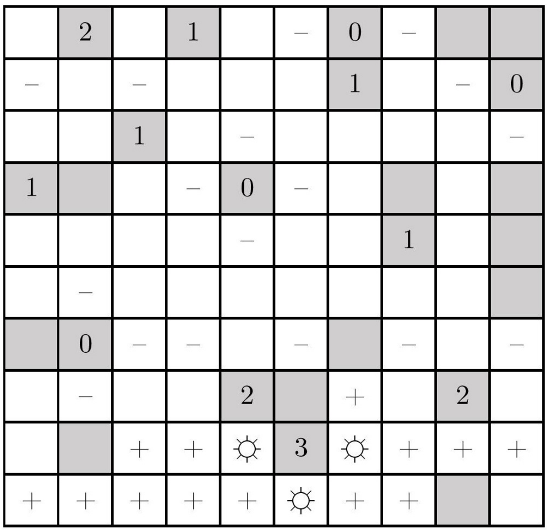
Rješenja

4.3.2. Prvo oko svih polja s brojem nula postavimo minuse. Oko polja s brojem 3 na jedina moguća mjesta postavimo žarulje i s plus označimo polja koja one osvjetljavaju.



Slika 4.3.14: Prvi korak u rješavanju zadane logičke zagonetke rasvjeta.

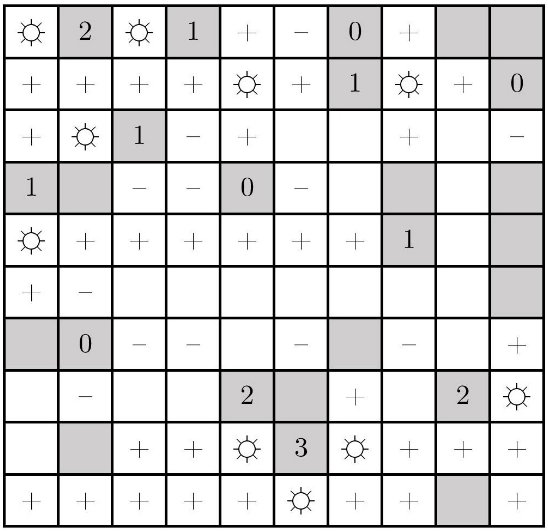
U prazna polja dijagonalno od polja s brojem 2 upišemo minuse (u polja u kojima ne smije biti žarulja jer u tom slučaju ne bismo mogli oko broja 2 upisati dvije žarulje.)



Slika 4.3.15: Drugi korak u rješavanju zadane logičke zagonetke rasvjeta.

Desno od gornjeg lijevog broja 2 polje mora biti obasjano pa na to mjesto mora doći žarulja. Od sada nakon svake upisane žarulje odmah upisujemo i znak plus u sva mjesta koja ona obasjava. Oko polja s brojem 1 u gornjem redu sada upisujemo znak minus jer je jedina žarulja oko tog mjesta već upisana.

Desno od polja s brojem jedan u gornjem redu polje mora biti obasjano. Upisujemo žarulju u polje ispod, dijagonalno dolje lijevo od spomenutog polja s brojem jedan. Sada znamo gdje oko polja s brojem 2 u gornjem redu mora doći druga žarulja. Ispod polja s brojem 1 u lijevom stupcu tablice sada postavljamo žarulju. Dalje rješavanje ove zagonetke ostavljamo čitatelju. (Mala pomoć: sljedeća polja koja se lako riješe su oko polja s upisanim brojem 1 u drugom redu, a onda se vidi da oko polja s brojem dva u predzadnjem stupcu žarulje nisu istovremeno gore i lijevo jer u tom slučaju jedinicu iznad ne možemo riješiti itd.)



Slika 4.3.16: Treći korak u rješavanju zadane logičke zagonetke rasvjeta.

U slučaju težeg primjerka zagonetke, u ovoj se zagonetki kao i u ostalim sličnim zagonetkama (u programiranju, ali i u ručnom rješavanju) koristi takozvani "backtracking" algoritam u kojemu se, kada više ne znamo koji znak treba sljedeći upisati u križaljku, upisuje npr. žarulja na prvo moguće mjesto te se dalje zagonetka rješava kao da je to bio ispravan izbor, a ako se u daljem rješavanju pokaže da je uz tu pretpostavku križaljku nemoguće riješiti, brišemo sve upise koje smo unijeli u križaljku nakon pretpostavljene žarulje, brišemo i tu žarulju te na to mjesto upisujemo minus koji nam znači da u tom polju sigurno nije žarulja.

4.4. Neboderi

Neboderi (engl. *Skyscrapers*), ili tornjevi (engl. *Towers*) su novija logička igra. Zanimljivo je da lakše verzije problema mogu rješavati i učenici nižih razreda osnovne škole, dok teže (ili vrlo teške) mogu biti nerješive i uz pomoć računala.

Literatura za ovo potpoglavlje jest:

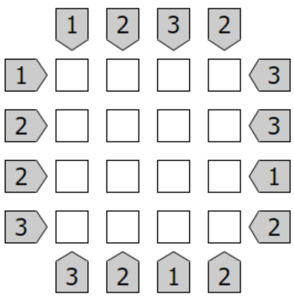
1. M. Maarse, *The NP–completeness of some lesser known logic puzzles*, Bachelor Kunstmatige Intelligentie Utrecht University June 28, 2019.
   https://studenttheses.uu.nl/bitstream/handle/20.500.12932/33867/Scriptie_Mieke_Maarse_5750032.pdf (zadnji pristup travanj 2022.)
   (Ova internetska stranica sadrži dokaz da je zagonetka neboderi NP teška.)

2. Daily Skyscrapers,
   https://www.brainbashers.com/skyscrapers.asp (zadnji pristup travanj 2022.)
   (Ova internetska stranica sadrži veliki broj logičkih zagonetki neboderi različitih veličina i težina.)

3. Skyscrapers techniques,
   https://www.conceptispuzzles.com/index.aspx?uri=puzzle/skyscrapers/techniques (zadnji pristup travanj 2022.)
   (Ova stranica sadrži video zapis s jednostavnim uputstvima kako riješiti logičku zagonetku neboderi.)

4. Skyscrapers tutorial,
   https://www.conceptispuzzles.com/index.aspx?uri=puzzle/skyscrapers/tutorial (zadnji pristup travanj 2022.)
   (Ova stranica sadrži uputstva kako riješiti logičku zagonetku neboderi.)

Pravila su jednostavna: zadana je kvadratna mreža veličine $n \times n$ (najčešće 4×4 ili 5×5) kao na slici 4.4.1.



Slika 4.4.1: Primjer zadane logičke zagonetke neboderi.

Zadatak je u prazne kvadratiće upisati brojeve od 1 do 4 (ili od 1 do n u zagonetki veličine $n \times n$) tako da u svakom redu i u svakom stupcu (kao kod zagonetke sudoku) budu prisutni svi brojevi od 1 do 4 (do n općenito). Dalje, raspored nam olakšavaju brojevi pored reda ili stupca koji nam govore koliko se, ako upisani brojevi predstavljaju veličine nebodera u katovima, s te točke vidi nebodera. Ako je prvi do promatrača npr. najviši neboder, vidjet ćemo samo njega jer se od njega ne vide oni manji (u potpunosti ih zaklanja i na tom će mjestu pisati broj 1). Broj 4 značit će da od tog mjesta treba upisati 1 2 3 4 jer slučajni prolaznik vidi sva četiri nebodera. Broj 3 može u ovom primjeru značiti da je raspored 1 2 4 3 (vidimo najmanji neboder koji je odmah do nas, zatim neboder veličine 2 te neboder veličine 4, a neboder veličine 3 zaklonjen je neboderom veličine 4 pa se on ne vidi), ili 1 3 4 2 ili 1 3 2 4 ili 2 3 4 1 ili 2 1 3 4 ili 2 3 1 4 (ukupno je, dakle, u taj red moguće upisati 6 mogućih kombinacija, a koju ćemo upisati, naravno, ne znamo, nego moramo razmisliti kojeg od brojeva gdje upisati obzirom na druge podatke (npr. broj sa suprotne strane križaljke ili već u tom redu upisane brojeve i slično). Na kraju dobivamo popunjenu križaljku kao na slici.

	1	2	3	2	
1	4	3	1	2	3
2	2	4	3	1	3
2	3	1	2	4	1
3	1	2	4	3	2
	3	2	1	2	

Slika 4.4.2: Rješenje zadane logičke zagonetke neboderi sa slike 4.4.1.

Primjer 4.4.1. Riješi zadanu logičku zagonetku neboderi.

	3	1	2	2	
2					3
2					1
2					2
1					4
	1	2	2	3	

Slika 4.4.3: Zadana logička zagonetka neboderi.

Rješenje. Prvo uočavamo na jednom mjestu broj 4. To nam je najvrjedniji podatak jer u taj red možemo upisati sve brojeve. Iz te točke, vide se, dakle, sva četiri nebodera, pa u taj red upisujemo 1 2 3 4, počevši od točke s brojem 4.

	3	1	2	2	
2					3
2					1
2					2
1	4	3	2	1	4
	1	2	2	3	

Slika 4.4.4: Prvi korak u rješavanju zadane logičke zagonetke neboderi.

Dalje, gdje god se nalazi broj 1 upisujemo neboder veličine 4 (samo on se vidi, ostali se ne vide od njega jer je najviši).

	3	1	2	2	
2		4			3
2				4	1
2					2
1	4	3	2	1	4
	1	2	2	3	

Slika 4.4.5: Drugi korak u rješavanju zadane logičke zagonetke neboderi.

Kao što smo i rekli, na kraju upisani brojevi moraju biti takvi da se i u svakom redu i u svakom stupcu nalazi svaki od brojeva 1, 2, 3 i 4. Kako su na gornjoj slici upisana tri broja 4, uočavamo da četvrta nedostaje u trećem redu i istovremeno u trećem stupcu pa na presjeku trećeg reda i trećeg stupca upisujemo broj 4.

	3	1	2	2	
2		4			3
2				4	1
2			4		2
1	4	3	2	1	4
	1	2	2	3	

Slika 4.4.6: Treći korak u rješavanju zadane logičke zagonetke neboderi.

U ovom trenutku rješavanja možemo upotrijebiti različite argumente za upis sljedećeg broja. Pogledajmo npr. zadani broj 3 gore desno. Iz te točke (u prvom redu tablice) vidimo tri nebodera. Kako je broj 4 u taj red već upisan, gledajući od zadanog broja 3, prema broju 4 možemo upisati (jer moraju se vidjeti 3 nebodera) ili 1 2 ili 1 3 ili 2 3.

No, u četvrtom je stupcu već upisan broj 1, pa ne smijemo početi s 1 jer bi onda u tom stupcu imali dva upisana broja 1. Dakle, upisujemo 2 3 4 1.

	3	1	2	2	
2	1	4	3	2	3
2				4	1
2			4		2
1	4	3	2	1	4
	1	2	2	3	

Slika 4.4.7: Četvrti korak u rješavanju zadane logičke zagonetke neboderi.

Sada je lako riješiti zadnja dva stupca jer samo jedan broj nedostaje. No, lako je riješiti prije toga i prvi stupac jer zadani broj 3 govori nam da iz te točke vidimo tri nebodera pa moramo upisati 1 3 2 4 (1 2 3 4 bi bilo kada bi vidjeli 4 nebodera). Konačno je rješenje

	3	1	2	2	
2	1	4	3	2	3
2	3	2	1	4	1
2	2	1	4	3	2
1	4	3	2	1	4
	1	2	2	3	

Slika 4.4.8: Konačno rješenje zadane logičke zagonetke neboderi.

Primjer 4.4.2. Riješi zadanu logičku zagonetku neboderi.

	3				
					3
					2
2					1
		3			

Slika 4.4.9: Zadana logička zagonetka neboderi.

Rješenje. Ovdje je zadano manje podataka nego u prethodnoj zagonetki neboderi, stoga je jasno da se radi o nešto težem zadatku.

Prvo uz zadani broj 1 upisujemo neboder visine 4. Kako je s druge strane istog reda zadan broj 2, tj. iz te točke gledajući vidimo točno dva nebodera, svakako ćemo vidjeti neboder visine 4 koji je na kraju reda. I neboder visine 3 koji mora iz točke gledišta doći na red za zapis prije njega svakako ćemo vidjeti. I to su onda ukupno dva nebodera pa taj red mora početi brojem 3.

Nad prvim stupcem zadan je broj 3. Kako će neboder visine 4, kako ga god zapisali u prvi stupac, zakriliti neboder visine 3 kojeg smo upravo upisali, očito ćemo iz te točke gledišta vidjeti nebodere visine 1, 2 i 4, stoga te nebodere moramo u prvi stupac upisati upravo tim redom.

	3				
	1				
	2				3
	4				2
2	3			4	1
		3			

Slika 4.4.10: Prvi korak u rješavanju zadane logičke zagonetke neboderi.

Desno od trećeg reda zadan je broj 2. No, neboder visine 4 koji je upisan u taj red sigurno ćemo vidjeti jer je najviši, a ako želimo vidjeti točno još jedan neboder, treći red gledano s desne strane mora početi brojem 3.

Desno od drugog reda zadan je broj 3. Dakle, iz te točke vidjet ćemo tri nebodera. Neboder visine dva koji je već upisan na početku tog reda sigurno neće biti među onima koje ćemo vidjeti jer će ga zakloniti neboderi visina 3 i 4. Zato moramo vidjeti sva tri preostala nebodera, pa u drugi red, počevši od desne strane moramo upisati redom 1, 3, 4.
Preostali broj 4 mora ići u presjek prvog reda i trećeg stupca.
Preostali broj 3 mora ići u presjek prvog reda i drugog stupca.
Dopunimo prvi red brojem 2 koji nedostaje.
Zbog zadanog broja 3 ispod drugog stupca, u drugi stupac gledano odozdo moramo upisati 1, 2.

Sada samo popunimo zadnje preostalo prazno polje u trećem i četvrtom redu i dobivamo konačno rješenje.

	3				
	1	3	4	2	
	2	4	3	1	3
	4	2	1	3	2
2	3	1	2	4	1
		3			

Slika 4.4.11: Konačno rješenje zadane logičke zagonetke neboderi.

Primjer 4.4.3. Riješi zadanu logičku zagonetku neboderi.

	3	2	2	2		
3						
						2
			1			2
3					3	2
			2			

Slika 4.4.12: Zadana logička zagonetka neboderi.

Rješenje. U ovu zagonetku upisujemo brojeve od 1 do 5.

U gornjem se redu broj 5 ne može nalaziti u prva četiri mjesta tog reda (zbog zadanih brojeva 3, 2, 2, i 2). Stoga broj 5 upisujemo u zadnje mjesto u tom redu.

Treći stupac ne može (gledajući odozgo) započeti brojevima 1 i 5 jer su oni već upisani u tom stupcu i redu. Treći stupac ne može počinjati brojem 2 jer nakon broja 2 mora, zbog zadanog broja 2, biti postavljen broj 5, a ispod broja 1 broj 3, što nije moguće jer bismo u četvrtom redu imali dva broja 3. Treći stupac ne može započinjati niti brojem 3. Zbog zadanog broja 3 na početku prvog reda, lijevo od upisanog broja 3, tada bismo morali upisati broj 4. Sada su mogućnosti za treći stupac ili 3 2 1 5 4, što je nemoguće jer zbog broja 5 na četvrtom mjestu morali bismo lijevo od njega upisati broj 4, što nije moguće zbog broja 4 u istom tom stupcu u prvom redu, ili 3 5 1 2 4, što je opet nemoguće jer morali bismo lijevo od broja 2 upisati broj 4, što nije moguće zbog broja 4 u istom tom stupcu u prvom redu. Treći stupac počinje, dakle, brojem 4.

U četvrtom redu broj 4 ne može biti na početku zbog zadanog broja 3 s lijeve strane. 4 ne može biti ni na sredini jer u tom je stupcu već upisan broj 4. Ne može biti niti na četvrtom mjestu jer onda bismo, gledajući s desne strane, vidjeli tri broja (3, 4 i 5), a zadan je broj 2 s desne strane. U četvrtom redu broj 4 sigurno se nalazi na drugom mjestu.

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

Slika 4.4.13: Prvi korak u rješavanju zadane logičke zagonetke neboderi.

Pogledajmo gdje u petom redu sada može stajati broj 5. Na zadnjem mjestu ne može jer je u tom stupcu već upisan. Na trećem mjestu ne može jer je ispod tog polja zadan broj 2. Na drugom mjestu ne može jer bi se odozgo vidjela minimalno tri broja, a zadan je broj 2. Na četvrtom mjestu ne može jer bi taj stupac odozgor gledajući morao početi onda brojem 4, a to nije moguće jer broj 4 je već upisan u prvom redu. Broj 5 mora, dakle, biti upisan na prvom mjestu. Upišimo tu peticu i nakon toga, na kraju reda ili stupca ispišimo što se sve može naći u zadanom retku i stupcu s obzirom na već upisane brojeve.

	3	2	2	2			
3			4		5		21435, 31425, 32415
						2	42351, 43251, 41352, 43512, 12354, 13254, 21354, 31254, 23514, 32514, 13524, 31524, 12534, 21534, 35214, 25314, 15234, 15324
			1			2	43152, 23154, 32154, 35124, 25134
3		4			3	2	14523, 14253, 24513,
	5						
			2				
	14325, 24315, 34215, 31425, 32415	15243, 15342, 25341, 21543, 35241, 31542, 32541,	42153, 43152, 45123	15324, 15423, 25314, 25413, 35214, 35412, 35421, 31524, 32514, 31254			

Slika 4.4.14: Drugi korak u rješavanju zadane logičke zagonetke neboderi.

Sada kombiniramo upisane brojeve.

Prvi red počinje s 2 ili s 3. Stoga i prvi stupac mora početi ili s 2 ili s 3, pa na kraju prvog stupca brišemo mogućnost 14325.

Drugi broj u prvom redu mora biti ili 1 ili 2. To znači da prvi broj u drugom stupcu mora biti ili 1 ili 2. Stoga brišemo kombinacije 35241, 31542 i 32541 na kraju drugog stupca. I tako dalje. Preostale su mogućnosti:

	3	2	2	2			
3			4		5		21435, 32415
						2	41352, 21354, 25314
			1			2	43152, 23154, 32154, 35124, 25134
3		4			3	2	14523
	5						
			2				
	24315, 34215, 32415	15243, 15342, 25341, 21543	43152	15324, 15423, 35421, 31524, 31254			

Slika 4.4.15: Treći korak u rješavanju zadane logičke zagonetke neboderi.

Sada možemo riješiti četvrti red i treći stupac jer su sve mogućnosti osim jedne izbrisane.

	3	2	2	2			
3			4		5		21435, 32415
			3			2	41352, 21354, 25314
			1			2	43152, 23154, 32154, 25134
3	1	4	5	2	3	2	14523
	5		2				
			2				
	24315, 34215, 32415	15243, 15342, 25341, 21543	43152	15324, 31524			

Slika 4.4.16: Četvrti korak u rješavanju zadane logičke zagonetke neboderi.

Sada u zadnjem stupcu broj 1 mora doći na zadnje mjesto. Kada to upišemo, u zadnjem će redu nedostajati brojevi 3 i 4. Zbog broja četiri u predzadnjem redu, jedini mogući raspored brojeva u zadnjem redu jest 53241. Na kraju, ako u prvi red postavimo kombinaciju 21435, onda u prvi stupac mora ići 24315, a u drugi 15243. To bi značilo da drugi red počinje s 4 5, što je nemoguće. Prvi je red, dakle, (jer samo su dvije mogućnosti) 32415. U četvrtom stupcu sada nedostaju 3 i 5 pa je četvrti stupac (zbog broja 3 u trećem stupcu) 15324. Sada se na isti način riješi i drugi stupac. Treći red sada moramo riješiti korištenjem pomoćnih kombinacija. Jedina je moguća kombinacija 25134. Preostale brojeve lako upišemo jer su jedini preostali u svojim stupcima.
Konačno je rješenje:

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

Slika 4.4.17: Konačno rješenje zadane logičke zagonetke neboderi.

Zadaci za vježbu

Zadatak 4.4.1. Napravi računalni program za pomoć u rješavanju logičke zagonetke neboderi.
Nije teško napraviti egzaktan, točan algoritam kojeg možemo koristiti za manje primjerke problema. Za veće primjerke problema korisnije je kreirati pametan brzi heuristički algoritam koji će pomoći na početku rješavanja.

4.5. Mostovi

Logička zagonetka mostovi (engleski *Bridges*, japanski *Hashi* ili *Hashiwokakero*) za razliku od gore navedenih zagonetki nije "tipa sudoku", tj. ne sastoji se od kvadratne ili pravokutne križaljke u koju se nešto upisuje. Premda, želimo li napraviti program na računalu koji će nam pomoći u rješavanju ove zagonetke, upravo pomoću kvadrata ili pravokutnika moramo zagonetku zapisati i rješavati. Kao i ostale zagonetke, i ova može biti vrlo jednostavna kao što može biti i nerješiva čak i uz pomoć računala (u nekom "normalnom" vremenu jer računalo uvijek može isprobati sve mogućnosti, što može trajati djelić sekunde kao i nekoliko stoljeća, ovisno o veličini i težini zadane zagonetke.)

Literatura za ovo potpoglavlje jest:

1. D. Andersson, *Hashiwokakero is NP–complete*, Information Processing Letters Volume 109, Issue 19, 15 September 2009, Pages 1145–1146.
   (Ovdje je dokazano da je logička zagonetka mostovi također NP–teška.)

2. Hashi techniques,
   https://www.conceptispuzzles.com/index.aspx?uri=puzzle/hashi/techniques (zadnji pristup travanj 2022.)
   (Na ovoj stranici nalaze se upute za rješavanje logičke zagonetke mostovi.)

3. Hashiwokakero,
   https://en.wikipedia.org/wiki/Hashiwokakero (zadnji pristup travanj 2022.)
   (Ovo je Wikipedijina stranica s osnovnim podacima o igri.)

4. Mostovi,
   https://hr.puzzle-bridges.com/ (zadnji pristup travanj 2022.)
   (Ovo je stranica na hrvatskom jeziku koja sadrži velik broj različitih zagonetki mostovi s odabirom veličine i težine zagonetke.)

Pravila rješavanja: Zadane krugove s upisanim brojevima koji predstavljaju otoke u moru treba spojiti mostovima tako da:

1. se mostovi nigdje ne sijeku,

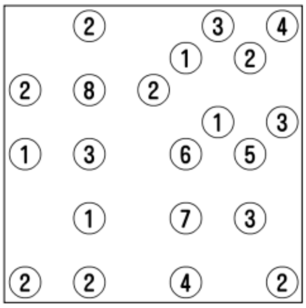
2. se mostovi povlače samo vodoravno i okomito,

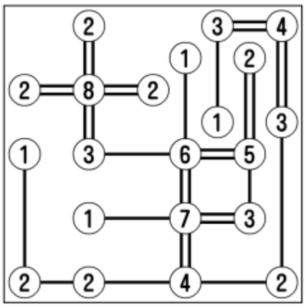
3. na kraju svi otoci budu povezani (s bilo kojeg od otoka možemo mostovima stići do bilo kojeg drugog otoka),

4. svaka dva susjedna otoka mogu biti međusobno povezana jednostrukom ili dvostrukom vezom (dvostruka se broji kao dva mosta),

5. broj na otoku govori s koliko je mostova taj otok spojen s okolnim otocima.

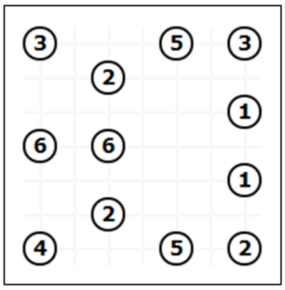
Primjer 4.5.1.





Slika 4.5.1: Zadana i riješena zagonetka mostovi.

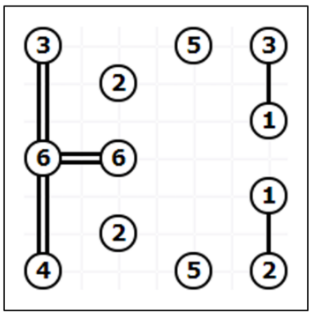
Primjer 4.5.2. Riješi logičku zagonetku mostovi.



Slika 4.5.2: Zadana logička zagonetka mostovi.

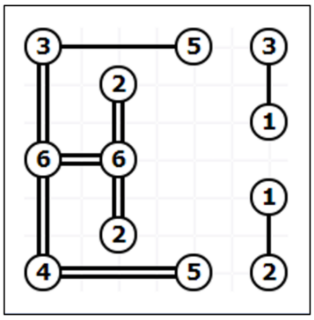
Rješenje. Prvo, spojimo li otoke koji na sebi imaju broj 1 mostom, više ih ne smijemo dalje spajati jer broj 1 znači da iz njih smije izlaziti samo jedan most. Tada bi oni bili odvojeni od ostalih otoka što nije dozvoljeno. Stoga te otoke ne smijemo međusobno povezati jednim mostom nego moramo iz njih povući mostove prema drugim susjednim otocima.

Lijevo na slici nalazi se otok s brojem 6. Kako iz svakog otoka moramo povući onoliko mostova koliko nam broj u njemu govori, a taj otok ima samo tri susjeda, moramo povući dvostruke mostove gore, dolje i desno.



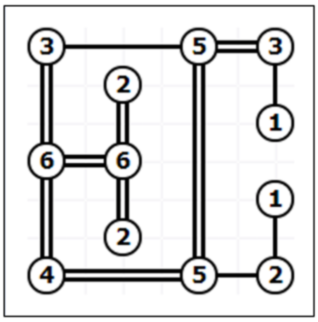
Slika 4.5.3: Prvi korak u rješavanju zadane logičke zagonetke mostovi.

Također, i za drugi otok na kojemu je broj 6 vrijedi da ga možemo spojiti samo s tri susjeda pa i iz njega povucimo još dvije dvostruke veze kako bi ukupno šest mostova iz njega izlazilo. Sada gornji lijevi otok na kojemu je broj 3 spojimo još jednim preostalim mostom s njemu desnim otokom, a donji lijevi otok na kojemu je broj 4 s njemu desnim otokom.



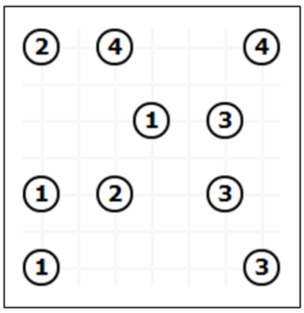
Slika 4.5.4: Drugi korak u rješavanju zadane logičke zagonetke mostovi.

Sada otok s brojem 3 gore desno moramo dvostrukom vezom spojiti s gornjim otokom na kojemu je broj 5, a otok s brojem 2 dolje desno s donjim otokom koji sadrži broj 5. Na kraju spojimo s dvama mostovima i ta dva otoka na kojima su petice i zadatak je gotov.



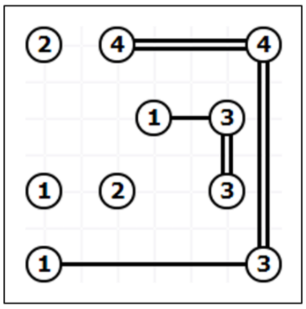
Slika 4.5.5: Konačno rješenje zadane logičke zagonetke mostovi.

Primjer 4.5.3. Riješi logičku zagonetku mostovi.



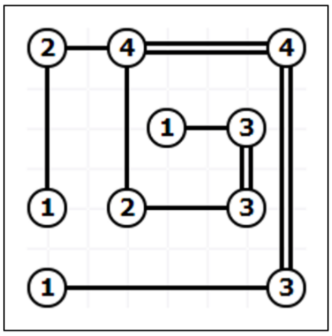
Slika 4.5.6: Zadana logička zagonetka mostovi.

Rješenje. Gore desno nalazi se otok s brojem 4 s kojega možemo povući mostove prema samo dva otoka. Povucimo, dakle, dvije dvostruke veze prema tim dvama otocima. Dolje desno nalazi se otok s brojem 3 s kojega također možemo povući mostove prema samo dva otoka. Povucimo veze prema tim dvama otocima. S otoka s brojem 1 koji je u sredini slike možemo most povući samo prema otoku s brojem 3 desno od njega. Sada s tog otoka s brojem 3 možemo preostale dvije veze povući samo prema dolje.



Slika 4.5.7: Prvi korak u rješavanju zadane logičke zagonetke mostovi.

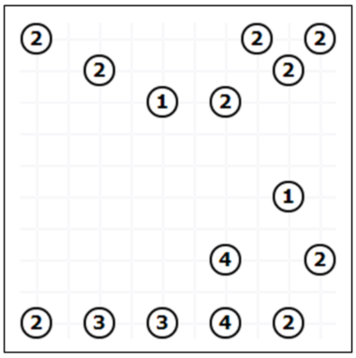
Nastavljamo gdje smo stali i s otoka s brojem 3 povlačimo posljednji most prema broju 2 lijevo. Iz tog srednjeg otoka s brojem 2 ne smijemo dalje povući most lijevo prema broju 1 jer bi srednji dio otočja tada bio izoliran od ostalih otoka (jer nema više načina da ih povezujemo dalje jer su svi brojevi na otocima zasićeni). Stoga iz otoka s brojem 2 moramo drugi most povući prema gore prema otoku s brojem 4, a iz tog otoka preostali most povlačimo lijevo, zatim jedan dolje i gotovi smo.



Slika 4.5.8: Konačno rješenje zadane logičke zagonetke mostovi.

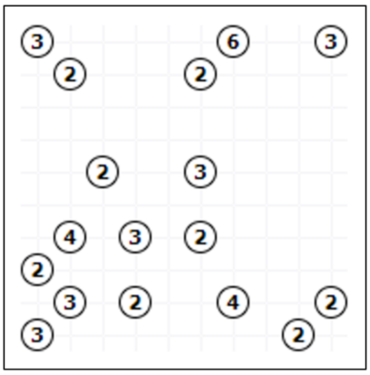
ZADACI ZA VJEŽBU

Zadatak 4.5.1. Riješi logičku zagonetku mostovi.



Slika 4.5.9: Zadana logička zagonetka mostovi.

Zadatak 4.5.2. Riješi logičku zagonetku mostovi.



Slika 4.5.10: Zadana logička zagonetka mostovi.

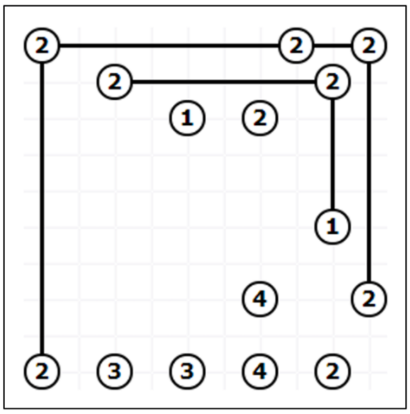
Zadatak 4.5.3. Izradi računalni program koji rješava zagonetku mostovi.

RJEŠENJA

4.5.1. Ova je zagonetka znatno teža od ostalih.

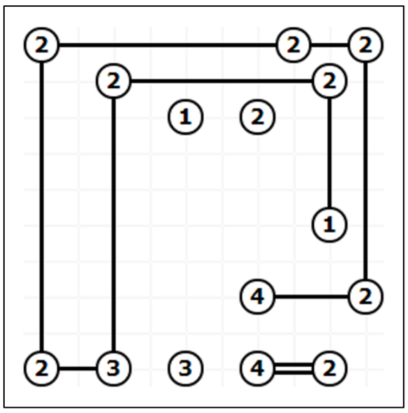
Na tri se vrha otočja nalazi broj 2. Niti jedan od tih otoka ne smijemo spajati dvostrukom vezom s bilo kojim od preostalih susjednih otoka na kojima je broj 2 jer bismo dobili dva izolirana otoka s kojih više ne možemo ostvariti vezu s nekim od preostalih otoka. Stoga sve te veze moraju biti jednostruke.

Sada u drugom redu otoka imamo dva otoka s brojem 2. Desni od tih otoka također ne smijemo spajati dvostrukom vezom s lijevim susjedom jer bismo opet dobili dva od ostalih otoka izolirana otoka. Stoga moramo i tu povući dva jednostruka mosta.



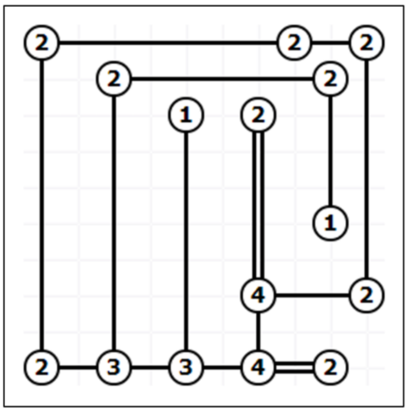
Slika 4.5.11: Prvi korak u rješavanju zadane logičke zagonetke mostovi.

Pogledajmo lijevi od tih dvaju otoka u drugom redu na kojima je broj 2. Iz njega preostali most ne možemo nacrtati prema desnom otoku, što znači da ga moramo nacrtati prema dolje. Također, iz donjeg lijevog otoka s brojem 2 most ne smijemo više povući prema gore pa moramo prema desnom otoku na kojemu je broj 3. Srednji otok u zadnjem stupcu otoka na kojemu je broj 2 možemo samo još spojiti s otokom koji mu je s lijeve strane. Na kraju, zadnji otok dolje desno koji na sebi ima broj 2 možemo spojiti samo s otokom koji je lijevo od njega i to dvostrukom vezom jer je na njemu broj 2.



Slika 4.5.12: Drugi korak u rješavanju zadane logičke zagonetke mostovi.

Drugi otok u zadnjem redu možemo spojiti još samo s otokom desno od njega. Iz otoka u predzadnjem redu koji na sebi ima broj 4 ne smijemo povući prema dolje dvostruku vezu jer bi onda iz otoka u zadnjem redu s brojem 3 morali povući dvije veze prema gore, što je nemoguće jer je gore otok s brojem 1. Stoga iz otoka s brojem 4 u predzadnjem redu treba povući jedan most prema dolje i dva prema gore. Preostalo je iz otoka s brojem 3 u zadnjem redu povući jedan most prema gore i jedan prema desno i zagonetka je riješena.

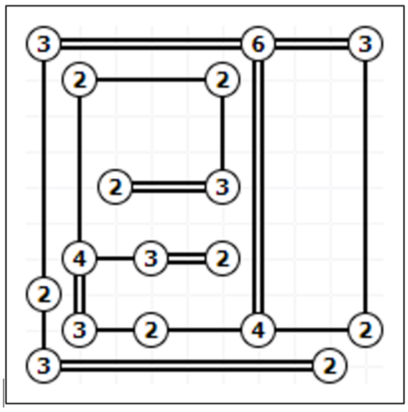


Slika 4.5.13: Konačno rješenje zadane logičke zagonetke mostovi.

4.5.2. Predlažemo čitatelju svakako da prvo pokuša samostalno riješiti ovu nešto težu zagonetku, a onda, ako to ne uspije, predlažemo sljedeći redoslijed poteza:

1. Povlačimo šest mostova iz otoka s brojem 6 u gornjem redu.
2. Zatim povlačimo prema dolje po jedan most iz dvaju otoka s brojem 3 u gornjem redu.
3. Iz otoka s brojem 2 u zadnjem redu povlačimo dvostruki most prema otoku lijevo od njega.
4. Iz otoka s brojem 3 u zadnjem redu povlačimo most prema otoku iznad njega.
5. Iz otoka s brojem 2 u zadnjem stupcu povlačimo most prema otoku lijevo od njega.
6. Iz otoka s brojem 4 u predzadnjem redu povlačimo most prema otoku lijevo od njega.
7. Povlačimo prema dolje po jedan most iz dvaju otoka s brojem 2 u drugom redu.
8. Dvostrukom vezom povezujemo otoke s brojevima 2 i 3 u trećem redu.
9. Spajamo otoke s brojem 2 u drugom redu.
10. Dvostrukom vezom povezujemo otoke s brojevima 2 i 3 u četvrtom redu.
11. Iz otoka s brojem 3 u predzadnjem redu povlačimo most prema otoku s brojem 2 koji se nalazi desno od njega i dvostruki most prema otoku s brojem 4 koji

je iznad njega.
Dalje je lako, a konačno rješenje dano je na slici dolje.



Slika 4.5.14: Konačno rješenje zadane logičke zagonetke mostovi.

4.6. Kakuro

Kakuro (japanski *Kasan Kurosu* - raskrižja zbrojeva, engleski *Cross Sums*) ponegdje se zove i matematička križaljka. Kakuro je u Japanu bio najpopularnija logička zagonetka–križaljka do 1992. godine kada ga je po popularnosti prestigao jednostavniji sudoku. Kakuro se u matematici može rješavati metodama cjelobrojnog programiranja. Za kakuro nema brzog i jednostavnog algoritma nego je kao i većina prethodnih zagonetki NP–težak.

Literatura za ovo potpoglavlje je

1. KakuroConquests,
   https://www.kakuroconquest.com/ (zadnji pristup travanj 2022.)
   (Stranica sadrži veliku količinu različitih vrsta kakuro križaljki razvrstanih po veličini i po težini.)

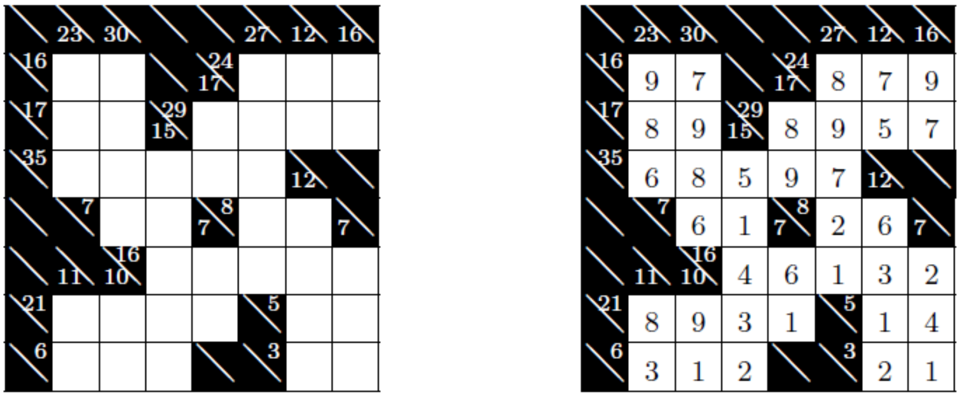
2. S. Sruk, *Kakuro, igra ili složeni problem u teoriji kompleksnosti.*
   https://mis.element.hr/fajli/491/39-10.pdf (zadnji pristup travanj 2022.)
   (Na ovoj stranici nalaze se upute za rješavanje logičke zagonetke kakuro kao i pregled osnovnih tehnika te na kraju i složenijih ideja koje bi mogle pomoći u rješavanju.)

3. S. Takahiro, *The Complexities of puzzles, cross sum and their Another Solution Problems (ASP)*, Submitted to the Department of Information Science the Faculty of Science, the University of Tokyo on February 5, 2002 in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science.

http://www-imai.is.s.u-tokyo.ac.jp/~seta/paper/senior_thesis/seniorthesis.pdf
(zadnji pristup travanj 2022.)
(Na ovoj stranici nalazi se dokaz da je logička zagonetka kakuro NP–teška.)

Upute za rješavanje: U zadanoj križaljci u svako je prazno polje potrebno upisati neki od brojeva od 1 do 9. Brojevi koje smo upisali kod nekog od zadanih brojeva moraju biti svi međusobno različiti, a u zbroju moraju dati zadani broj.

Primjer 4.6.1. Na slici 4.6.1 nalaze se zadani prazni kakuro i desno od njega pripadno rješenje. Lijevo gore zadan je broj 16. Na desnoj slici s rješenjem desno od broja 16 upisani su 9 i 7 koji su različiti i u zbroju daju 16. U gornjem redu zadan je broj 30. Na slici desno ispod broja 30 upisani su redom 7, 9, 8 i 6 koji su međusobno različiti i u zbroju daju $7 + 9 + 8 + 6 = 30$.



Slika 4.6.1: Zadani i riješeni primjer logičke zagonetke kakuro.

U rješavanju logičke zagonetke kakuro od velike nam je pomoći sljedeći popis zbrojeva. Brojevi navedeni u sljedećem popisu samo se na jedan način mogu zapisati kao zbroj različitih pribrojnika (većih ili jednakih 1 i manjih ili jednakih 9).

3 u 2 polja: $1 + 2$ (Ako je zadan broj 3, u polja ispod njega ili desno od njega, možemo upisati samo 2 pa 1 ili 1 pa 2 i nema drugih mogućnosti).

4 u 2 polja: $1 + 3$

16 u 2 polja: $7 + 9$

17 u 2 polja: $8 + 9$

6 u 3 polja: $1 + 2 + 3$

7 u 3 polja: $1 + 2 + 4$

23 u 3 polja: $6 + 8 + 9$

24 u 3 polja: $7 + 8 + 9$

10 u 4 polja: $1 + 2 + 3 + 4$

11 u 4 polja: $1 + 2 + 3 + 5$

29 u 4 polja: $5 + 7 + 8 + 9$

30 u 4 polja: $6 + 7 + 8 + 9$

15 u 5 polja: $1 + 2 + 3 + 4 + 5$

16 u 5 polja: $1 + 2 + 3 + 4 + 6$

34 u 5 polja: $4 + 6 + 7 + 8 + 9$

35 u 5 polja: $5 + 6 + 7 + 8 + 9$

21 u 6 polja: $1 + 2 + 3 + 4 + 5 + 6$

22 u 6 polja: $1 + 2 + 3 + 4 + 5 + 7$

38 u 6 polja: $3 + 5 + 6 + 7 + 8 + 9$

39 u 6 polja: $4 + 5 + 6 + 7 + 8 + 9$

28 u 7 polja: $1 + 2 + 3 + 4 + 5 + 6 + 7$

29 u 7 polja: $1 + 2 + 3 + 4 + 5 + 6 + 8$

41 u 7 polja: $2 + 4 + 5 + 6 + 7 + 8 + 9$

42 u 7 polja: $3 + 4 + 5 + 6 + 7 + 8 + 9$

36 u 8 polja: $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8$

37 u 8 polja: $1 + 2 + 3 + 4 + 5 + 6 + 7 + 9$

38 u 8 polja: $1 + 2 + 3 + 4 + 5 + 6 + 8 + 9$

39 u 8 polja: $1 + 2 + 3 + 4 + 5 + 7 + 8 + 9$

40 u 8 polja: $1 + 2 + 3 + 4 + 6 + 7 + 8 + 9$

41 u 8 polja: $1 + 2 + 3 + 5 + 6 + 7 + 8 + 9$

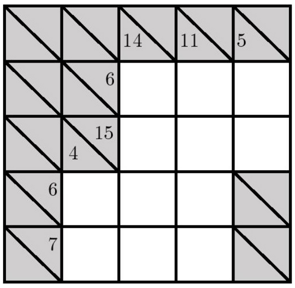
42 u 8 polja: $1 + 2 + 4 + 5 + 6 + 7 + 8 + 9$

43 u 8 polja: $1 + 3 + 4 + 5 + 6 + 7 + 8 + 9$

44 u 8 polja: $2 + 3 + 4 + 5 + 6 + 7 + 8 + 9$

45 u 9 polja: $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9$

Primjer 4.6.2. Riješi logičku zagonetku kakuro:

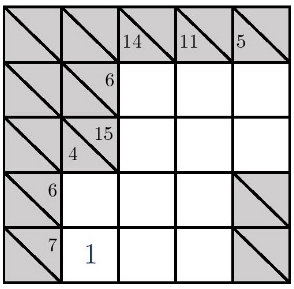


Slika 4.6.2: Zadana logička zagonetka kakuro.

Rješenje. U prvi red moramo upisati brojeve koji u zbroju daju broj 6. Broj 6 može se dobiti pomoću triju različitih prirodnih pribrojnika samo pomoću brojeva 1, 2 i 3 (6 u tri polja naveden je u tablici iznad). No, ta tri broja možemo upisati u prvi red na točno $3! = 6$ načina, tj. možemo upisati redom ili 1, 2, 3 ili 1, 3, 2 ili 2, 1, 3 ili 2, 3, 1 ili 3, 1, 2 ili 3, 2, 1. Dakle, tu ne znamo što treba upisati.

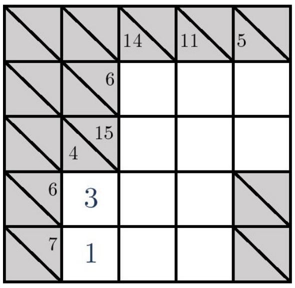
Potrebno je nakon ovog neuspjelog pokušaja sada dalje pretraživati križaljku i naći mjesto koje se, s obzirom na zadane brojeve, može realizirati na samo jedan način.

U donjem redu zadan je broj 7. Po gornjoj tablici (7 u 3 polja), broj 7 može se zapisati kao zbroj triju prirodnih brojeva jedino pomoću brojeva 1, 2 i 4. No, prvi upisani broj ne može biti 2 jer bi zadani broj 4 iznad tog broja 2 mogli zapisati onda samo kao $2 + 2$, što nije dozvoljeno jer upisani pribrojnici moraju biti različiti. Prvi upisani broj ne može biti niti 4 jer bi zadani broj 4 iznad tog broja 2 mogli zapisati onda samo kao $0 + 4$, što nije dozvoljeno jer upisani pribrojnici moraju biti veći od nule. Jedino u obzir onda dolazi za to polje broj 1.



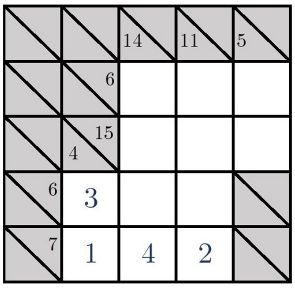
Slika 4.6.3: Prvi korak u rješavanju zadane logičke zagonetke kakuro.

Iznad upisanog broja 1 zadan je broj 4 pa onda iznad 1 upisujemo 3.



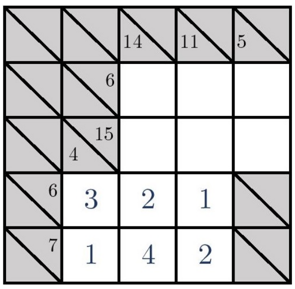
Slika 4.6.4: Drugi korak u rješavanju zadane logičke zagonetke kakuro.

Sada treba gledati malo pažljivije. U gornjem dijelu križaljke zadan je broj 11. On se mora ostvariti kao zbroj četiriju brojeva, a to možemo ostvariti na samo jedan način.
11 u 4 polja : $1 + 2 + 3 + 5$. U zadnje polje tog stupca određenog zbrojem 11 ne smijemo upisati broj 1 jer je on već upisan u tom redu. Ne smijemo upisati niti 3, a niti 5 jer njih nema u zapisu broja 7 koji je zadan s lijeve strane tog praznog polja. Jedino je moguće upisati u to polje broj 2. Budući da je lijevo zadan broj 7, upisat ćemo desno od sedmice 1, 4, 2.



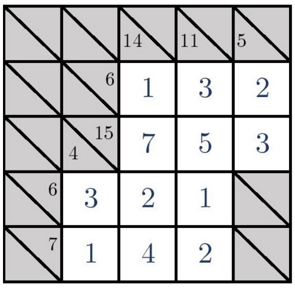
Slika 4.6.5: Treći korak u rješavanju zadane logičke zagonetke kakuro.

Sada broj 6 koji je zadan iznad upravo riješenog broja 7 možemo realizirati samo pomoću kombinacije $3 + 2 + 1$.



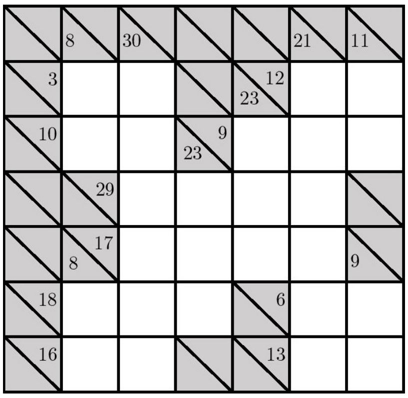
Slika 4.6.6: Četvrti korak u rješavanju zadane logičke zagonetke kakuro.

U prvom je redu zadan broj 6. Pribrojnici su sigurno 1, 2 i 3. No, pribrojnik kojeg ćemo upisati na drugo mjesto ne smije biti niti 1 niti 2 jer oni su već upisani u taj stupac. Moramo upisati broj 3. Prvi pribrojnik za tu šesticu onda mora također zbog brojeva ispod i desno biti 1, a onda je lako riješiti i sve ostale brojeve. Konačno je rješenje



Slika 4.6.7: Konačno rješenje zadane logičke zagonetke kakuro.

Primjer 4.6.3. Riješi logičku zagonetku kakuro:



Slika 4.6.8: Zadana logička zagonetka kakuro.

Rješenje.

1. U trećem redu zadan je broj 29. 29 u četirima poljima može biti ostvaren samo pomoću brojeva 5, 7, 8 i 9. U predzadnjem stupcu zadan je broj 21 koji se u zadanih šest polja može upisati samo pomoću 1, 2, 3, 4, 5 i 6. Na križanju tog reda i stupca mora biti broj koji je i u jednom i u drugom rastavu, a jedini takav je 5.

2. U drugom redu zadan je broj 9. 9 u trima poljima može biti ostvaren samo pomoću brojeva manjih od 7. U četvrtom stupcu zadan je broj 23 koji se u zadanim trima poljima može upisati samo pomoću 6, 8 i 9. Na križanju tog reda i stupca mora biti broj koji je i u jednom i u drugom rastavu, a jedini takav je 6.

3. Za isti taj broj 9 nakon upisane šestice nije moguće upisati 2 pa 1 jer bi iznad broja 1 bio zadani 11 kojeg bismo morali realizirati kao $10 + 1$. Zato iza 9 moraju biti 6 pa 1 pa 2. Odmah rješavamo 11 iznad upisanog broja 1 i 12 lijevo.

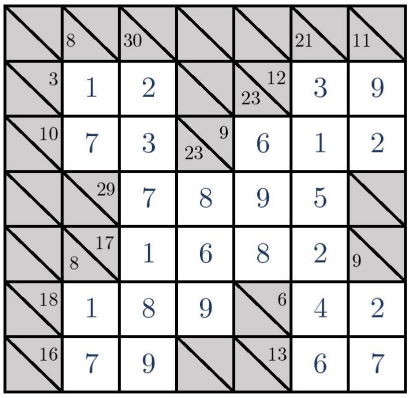
4. U predzadnjem stupcu zadan je broj 21 koji se u zadanih šest polja može upisati samo pomoću 1, 2, 3, 4, 5 i 6. 1, 3 i 5 smo upravo upisali. Na dnu tog stupca uz zadani broj 13 ne može biti upisan 2, a niti 4 zbog broja 9 u polju gore desno od tog 13. Stoga u to zadnje polje tog stupca moramo upisati 6 i odmah desno od te

šestice 7, iznad tog broja 7 broj 2, a lijevo od tog broja 2 broj 4. Sada je u stupcu zadanog broja 21 preostao samo broj 2 pa upišemo i njega.

5. U polju dolje lijevo zadan je broj 16. Upisujemo, dakle, ili 7, 9, ili 9, 7. No, zbog zadanog broja 8, iznad upisujemo 7, 9. Iznad tog broja 7 upisujemo 1, a desno od toga 8 pa 9.

6. U trećem redu zadan je broj 29, a u drugom stupcu broj 30. U polje u kojemu se oni križaju mora, zbog rastava broja 29, biti upisan ili 7 ili 8 ili 9. No, 8 i 9 su već upisani u tom stupcu pa tu moramo postaviti broj 7. Sada desno od 7 moramo upisati 8 pa 9. Ispod te osmice odmah upisujemo 6, a ispod 9 upisujemo 8. Lijevo od upisanog broja 6 upisujemo broj 1.

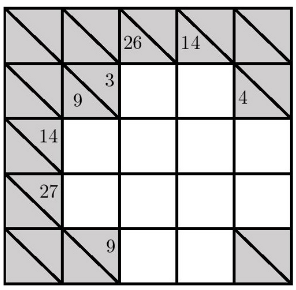
7. Na kraju, u prva dva reda upisujemo redom 1 pa 2 te u drugi red 7 pa 3. Konačno je rješenje



Slika 4.6.9: Konačno rješenje logičke zagonetke kakuro.

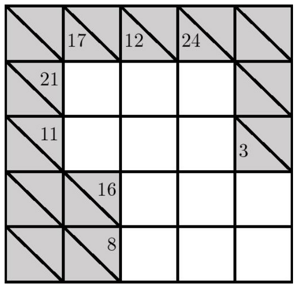
Zadaci za vježbu

Zadatak 4.6.1. Riješi logičku zagonetku kakuro:



Slika 4.6.10: Zadana logička zagonetka kakuro.

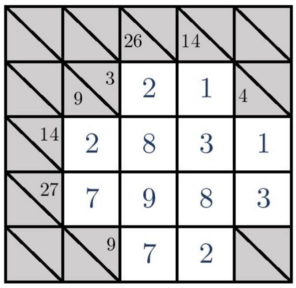
Zadatak 4.6.2. Riješi logičku zagonetku kakuro:



Slika 4.6.11: Zadana logička zagonetka kakuro.

RJEŠENJA

4.6.1. Započinjemo od zadanog broja 3, a ostalo ide dosta lako pa postupak nećemo detaljno objašnjavati. Konačno je rješenje



Slika 4.6.12: Konačno rješenje zadane logičke zagonetke kakuro.

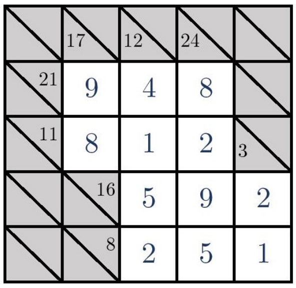
4.6.2. Ova je križaljka nešto teža od prethodnih.

1. Krećemo od broja 17. Upisujemo ili 8 pa 9 ili 9 pa 8. Zbog zadanog broja 11, mora biti upisano 9 pa 8. To je bilo lako za uočiti. Dalje više nije tako jednostavno.

2. Iza zadanog broja 21, a nakon upisanog broja 9, u sljedeća dva polja moramo upisati ili brojeve iz skupa $\{4, 8\}$ ili brojeve iz skupa $\{5, 7\}$. Drugo, kako zadani broj 12 možemo rastaviti samo na dva načina, pomoću brojeva iz skupa $\{1, 2, 3, 6\}$ ili pomoću brojeva iz skupa $\{1, 2, 4, 5\}$, slijedi da će se taj broj 12 zapisati pomoću brojeva iz skupa $\{1, 2, 4, 5\}$ jer skup $\{1, 2, 3, 6\}$ ne sadrži niti jedan broj za prikaz prije razmatranog broja 21.
   Zadani broj 3 možemo zapisati samo kao $1 + 2$ ili kao $2 + 1$. Slijedi da zadani broj 16 sadrži u rastavu ili broj 1 ili broj 2 (koji su ispod zadanog broja 3).

Samo su četiri načina da se 16 zapiše koristeći 1 ili 2. Možemo ga zapisati samo pomoću brojeva iz skupova $\{1, 6, 9\}$, $\{1, 7, 8\}$, $\{2, 5, 9\}$ i $\{2, 6, 8\}$. Dakle, na presjeku rješenja za 16 i 12 mora biti broj 5. Odmah iza 5 upisujemo 9 i 2.

3. Sada lako riješimo redom zadane brojeve: 3, 21, 8, 12, 24. Konačno je rješenje



Slika 4.6.13: Konačno rješenje zadane logičke zagonetke kakuro.

4.7. Integram

Riječ integram dolazi od latinske riječi *"integer"* – cijeli, sav jer iz dijela priče moramo rekonstruirati cijelu priču, cijeli tekst. Integram je hrvatski naziv za ovakvu vrstu zagonetke dok se u engleskom govornom području ovakve zagonetke zovu uglavnom "logic puzzle" ili "logic grid puzzles". Kao i za rekurzivne logičke zagonetke, i za integram je vrlo teško napisati program za računalo koji bi dao rješenje za unesenu zagonetku ovog tipa.

Cjelinu Integrami treba obraditi poslije obrade cjeline Relacije. Cilj je integrama zaključiti koji je pojam u relaciji. U zaključivanju se koriste simetričnost, tranzitivnost te ponegdje linearnost relacija.

Literatura za ovo potpoglavlje jest:

1. Brainzilla,
   https://www.brainzilla.com/logic/logic-grid/
   (zadnji pristup travanj 2022.)
   (Internetska stranica s velikim brojem integrama razvrstanih po stupnju težine. Ova stranica sadrži i dio s uputstvima za rješavanje.)

2. Logičke Mozgalice. Integrami - Artrea,
   https://www.artrea.com.hr/mozgalice6.html (zadnji pristup travanj 2022.)
   (Ovo je izvrsna hrvatska intrnetska stranica s mnoštvom integrama različitih veličina.)

3. Puzzle Baron's Logic puzzles,
   https://logic.puzzlebaron.com/ (zadnji pristup travanj 2022.)
   (Na ovoj internetskoj stranici nalazi se veliki broj integrama različitih veličina i težina. Na ovoj stranici čitatelj se može prijaviti na online natjecanje koje se održava svakog mjeseca.)

Primjer 4.7.1. Ana, Ena i Ina su studentice koje imaju 22, 23 i 24 godine. Jednoj je omiljeni sport šah, jednoj bob, a jednoj K–1. Koliko godina ima svaka od djevojaka i koji joj je hobi, ako znamo:

1. Osoba koja ima 23 godine ne voli K–1.
2. Ena ima 23 godine.
3. Inin omiljeni sport nije K–1.
4. Studentica koja ima 23 godine ne bavi se šahom.
5. Ina je starija od Ane.

Rješenje. Pokazuje se kako se ovakve logičke zagonetke najlakše rješavaju tablicom koju kreiramo tako da u njoj postoje područja gdje se sreću imena i godine, imena i omiljeni sportovi te godine i sportovi, odnosno tablicom kao na slici 4.7.1.

Sada u tu tablicu na mjesto gdje dvije pojave sigurno jesu u relaciji postavljamo znak O (oks ili veliko slovo O), a gdje nisu u relaciji postavljamo veliko iks – X.

		Imena			Hobiji		
		Ana	Ena	Ina	Šah	Bob	K-1
Godine	22						
	23						
	24						
Hobiji	Šah						
	Bob						
	K-1						

Slika 4.7.1: Početna prazna tablica.

1. Rečenica broj 1 kaže da osoba koja ima 23 godine ne voli K-1. Nalazimo dio tablice gdje se susreću godine i hobiji te na presjeku broja 23 i hobija K-1 postavimo X (jer rečenica je oblika x "ne voli" y), kao na slici 4.7.2.

		Imena			Hobiji		
		Ana	Ena	Ina	Šah	Bob	K-1
Godine	22						
	23						X
	24						
Hobiji	Šah						
	Bob						
	K-1						

Slika 4.7.2: Početna prazna tablica nakon prvog zaključka.

2. Ena ima 23 godine.

Pronalazimo dio tablice gdje se susreću imena i godine te na presjek imena Ena i broja godina 23 postavimo O (jer rečenica je afirmativna, s glagolom "ima"), kao na slici 4.7.3.

		Imena			Hobiji		
		Ana	Ena	Ina	Šah	Bob	K-1
Godine	22						
	23		O				X
	24						
Hobiji	Šah						
	Bob						
	K-1						

Slika 4.7.3: Tablica nakon dvaju zaključaka.

Sada na osnovu ovih dvaju znakova zaključujmo sljedeće.
Prvo, ako Ena ima 23 godine, onda 23 godine nemaju Ana i Ina, pa stavljamo X lijevo i desno od znaka O. Drugo, ako Ena ima 23 godine, onda Ena nema 22 godine niti 24 godine, pa stavljamo X ispod i iznad znaka O. Tako će biti uvijek u svim tablicama – ako smo negdje postavili O onda u sva mjesta lijevo, desno, ispod i iznad tog mjesta do granica "podkvadrata" postavljamo znak X.
Treće, u tablici se desno od upisanog O već nalazio jedan X koji je rekao da osoba od 23 godine ne voli K–1. No, to je Ena, pa odmah znači da Ena ne voli K–1. Tako

će biti i inače: ako smo upisali negdje O (koji znači da nešto jest), a bilo gdje dalje u tom redu ili stupcu postoji znak X, onda će u tablici morati biti novi znak X te su ti X-ovi simetrični s obzirom na zadani O.

		Imena			Hobiji		
		Ana	Ena	Ina	Šah	Bob	K-1
Godine	22		X				
	23	X	O	X			X
	24		X				
Hobiji	Šah						
	Bob						
	K-1		X				

Slika 4.7.4: "Simetrični" znaci X oko određenog znaka O.

3. Inin omiljeni sport nije K–1.

Postavljamo X, a onda odmah i O generiram s dvama znakovima X u istom redu (jer ako Ena ne voli K–1 i Ina ne voli K–1, onda sigurno Ana voli K–1). Dodajemo i dva znaka X iznad upisanog O.

		Imena			Hobiji		
		Ana	Ena	Ina	Šah	Bob	K-1
Godine	22		X				
	23	X	O	X			X
	24		X				
Hobiji	Šah	X					
	Bob	X					
	K-1	O	X	X			

Slika 4.7.5: Tablica nakon zaključka broj 3.

4. Studentica koja ima 23 godine ne bavi se šahom.

Postavljamo X, a onda odmah i O generiram s dvama znakovima X u istom redu (jer ako osoba stara 23 godine ne voli ni šah ni K–1, onda sigurno voli bob). Dodajemo i dva znaka X iznad upisanog O.

		Imena			Hobiji		
		Ana	Ena	Ina	Šah	Bob	K-1
Godine	22		X			X	
	23	X	O	X	X	O	X
	24		X			X	
Hobiji	Šah	X					
	Bob	X					
	K-1	O	X	X			

Slika 4.7.6: Tablica nakon zaključka broj 4.

5. Ina je starija od Ane.

   Jedino je moguće rješenje da Ina onda ima 24 godine, a Ana 22. Ispunimo ostatak tog područja znacima X. Uočimo iz prvog stupca tablice kako Ana ima 22 godine i omiljeni joj je sport K–1. Tako ta dva znaka O tvore odmah i treći u području u kojemu se križaju godine i sportovi, tj. osoba stara 22 godine tada voli K–1. Preostalo je da osoba od 24 godine voli šah, a to je Ina i tada je zagonetka riješena.

		Imena			Hobiji		
		Ana	Ena	Ina	Šah	Bob	K-1
Godine	22	O	X	X	X	X	O
	23	X	O	X	X	O	X
	24	X	X	O	O	X	X
Hobiji	Šah	X	X	O			
	Bob	X	O	X			
	K-1	O	X	X			

Slika 4.7.7: Tablica nakon zaključka broj 5.

Rješenje: Ana ima 22 godine i omiljeni joj je sport K-1, Ena ima 23 godine i omiljeni joj je sport bob, Ina ima 24 godine i omiljeni joj je sport šah.

Primjer 4.7.2 (Slike s kršćanskim motivima)**.** Pet slika nalaze se u pet različitih gradova. Svaka je posebne veličine i svaka je u jednom od pet navedenih gradova. Na osnovu zadanih rečenica odredi koja je slika u kojem od gradova, koje je veličine (od zadanih veličina u tablici) i koji ju je umjetnik nacrtao.

1. Slika Skidanje s križa manja je od slike koja je u budimpeštanskom "Muzeju lijepih umjetnosti".
2. Tizian nije autor Posljednje večere.
3. U milanskoj "Pinacoteci di brera" izložena je najveća slika. To nije slika Krist poslije bičevanja.
4. Slika Polaganje u grob u pariškom "Louvreu" veća je od El Grecove slike Krist na Maslinskoj gori.
5. Najmanja slika jedna je od najspektakularnijih u Van Dyckovoj ikonografiji.
6. U londonskoj "Nacionalnoj galeriji" nalazi se Velazquezova slika, dakle ne i slika veličine 170×112 cm.
7. Sve "veće" u gore navedenim rečenicama znači neposredno veće, tj. "veće i odmah do", kao i manje.

Konačno rješenje zapiši u sljedećoj tablici:

Tablica 4.7.1: Forma konačnog rješenja

Platno	Autor	Veličina	Grad
Krist na Maslinskoj gori			
Krist poslije bičevanja			
Polaganje u grob			
Posljednja večera			
Skidanje s križa			

Rješenje. Prvo moramo kreirati uobičajenu tablicu u kojoj će morati biti svi presjeci zadanih područja – presjek imena slike i veličine, presjek imena slike i autora, ..., presjek autora i veličine. Bit će, dakle, ukupno deset područja kao na slici 4.7.8.

	149×109 cm	170×112 cm	225×148 cm	206×165 cm	304×250 cm	El Greco	Rubens	Tizian	Van Dyck	Velazquez	Budimpešta	London	Milano	München	Pariz
Krist na Maslin. gori															
Krist poslije bičevanja															
Polaganje u grob															
Posljednja večera															
Skidanje s križa															
Budimpešta															
London															
Milano															
München															
Pariz															
El Greco															
Rubens															
Tizian															
Van Dyke															
Velazquez															

Slika 4.7.8: Prazna tablica sa svim presjecima područja.

Upišimo sada na osnovu zadanih podataka znakove O ako nešto jest u relaciji i X ako nije.

1. Slika Skidanje s križa manja je od slike koja je u budimpeštanskom “Muzeju lijepih umjetnosti”.

   Iz ove rečenice, pažljivije čitajući (i više puta, predlažemo) saznajemo:

   - Slika Skidanje s križa nije najveća slika (pišemo X kod imena te slike i najveće veličine).
   - Slika Skidanje s križa ne nalazi se u Budimpešti.
   - Slika koja je u Budimpešti nije najmanja slika.

	149×109 cm	170×112 cm	225×148 cm	206×165 cm	304×250 cm	El Greco	Rubens	Tizian	Van Dyck	Velazquez	Budimpešta	London	Milano	München	Pariz
Krist na Maslin. gori															
Krist poslije bičevanja															
Polaganje u grob															
Posljednja večera															
Skidanje s križa					X						X				
Budimpešta	X														
London															
Milano															
München															
Pariz															
El Greco															
Rubens															
Tizian															
Van Dyke															
Velazquez															

Slika 4.7.9: Tablica nakon provođenja zaključaka iz rečenice broj 1.

2. Tizian nije autor Posljednje večere.
   U presjeku reda Posljednja večera i stupca Tizian pišemo X.

3. U milanskoj "Pinacoteci di brera" izložena je najveća slika. To nije slika Krist poslije bičevanja.

   - U presjeku pojmova Milano i najveća slika postavljamo O. Čim smo postavili znak O gledamo što se u tom retku i stupcu nalazi i sve znakove X i O iz tog reda i stupca prebacujemo u još jedno polje. Konkretno, u tablici se u stupcu najveće slike već nalazi X kod reda Skidanje s križa. Upravo upisani O znači da je u Milanu najveća slika, a prije toga upisani X znači da najveća slika nije Skidanje s križa. Ukupno zaključujemo kako u Milanu nije Skidanje s križa i tu upisujemo još jedan X. (Ovdje se lijepo vidi tranzitivnost zadanih relacija.)
   - U Milanu nije Krist poslije bičevanja i najveća slika nije Krist poslije bičevanja.

	149×109 cm	170×112 cm	225×148 cm	206×165 cm	304×250 cm	El Greco	Rubens	Tizian	Van Dyck	Velazquez	Budimpešta	London	Milano	München	Pariz
Krist na Maslin. gori															
Krist poslije bičevanja					X								X		
Polaganje u grob															
Posljednja večera								X							
Skidanje s križa					X						X		X		
Budimpešta	X				X										
London					X										
Milano	X	X	X	X	O										
München					X										
Pariz					X										
El Greco															
Rubens															
Tizian															
Van Dyke															
Velazquez															

Slika 4.7.10: Tablica nakon provođenja zaključaka iz rečenica 1., 2. i 3. Uočimo kako iznad znaka O koji povezuje Milano i najveću sliku imamo dva znaka X i automatski ta dva znaka imamo i ispod pojma Milano.

Nakon sličnih razmatranja u sljedećim rečenicama i, nakon što smo u zadnjoj rečenici saznali da su svi "manje od" i "veće od" značenja neposredno manje od i "neposredno" veće od, dobivamo konačno rješenje.

	149×109 cm	170×112 cm	225×148 cm	206×165 cm	304×250 cm	El Greco	Rubens	Tizian	Van Dyck	Velazquez	Budimpešta	London	Milano	München	Pariz
Krist na Maslin. gori	X	O	X	X	X	O	X	X	X	X	O	X	X	X	X
Krist poslije bičevanja	X	X	X	O	X	X	X	X	X	O	X	O	X	X	X
Polaganje u grob	X	X	O	X	X	X	X	O	X	X	X	X	X	X	O
Posljednja večera	X	X	X	X	O	X	O	X	X	X	X	X	O	X	X
Skidanje s križa	O	X	X	X	X	X	X	X	O	X	X	X	X	O	X
Budimpešta	X	O	X	X	X	O	X	X	X	X					
London	X	X	X	O	X	X	X	X	X	O					
Milano	X	X	X	X	O	X	O	X	X	X					
München	O	X	X	X	X	X	X	X	O	X					
Pariz	X	X	O	X	X	X	X	O	X	X					
El Greco	X	O	X	X	X										
Rubens	X	X	X	X	O										
Tizian	X	X	O	X	X										
Van Dyke	O	X	X	X	X										
Velazquez	X	X	X	O	X										

Slika 4.7.11: Konačno rješenje.

ZADACI ZA VJEŽBU

Zadatak 4.7.1 (Einsteinova zagonetka)**.** U ulici se nalazi pet kuća obojenih u pet različitih boja. U svakoj kući živi jedan čovjek drugačije nacionalnosti. Svaki od njih pije neko piće, puši određenu marku cigareta i ima kućnog ljubimca. Niti jedan od njih ne pije istu vrstu pića, ne puši istu marku cigareta i nema istog ljubimca.

1. Britanac živi u crvenoj kući.
2. Šveđanin ima psa za ljubimca.
3. Danac pije čaj.

4. Zelena kuća nalazi se s lijeve strane bijele kuće (prva do nje).
5. Vlasnik zelene kuće pije kavu.
6. Vlasnik koji puši Pal Mal ima ptice za ljubimce.
7. Stanovnik žute kuće puši Dunhill.
8. Čovjek koji živi u kući u sredini pije mlijeko.
9. Norvežanin živi u prvoj kući.
10. Vlasnik koji puši Blends živi pokraj kuće čiji vlasnik ima mačku.
11. Čovjek koji ima konja živi pokraj čovjeka koji puši Dunhill.
12. Čovjek koji puši marku cigareta Bluemaster pije pivo.
13. Nijemac puši marku cigareta Prince.
14. Norvežanin živi pokraj plave kuće.
15. Čovjek koji puši Blends živi pokraj čovjeka koji pije vodu.

Pitanje: Čiji je kućni ljubimac ribica?

Zadatak 4.7.2. Premda je nemoguće iz teksta postaviti pravilno znakove O i X u tablicu, programer može ipak napraviti nešto za pomoć rješavačima integrama.
Izradi program koji će kreirati tablicu za integram i nakon unesenih znakova O i X generirati, ako je moguće, neupisane X i O koji slijede iz već upisanih (kao u argumentaciji pod 3 kod integrama sa slikama.).

Rješenja

4.7.1. Zadatak ima jedno područje više od prethodnog, pa treba napraviti tablicu sljedećeg oblika:

Tablica 4.7.2: Forma u kojoj se susreću sva područja iz priče.

	Boja kuće	Ljubimci	Piće	Cigarete
Nacionalnost				
Cigarete				
Pića				
Ljubimci				

Ili, ako ubacimo sve podatke, dobivamo:

	Bijela	Crvena	Plava	Zelena	Žuta	Konj	Mačka	Pas	Ptica	Ribica	Čaj	Kava	Mlijeko	Pivo	Voda	Blend	Bluemaster	Dunhill	Pall Mall	Prince
Britanac																				
Danac																				
Norvežanin																				
Nijemac																				
Švedanin																				
Blend																				
Bluemaster																				
Dunhill																				
Pall Mall																				
Prince																				
Čaj																				
Kava																				
Mlijeko																				
Pivo																				
Voda																				
Konj																				
Mačka																				
Pas																				
Ptica																				
Ribica																				

Rješenja ćemo upisati u sljedeću tablicu

Tablica 4.7.3: Oblik konačnog rješenja.

	Boja kuće	Ljubimci	Piće	Cigarete
Britanac				
Danac				
Norvežanin				
Nijemac				
Švedanin				

Konačno je rješenje da Nijemac kao kućnog ljubimca drži ribicu, no svakako čitatelju predlažemo popuniti što veći dio tablice kako bi to i sam izveo iz zadanih rečenica što je s čim u relaciji.

4.8. Sudoku

Sudoku (japanski – *"jedna znamenka"*) je logička zagonetka koja je vrlo stara, no veću popularnost stječe krajem osamdesetih godina prošlog stoljeća u Japanu, a na zapadu sredinom 2000–tih.

Pravila: Zadana je križaljka s n polja u svakom redu, n polja u svakom stupcu i n polja u svakom istaknutom podskupu te križaljke. U svako prazno polje treba upisati neki od brojeva od 1 do n tako da se u svakom redu, svakom stupcu i svakom istaknutom podskupu veličine n polja nađu svi brojevi od 1 do n. Drugim riječima, na kraju će u svakom redu biti svi brojevi od 1 do n, tj. niti jedan od brojeva neće se pojaviti dva ili više puta. Svaki jednom i to točno jednom. Isto vrijedi i za stupce i za istaknute podskupove.

Pogledajmo kako izgleda jedan primjer zadane i odmah pokraj njega riješene sudoku zagonetke.

	2							
			6					**3**
	7	**4**		**8**				
					3			**2**
	8			**4**			**1**	
6			**5**					
				1		**7**	**8**	
5					**9**			
							4	

1	**2**	6	4	3	7	9	5	8
8	9	5	**6**	2	1	4	7	**3**
3	**7**	**4**	9	**8**	5	1	2	6
4	5	7	1	9	**3**	8	6	**2**
9	**8**	3	2	**4**	6	5	**1**	7
6	1	2	**5**	7	8	3	9	4
2	6	9	3	**1**	4	**7**	**8**	5
5	4	8	7	6	**9**	2	3	1
7	3	1	8	5	2	6	**4**	9

Slika 4.8.1: S lijeve strane je zadani sudoku u kojemu treba prazna polja popuniti brojevima od 1 do 9. Postoji samo jedno rješenje i ono je dano na desnoj slici.

U desnoj križaljci slike 4.8.1 zaista se u svakom redu, stupcu i potpolju nalaze svi brojevi od 1 do 9.

Primjer 4.8.1. Riješi sudoku:

	4		
			4
			2
	1		3

Slika 4.8.2: Zadana logička zagonetka sudoku.

Rješenje. U zadnjem stupcu već imamo 4, 2 i 3 pa je potrebno upisati broj 1. Dobivamo

	4		1
			4
			2
	1		3

Slika 4.8.3: Prvi korak u rješavanju zadane logičke zagonetke sudoku.

Pogledajmo sada donji desni kvadratić veličine 2×2. U njemu su 2 i 3. Nedostaju, dakle, 1 i 4. Možemo postaviti gore 1 i dolje 4 ili obrnuto. No, obrnuta situacija, u kojoj je gore 4, a dolje 1 ne dolazi u obzir jer bi tada, gledajući cijelu križaljku, u četvrtom redu imali dva broja 1, što se ne smije dogoditi.

	4		1
			4
		1	2
	1	4	3

Slika 4.8.4: Drugi korak u rješavanju zadane logičke zagonetke sudoku.

Pogledajmo sada broj 1. Broj 1 nedostaje u drugom redu i u prvom stupcu. Zato upisujemo broj 1 u sjecište drugog reda i prvog stupca.

	4		1
1			4
		1	2
	1	4	3

Slika 4.8.5: Treći korak u rješavanju zadane logičke zagonetke sudoku.

Tri su broja 4 upisana. Znači da nedostaje još jedan. Zadnji broj 4 upisujemo u treći red, prvi stupac.

	4		1
1			4
4		1	2
	1	4	3

Slika 4.8.6: Četvrti korak u rješavanju zadane logičke zagonetke sudoku.

Pogledajmo sada donji lijevi kvadratić veličine 2×2. U njemu su 4 i 1. Nedostaju, dakle, 2 i 3. Možemo postaviti gore 2 i dolje 3 ili obrnuto. Zbog brojeva 2 i 3 u zadnjem stupcu, jedini je raspored koji dolazi u obzir

	4		1
1			4
4	3	1	2
2	1	4	3

Slika 4.8.7: Peti korak u rješavanju zadane logičke zagonetke sudoku.

U drugom stupcu sada nedostaje samo broj 2.

	4		1
1	2		4
4	3	1	2
2	1	4	3

Slika 4.8.8: Šesti korak u rješavanju zadane logičke zagonetke sudoku.

Sada, popunjavanjem drugog reda pa prvog stupca pa trećeg stupca dobivamo konačno rješenje u kojemu su zaista u svakom redu, stupcu i podkvadratu po jedna jedinica, jedna dvojka, jedna trojka i jedna četvorka.

3	4	2	1
1	2	3	4
4	3	1	2
2	1	4	3

Slika 4.8.9: Konačno rješenje zadane logičke zagonetke sudoku.

Poznato je da ne postoji polinomijalni algoritam za rješavanje sudoku zagonetke veličine $n \times n$ (sudoku je NP – težak, čak NP – potpun), pa je zanimljiv izazov napraviti brzi algoritam za rješavanje sudokua. Dobro je započeti sa sudokuom veličine

4×4, kao u našem primjeru 4.8.1, zatim s 9×9 i na kraju s općim sudokuom, što je u stvari vrlo težak zadatak jer istaknuta potpolja mogu biti postavljena na najrazličitije načine.

Sudoku jedne te iste dimenzije može biti zadan na različite načine. Pogledajmo tri različita sudokua veličine 6×6.

Primjer 4.8.2. Riješi sudoku:

			1	3	
					4
5	1				
	4				
	2	4			
					2

Slika 4.8.10: Zadana logička zagonetka sudoku.

U ovoj sudoku zagonetki u svakom redu, u svakom stupcu i na svakoj od dviju dijagonala moraju se naći svi brojevi od 1 do 6.

Rješenje. Za početak uočimo kako je u zadanoj mreži najviše četvorki. Pogledajmo gdje možemo staviti broj 4 na glavnu dijagonalu (dijagonala od gornjeg lijevog do donjeg desnog vrha kvadrata).
Broj 4 ne može ići skroz dolje desno jer je tu već broj 2. Broj 4 ne može biti postavljen niti na polje uz njega jer je lijevo od tog polja, u tom redu, također broj 4. I tako dalje. Jedino polje gdje može doći broj 4 u tu dijagonalu je gornje lijevo polje.

4			1	3	
					4
5	1				
	4				
	2	4			
					2

Slika 4.8.11: Prvi korak u rješavanju zadane logičke zagonetke sudoku.

Na drugoj, sporednoj dijagonali (od donjeg lijevog do gornjeg desnog vrha) broj 4 sada mora ići na četvrto polje slijeva. Onda ostaje samo još jedno mjesto za zadnji neupisani broj 4.

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

Slika 4.8.12: Drugi korak u rješavanju zadane logičke zagonetke sudoku.

Sada smo u križaljku upisali sve brojeve 4.

Pogledajmo sada treći red i zapitajmo se gdje u njega možemo postaviti broj 2. Na treće mjesto u tom redu ne možemo ju upisati jer to mjesto pripada i dijagonali koja već sadrži broj 2. U zadnjem stupcu već je upisan broj 2. Jedino slobodno mjesto za broj 2 je peto, predzadnje mjesto tog reda.

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

Slika 4.8.13: Treći korak u rješavanju zadane logičke zagonetke sudoku.

Sada upisujemo broj 2 u četvrti red, pa u prvi pa u drugi.

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

Slika 4.8.14: Četvrti korak u rješavanju zadane logičke zagonetke sudoku.

Dalje upisujemo broj 1 na glavnu dijagonalu dolje pa u zadnji stupac na četvrto mjesto, pa u sporednu dijagonalu i na kraju u drugi red. Zatim upisujemo broj 3 na sporednu dijagonalu. Sada na križanju trećeg reda i trećeg stupca mora biti prvi upisani broj 6, a dalje je sve lako. Konačno je rješenje dano na sljedećoj slici.

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

Slika 4.8.15: Konačno rješenje zadane logičke zagonetke sudoku.

ZADACI ZA VJEŽBU

Zadatak 4.8.1. Riješi sudoku:

		4	6		
	2			1	
	3			2	
		6	5		

Slika 4.8.16: Zadana logička zagonetka sudoku.

Zadatak 4.8.2. Riješi sudoku:

	5			6	
3					5
5	4	3		2	
	6		5	3	4
4					2
	2			5	

Slika 4.8.17: Zadana logička zagonetka sudoku.

Zadatak 4.8.3. Riješi sudoku (bez unutrašnjih podskupova, brojevi od 1 do 6 moraju se pojaviti samo u redu i stupcu):

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

Slika 4.8.18: Zadana logička zagonetka sudoku.

Zadatak 4.8.4. Riješi sudoku:

4				9	5			
1			6			8	5	2
2								7
	9				1		2	
	8				2	9	4	
				5	3			
9		3						
			4			1	7	9
		6	1			2		

Slika 4.8.19: Zadana logička zagonetka sudoku.

Rješenja

4.8.1. Prvo se lako ispune četiri polja u sredini.

				A	B
		4	6	C	D
	2	5	3	1	E
	3	1	4	2	F
		6	5		

Slika 4.8.20: Prvi korak u rješavanju zadane logičke zagonetke sudoku.

Sada slijedi ključno razmišljanje. Pogledajmo gornji desni, potpuno prazni oblik u kojem su sva polja označena slovima i upitajmo se gdje u njega možemo upisati brojeve 1 i 2. 1 i 2 ne mogu ići u polja A i C jer su u tom stupcu već postavljeni. Dakle, 1 i 2 sigurno moraju ići u B, D, E ili F. No, to znači da u donjem desnom osjenčanom obliku 1 i 2 ne mogu biti postavljeni u zadnji stupac. Također, 1 i 2 ne mogu biti postavljeni niti u predzadnji stupac jer se tu već nalaze. Konačno, 1 i 2 u osjenčanom donjem desnom obliku moraju ići na prvo i drugo mjesto s lijeve strane. Kako je iznad krajnjeg lijevog polja već upisan broj 1, u to polje moramo upisati broj 2, a odmah do njega onda broj 1.

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

Slika 4.8.21: Drugi korak u rješavanju zadane logičke zagonetke sudoku.

Sada možemo odmah popuniti te stupce do kraja.
Zatim upisujemo preostala dva broja 2 itd. Konačno je rješenje

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

Slika 4.8.22: Konačno rješenje zadane logičke zagonetke sudoku.

4.8.2.

	5			6	
3	A				5
5	4	3		2	
	6		5	3	4
4	B				2
	2			5	

Slika 4.8.23: Prvi korak u rješavanju zadane logičke zagonetke sudoku.

Prvo u polje A upisujemo 1 jer u gornjem lijevom pravokutniku već imamo 3 i 5, a u stupcu u kojem je A upisani su već 2, 4 i 6. Zatim ispunimo taj cijeli stupac, tj. u polje B upišemo broj 3. Zatim popunimo cijeli 4 stupac, itd. Konačno je rješenje

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

Slika 4.8.24: Konačno rješenje zadane logičke zagonetke sudoku.

4.8.3. U trećem redu broj 2 možemo upisati samo na peto mjesto u redu. Sada u trećem stupcu također upisujemo broj 2, pa u drugom redu. Dvojke su sve sada upisane. Sada upisujemo broj 1: prvo u treći red, pa u četvrti pa u prvi. Zatim sređujemo cijeli četvrti red pa treći i dalje je jednostavno.

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

Slika 4.8.25: Konačno rješenje zadane logičke zagonetke sudoku.

4.8.4. Ovaj sudoku nije puno teži od prethodnih. Najčešćih je, možemo reći gotovo standardnih, dimenzija, 9×9. Uz malo strpljenja i malo više vremena nego što smo potrošili kod prethodnih sudokua može ga se riješiti. U ovoj zagonetki sudoku nećemo vam davati redom ideje kako ga treba započeti itd. Prepuštamo ga u potpunosti čitatelju.

4	7	8	2	9	5	3	6	1
1	3	9	6	7	4	8	5	2
2	6	5	3	1	8	4	9	7
3	9	7	8	4	1	5	2	6
5	8	1	7	6	2	9	4	3
6	2	4	9	5	3	7	1	8
9	1	3	5	2	7	6	8	4
8	5	2	4	3	6	1	7	9
7	4	6	1	8	9	2	3	5

Slika 4.8.26: Konačno rješenje zadane logičke zagonetke sudoku.

4.9. Što mogu 1, 2, 3, 4 i 5?

Zadatak 4.9.1. Koristeći brojeve 1, 2, 3, 4 i 5, svaki točno jednom, i četiri osnovne računske operacije, $+$, $-$, $\cdot$ i $:$, te proizvoljan broj zagrada, počevši od broja 1 zapiši točnim matematičkim izrazom redom što više prirodnih brojeva (do nekog broja n). Brojeve nije dozvoljeno lijepiti u neki višeznamenkasti broj, tj. nije dozvoljeno, na primjer od 2 i 5, napraviti 25.

Započnimo s nekoliko manjih, a čitatelj će nastaviti dalje.

$$
\begin{aligned}
0 &= (5 - 4 - 1) \cdot 2 \cdot 3 \\
1 &= 5 + 3 - 1 - 2 - 4 \\
2 &= 1 + (5 - 4) \cdot (3 - 2) \\
&\vdots
\end{aligned}
$$

Zadatak je, kao i sljedeći, pogodan za rad u grupama.

Rješenje. Svi brojevi od 1 do 75 mogu se zapisati na način zadan u zadatku, a računalom su dobivena rješenja (računalo je radilo tako da je pokušalo očuvati redoslijed 1, 2, 3, 4, 5, što nije nužno za rješenje zadatka):

$$
\begin{aligned}
1 &= 1 + 2 - (3 + 4) + 5\\
2 &= 1 + (2 - 3) \cdot 4 + 5\\
3 &= 1 - 2 + 3 - 4 + 5\\
4 &= 1 \cdot 2 + 3 + 4 - 5\\
5 &= 1 + 2 + 3 + 4 - 5))\\
6 &= 1 \cdot 2 + 3 - 4 + 5\\
7 &= 1 + 2 + 3 - 4 + 5\\
8 &= 1 \cdot 2 - 3 + 4 + 5\\
9 &= 1 + 2 - 3 + 4 + 5\\
10 &= 1 + 2 + 3 \cdot 4 - 5\\
11 &= 1 - 2 + 3 + 4 + 5\\
12 &= (1 + 2) \cdot ((3 - 4) + 5\\
13 &= (1 - 2 + 3) \cdot 4 + 5\\
14 &= 1 \cdot 2 + 3 + 4 + 5\\
15 &= 1 + 2 + 3 + 4 + 5\\
16 &= 1 + 2 \cdot 3 + 4 + 5\\
17 &= (1 - 2) \cdot 3 + 4 \cdot 5\\
18 &= (1 + 2) \cdot 3 + 4 + 5\\
19 &= 1 \cdot 2 + 3 \cdot 4 + 5\\
20 &= 1 + 2 + 3 \cdot 4 + 5\\
21 &= (1 + 2) : 3 + 4 \cdot 5\\
22 &= 1 - 2 + 3 + 4 \cdot 5\\
23 &= (1 + 2 \cdot 3) \cdot 4 - 5\\
24 &= 1 \cdot 2 \cdot (3 + 4 + 5)\\
25 &= 1 \cdot 2 + 3 + 4 \cdot 5\\
26 &= 1 + 2 + 3 + 4 \cdot 5\\
27 &= 1 + 2 \cdot 3 + 4 \cdot 5\\
28 &= (1 + 2) \cdot (3 + 5) + 4\\
29 &= (1 + 2 + 3) \cdot 4) + 5\\
&\ \vdots
\end{aligned}
$$

Uočimo da sve do broja 27 možemo brojeve zapisati na željeni način čak i poštujući red 1, 2, 3, 4, 5 korištenja zadanih brojeva. (Redoslijed 5, 4, 3, 2, 1 može, uz dana pravila, dati sve brojeve od 1 do 38.)

Naravno, pripadni računalni zadatak je računalu zadati pet brojeva (jednoznamenkastih) i uz gornja pravila pokušati dobiti što više prirodnih brojeva od 1 pa na dalje. Koristeći brojeve od 1 do 5 kao gore, ispravnim matematičkim izrazom, možemo prikazati sve brojeve od 1 do 75. A brojevi 2, 3, 4, 5 i 6 dat će po gornjim pravilima sve brojeve do gotovo nevjerojatnih 117.

Također, izazov je napraviti i računalni program u kojemu se, uz sva gore navedena pravila, znamenke smiju i spajati u višeznamenkasti broj, tj. od 2 i 5 smije se napraviti 25 (i 52).

Zadatak 4.9.2. Na papiriću je napisano 1 2 3 4.
Dodaj tom zapisu matematičke operacije kako bi dobio matematički izraz čija je vrijednost 1, 2, 3, ... Za razliku od prethodnog zadatka, ovdje moramo poštovati redoslijed zadanih brojeva, ali možemo ih lijepiti u jedan broj kao i koristiti proizvoljne matematičke operacije i funkcije, ne samo $+$, $-$, $\cdot$ i $:$.

Nije dozvoljeno dodavati brojeve, čak niti u eksponent, kao niti π, e, ... nego samo matematičke funkcije.

Rješenje.

$$\begin{aligned}
1 &= 12 : 3 : 4\\
2 &= -1 + 2 - 3 + 4\\
3 &= (1 + 2) \cdot (-3 + 4)\\
4 &= 1 + 2 - 3 + 4\\
5 &= (1 + 2) : 3 + 4\\
6 &= (1 + 23) : 4\\
7 &= (-1 + 2) \cdot 3 + 4\\
8 &= (1 - 2 + 3) \cdot 4\\
9 &= 12 \cdot 3 : 4\\
10 &= 1 \cdot 2 \cdot 3 + 4\\
&\vdots\\
20 &= 1 + 23 - 4\\
&\vdots\\
50 &= \lfloor (12 - \sqrt{3}) \cdot \sqrt{4!} \rfloor
\end{aligned}$$

(ovdje funkciju = $\lfloor \quad \rfloor$ koja daje najveći cijeli dio broja smatramo matematičkom funkcijom, no možemo, naravno, (po dogovoru) raditi i bez nje.)

Ovaj je zadatak puno teže riješiti računalom (teži je čak i od verzije prethodnog zadatka sa spajanjem brojeva) jer prije svega treba uzeti u obzir velik broj matematičkih operatora i funkcija, a onda sve to i implementirati na računalu. Pokazuje se da je s četirima osnovnim računskim operacijama, sa zagradama, s korijenom i faktorijelom te funkcijama pod i strop, moguće dobiti bar prvih 50 prirodnih brojeva.

Koliko znamo, ovo je otvoren problem o kojemu još nema nikakvih rezultata.

4.10. Logička ispunjaljka

Logička ispunjaljka, poznata i kao nonogram ili logičke slike (engl. *Picross*, *Griddlers*, *Pic-a-pix*) je logička zagonetka u obliku mreže čija polja treba zacrniti kako bismo dobili crno-bijelu sliku (najčešće) poznatog obrisa (neki predmet, lik, ...). Koja polja treba osjenčati i koliko ih treba osjenčati govore nam brojevi uz svaki red i stupac križaljke. Nonogram je nastao 1987. godine u Japanu.

Rješavanje nonograma na računalu također je NP–težak problem.

Literatura za ovo potpoglavlje jest:

1. N. Ueda, T. Nagao, *NP–completeness results for NONOGRAM via Parsimonious Reductions*, Technical Report, Department of Computer Science, Tokyo Institute of Technology, 1996.
   (U ovom je članku pokazano da je nonogam NP–težak.)

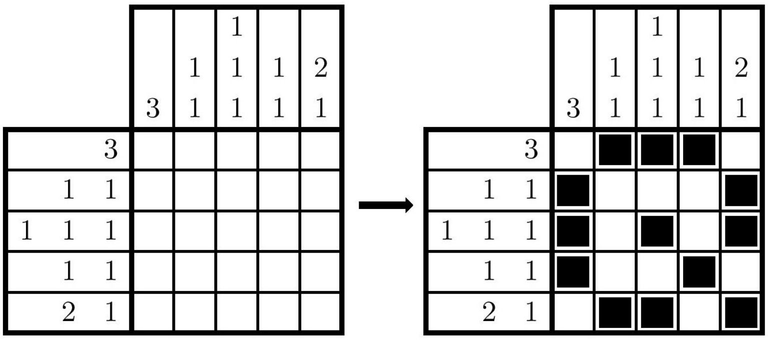
2. https://en.wikipedia.org/wiki/Nonogram (zadnji pristup travanj 2022.)
   (Na Wikipedijinoj stranici odlično je objašnjeno kako se nonogram rješava, koje su matematičke metode najčešće prisutne u rješavanju te koje su najčešće taktike traženja polja koje je potrebno zacrniti. Također je priloženo i nekoliko primjera.)

3. https://puzzlemadness.co.uk/nonograms/medium (zadnji pristup travanj 2022.)
   (Internetska stranica sa svakodnevno novim zagonetkama i mogućnošću online natjecanja s ostalim rješavačima.)

Pravila rješavanja:
Zadana je prazna (rijetko kada i već detaljno riješena) pravokutna mreža praznih polja. Pored svakog stupca i reda nalaze se brojevi a, b, c, ... koji nam govore da je u tom retku ili stupcu nekoliko (ili moguće nula) bijelih polja, pa a polja zaredom crne boje, zatim

slijedi bar jedno bijelo polje, onda opet b crnih polja pa bar jedno bijelo itd. Ponekad nonogram sadrži i brojeve koji su u boji kako bi i konačna slika bila u boji.

Primjer zadane i riješene zagonetke logička ispunjaljka:

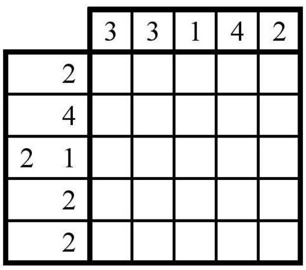


Slika 4.10.1: Primjer zadane i riješene crno-bijele zagonetke logička ispunjaljka.

Kako je rješavanje nonograma također NP–težak problem, tj. za sada nema brzog polinomijalnog algoritma, veće nonograme moći ćemo rješavati samo heurističkim metodama ako želimo u razumnom vremenu računalno dobiti rješenje.

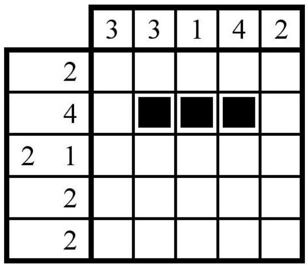
Najčešće će taktika biti započeti od najvećih zadanih brojeva, a onda naizmjenično, gledajući retke pa stupce koji sadrže upisana polja, dodavati, na osnovu zadanih brojeva, nova crna polja. Druga je ideja primijeniti već navedeni "backtracking" algoritam. On će pokušati, najbolje opet na mjestima s većim brojevima, upisati crno polje, a onda, ako se to pokaže kao odluka koja dovodi do nemoguće situacije, potrebno je obrisati sve znakove koje smo upisali nakon navedenog pretpostavljenog polja, a crno polje pretvoriti u znak koji znači da na tom mjestu sigurno nije crno polje.

Primjer 4.10.1. Riješi logičku ispunjaljku:



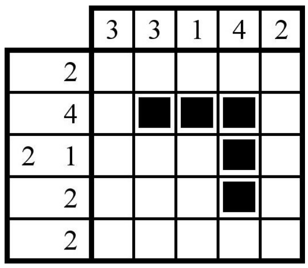
Slika 4.10.2: Zadana logička ispunjaljka.

Rješenje. U drugom redu pojavljuje se broj 4. To znači da u tom redu imamo 4 neprekidna crna polja u nizu. Kako je u tom redu ukupno 5 polja (cijela logička ispunjaljka je 5×5), slijedi da su ta četiri polja ili odmah na početku reda ili na kraju, a u oba slučaja drugo, treće i četvrto polje tog reda su crne boje, kao na sljedećoj slici.



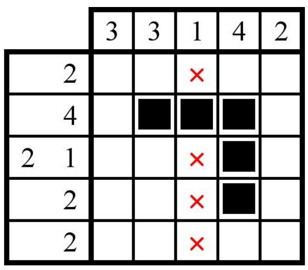
Slika 4.10.3: Prvi korak u rješavanju zadane logičke ispunjaljke.

Isto vrijedi za četvrti stupac.



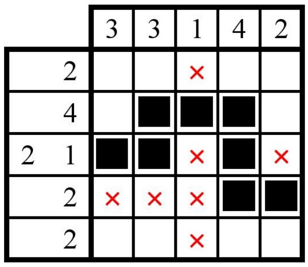
Slika 4.10.4: Drugi korak u rješavanju zadane logičke ispunjaljke.

Sada je jasno da se broj 1 iznad trećeg stupca odnosi na upisani crni kvadratić pa sve ostale kvadratiće tog stupca možemo označiti malim znakom $\times$ koji će nam značiti da na tom mjestu sigurno nije crno polje.



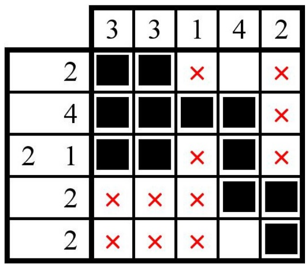
Slika 4.10.5: Treći korak u rješavanju zadane logičke ispunjaljke.

Sada možemo riješiti treći i četvrti red tablice. U trećem redu brojevi 2 i 1 jedino mogu biti (zbog upisanog znaka $\times$) ostvareni tako da se prije znaka $\times$ upišu dva, a poslije znaka $\times$ jedno crno polje (koje je već upisano) i u preostalo mjesto treba upisati $\times$. U četvrtom redu nalaze se samo dva crna polja u nizu. Jedno je već upisano pa preostalo polje samo dodamo njemu.



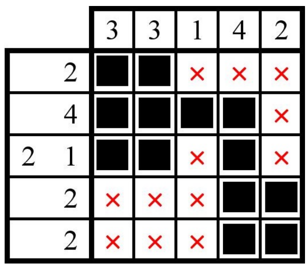
Slika 4.10.6: Četvrti korak u rješavanju zadane logičke ispunjaljke.

Sada možemo odmah riješiti prvi, drugi i zadnji stupac.



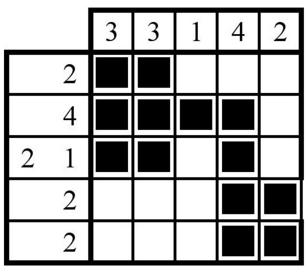
Slika 4.10.7: Peti korak u rješavanju zadane logičke ispunjaljke.

Na kraju, rješavanjem prvog i zadnjeg reda dobivamo konačno rješenje.



Slika 4.10.8: Konačno rješenje zadane logičke ispunjaljke.

Ili, bez pomoćnih znakova,



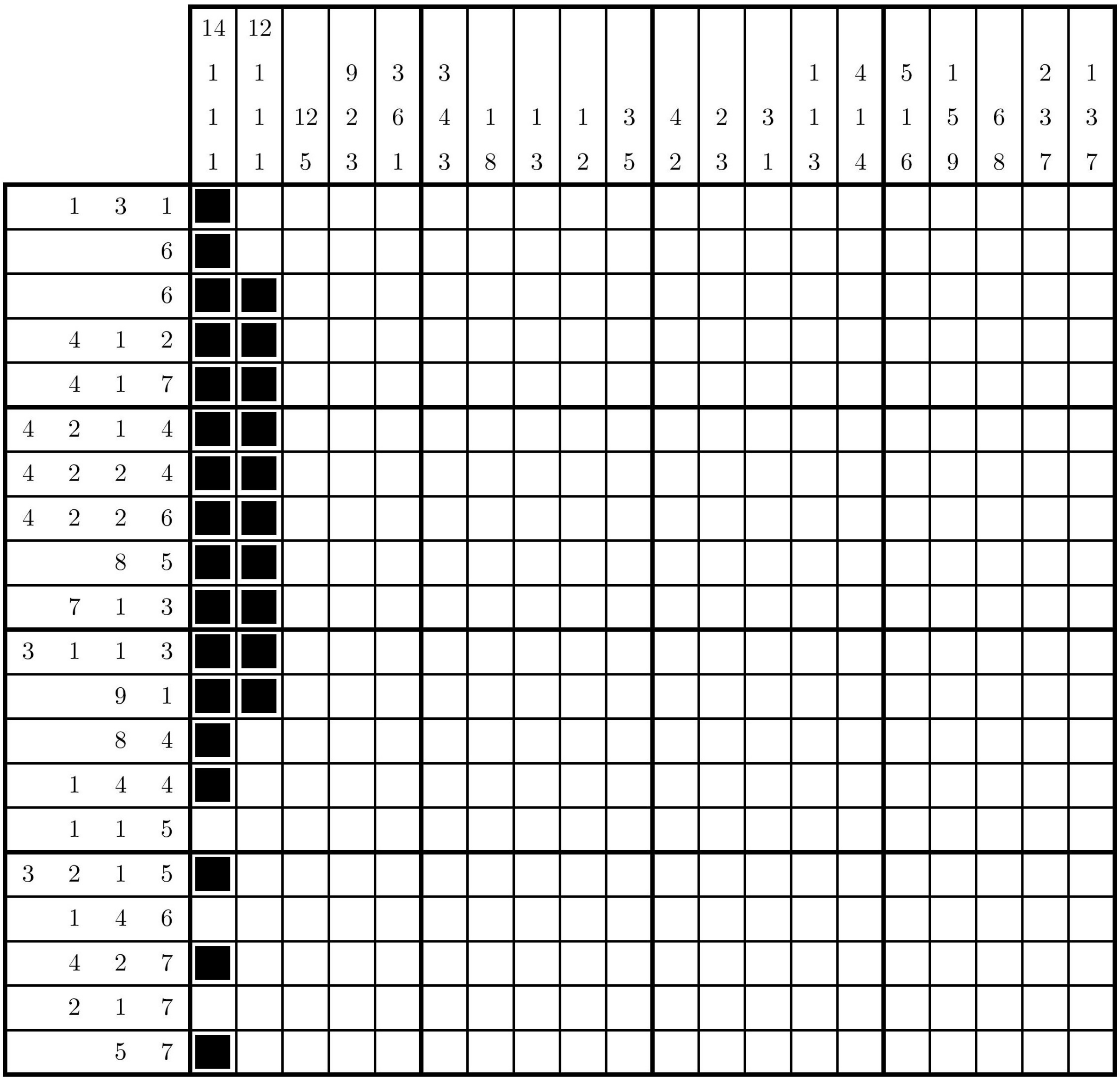
Slika 4.10.9: Konačno rješenje zadane logičke ispunjaljke bez pomoćnih znakova.

Primjer 4.10.2. Riješi nonogram:

	14	12																		
	1	1		9	3	3								1	4	5	1		2	1
	1	1	12	2	6	4	1	1	1	3	4	2	3	1	1	1	5	6	3	3
	1	1	5	3	1	3	8	3	2	5	2	3	1	3	4	6	9	8	7	7
1 3 1																				
6																				
6																				
4 1 2																				
4 1 7																				
4 2 1 4																				
4 2 2 4																				
4 2 2 6																				
8 5																				
7 1 3																				
3 1 1 3																				
9 1																				
8 4																				
1 4 4																				
1 1 5																				
3 2 1 5																				
1 4 6																				
4 2 7																				
2 1 7																				
5 7																				

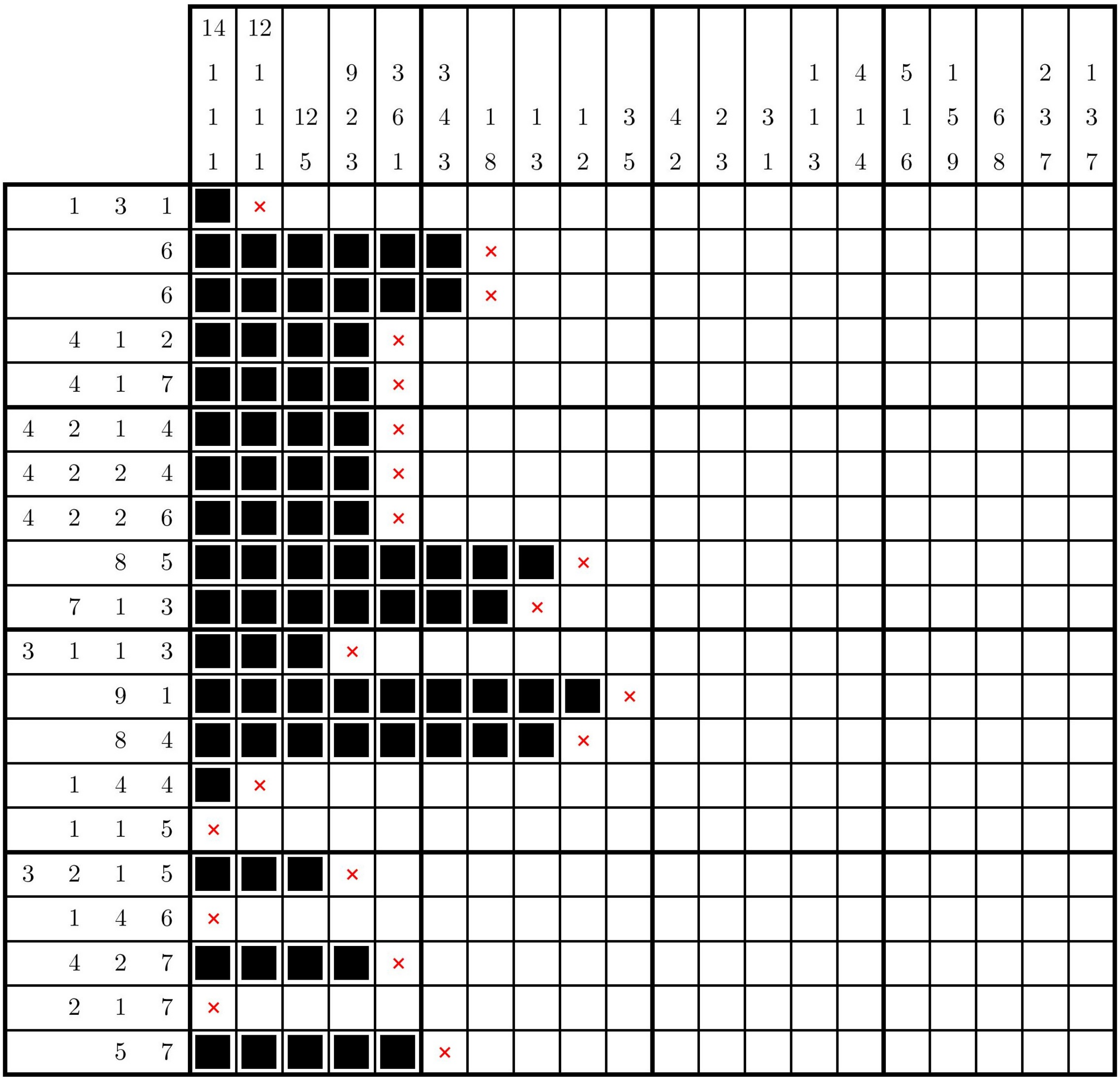
Slika 4.10.10: Zadana logička zagonetka nonogram.

Rješenje. Za početak pogledajmo gdje su najveći brojevi i odredimo, s obzirom na te brojev, polja koja su sigurno crna. U prvom stupcu nalazi se 14 1 1 1, što znači da će ta crna polja zajedno s minimalnim razmacima zauzeti 20 polja. Kako mi upravo imamo zadanih 20 polja, moramo početi s 14 polja odmah od gornjeg kvadratića i sve upisati redom. Odmah nakon toga rješavamo i drugi stupac. Skupina 12 1 1 1 mora početi ili odmah od prvog mjesta u tom stupcu ili od drugog ili od trećeg. Sigurno je da polja od trećeg do dvanaestog moraju biti crna.



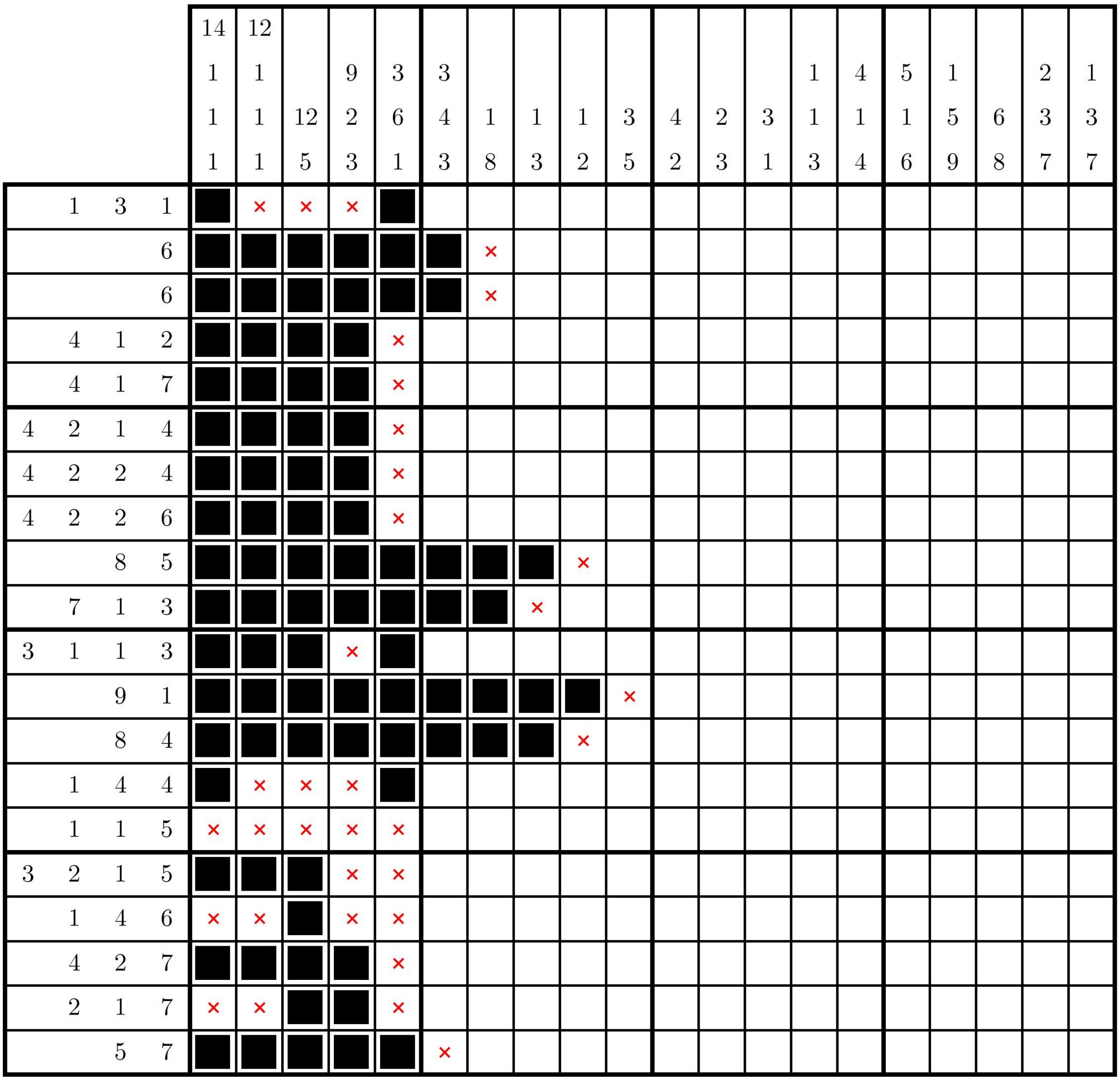
Slika 4.10.11: Prvi korak u rješavanju zadane logičke zagonetke nonogram.

Sada broj 1 u prvom redu kaže da, nakon prvog crnog polja, moramo upisati bar jedno bijelo, tj. $\times$, broj 6 u drugom redu govori da imamo odmah na početku niz od 6 polja, a onda samo praznine, itd. Uzimajući u obzir sve početne brojeve u redovima, dobivamo



Slika 4.10.12: Drugi korak u rješavanju zadane logičke zagonetke nonogram.

Sada, nakon što smo uzeli redove u obzir, gledamo stupce počevši od prvog te popunjavamo ono što je očito.

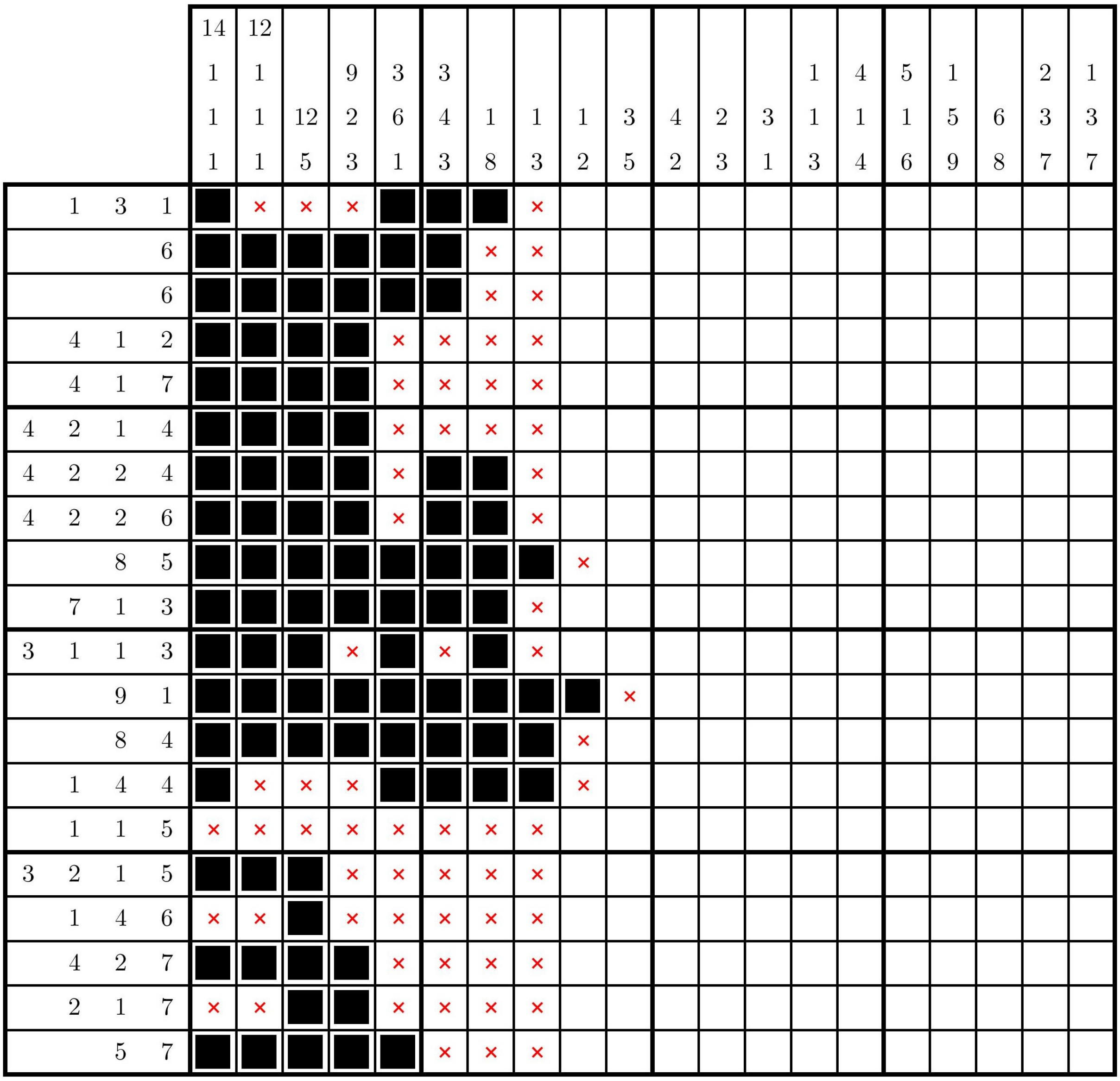


Slika 4.10.13: Treći korak u rješavanju zadane logičke zagonetke nonogram.

Prvih je pet stupaca gotovo. Dalje, za razliku od gore navedenih logičkih zagonetki, rješavanje može postati nešto teže iako smo dosta crnih polja već pronašli.

Sada prvo promotrimo šesti stupac. Za njega su zadana tri broja 3, 4 i 3. No, u njemu već imamo tri dijela crnih polja i jedini način da ostvarimo 3, 4 i 3 jest da odmah na početku postavimo 3 polja (jer u prvom redu imamo nakon jednog crnog polja kojeg smo upisali tri crna polja koja smo upravo započeli) te da od dvaju skupova crnih polja ostvarimo 4 i 3.

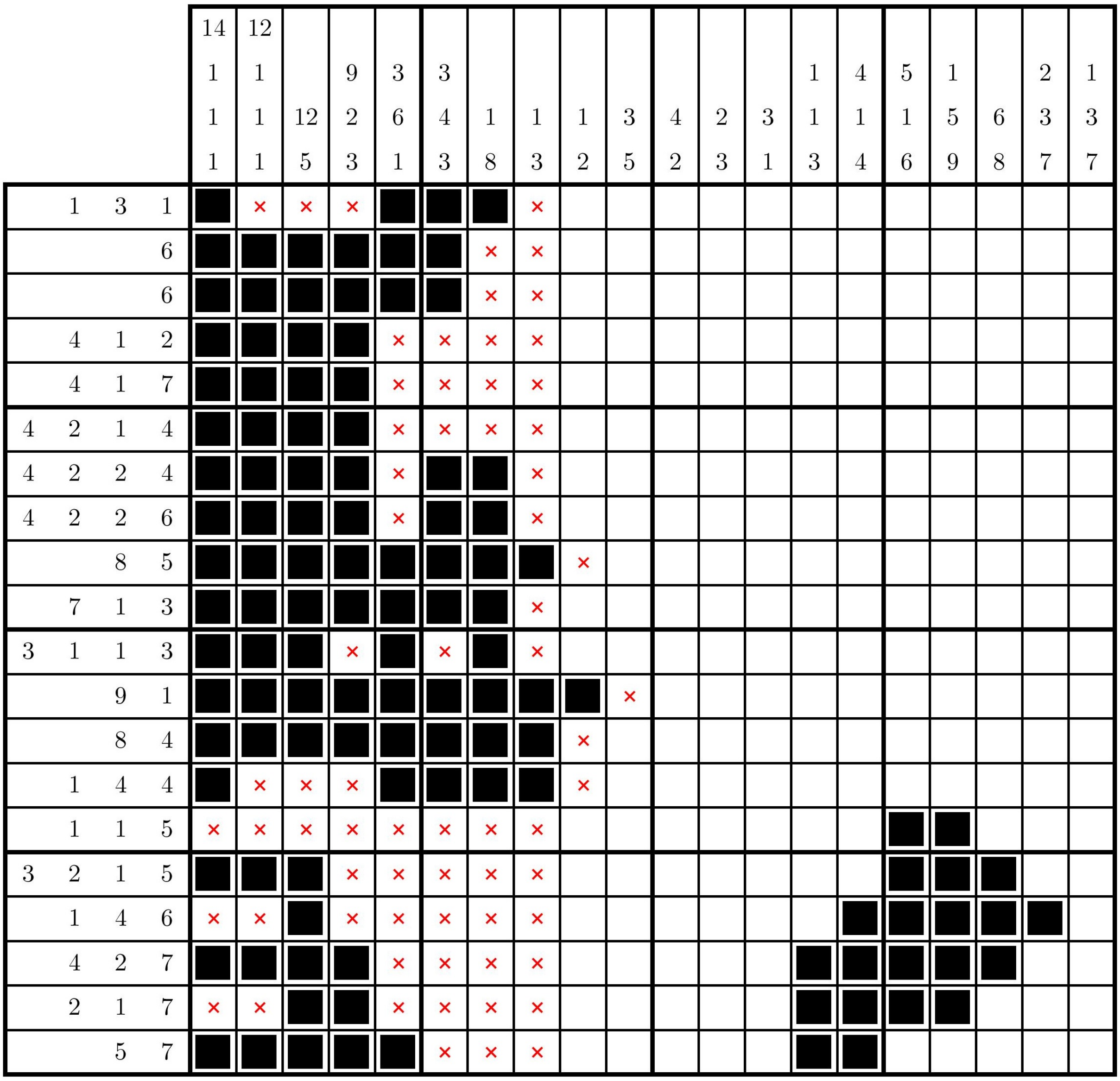
Sedmi je stupac označen s 1 8. Jedno polje mora biti odmah gore (zbog broja 3 u prvom redu), a 8 polja lako dobivamo spajanjem već postojećih crnih polja u tom stupcu i dodavanjem novih s obzirom na brojeve sa strane. Dobivamo situaciju kao na sljedećoj slici.



Slika 4.10.14: Četvrti korak u rješavanju zadane logičke zagonetke nonogram.

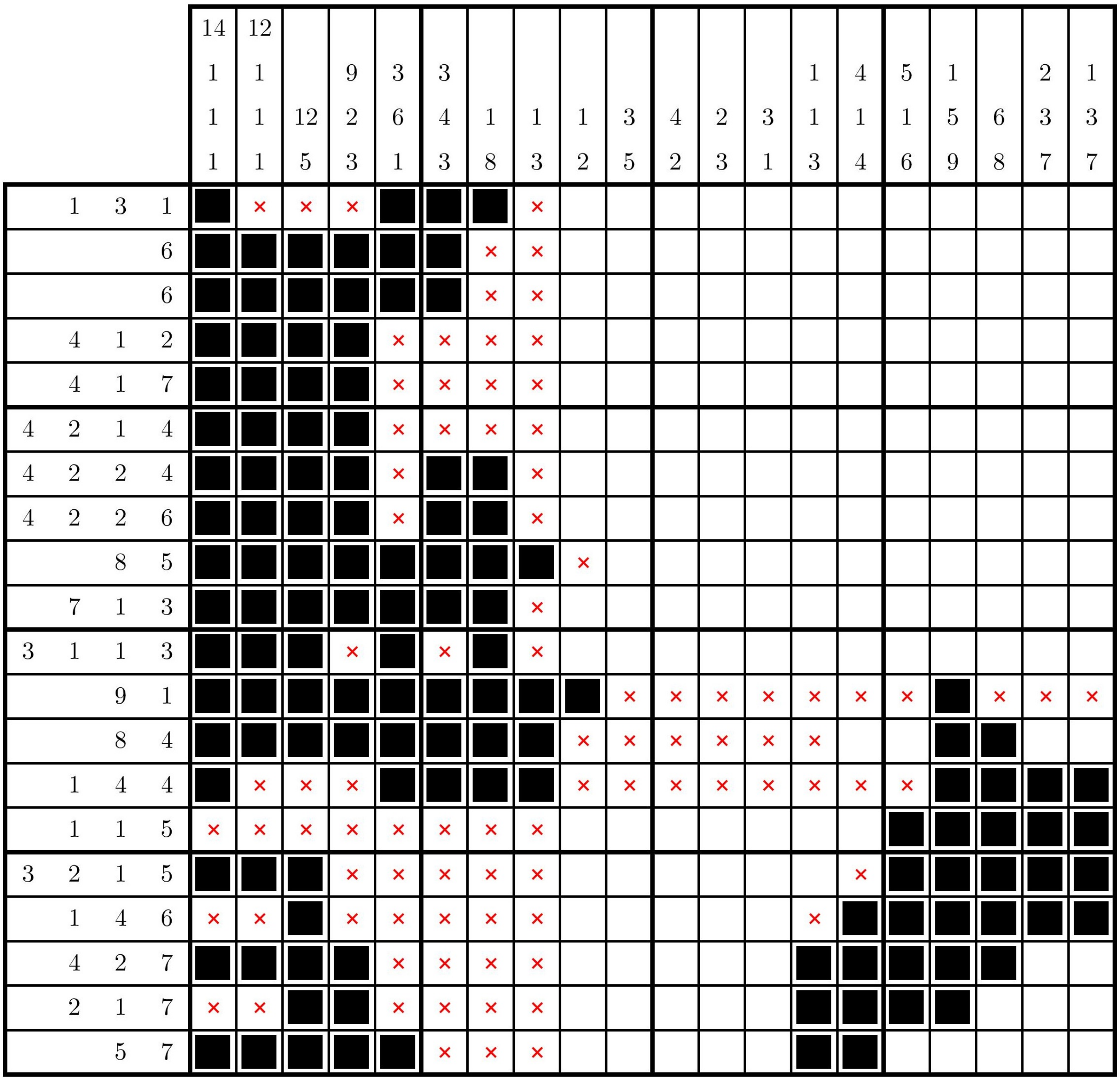
Sada je prvih osam stupaca riješeno. Iako je skoro pola zagonetke gotovo, situacija je sada teža nego na početku.

Promotrimo zadnji red. Pet crnih polja već smo upisali. Sljedećih 7 polja moramo upisati u preostalih 12 praznih polja. Znači da će srednja dva polja od tih 12 polja sigurno biti crna. Iz istog razloga u predzadnjem redu gdje nam je preostalo 1 pa 7 crnih polja, četiri su polja sigurno crna. U zadnjih šest redova moraju biti zacrnjena sljedeća polja:



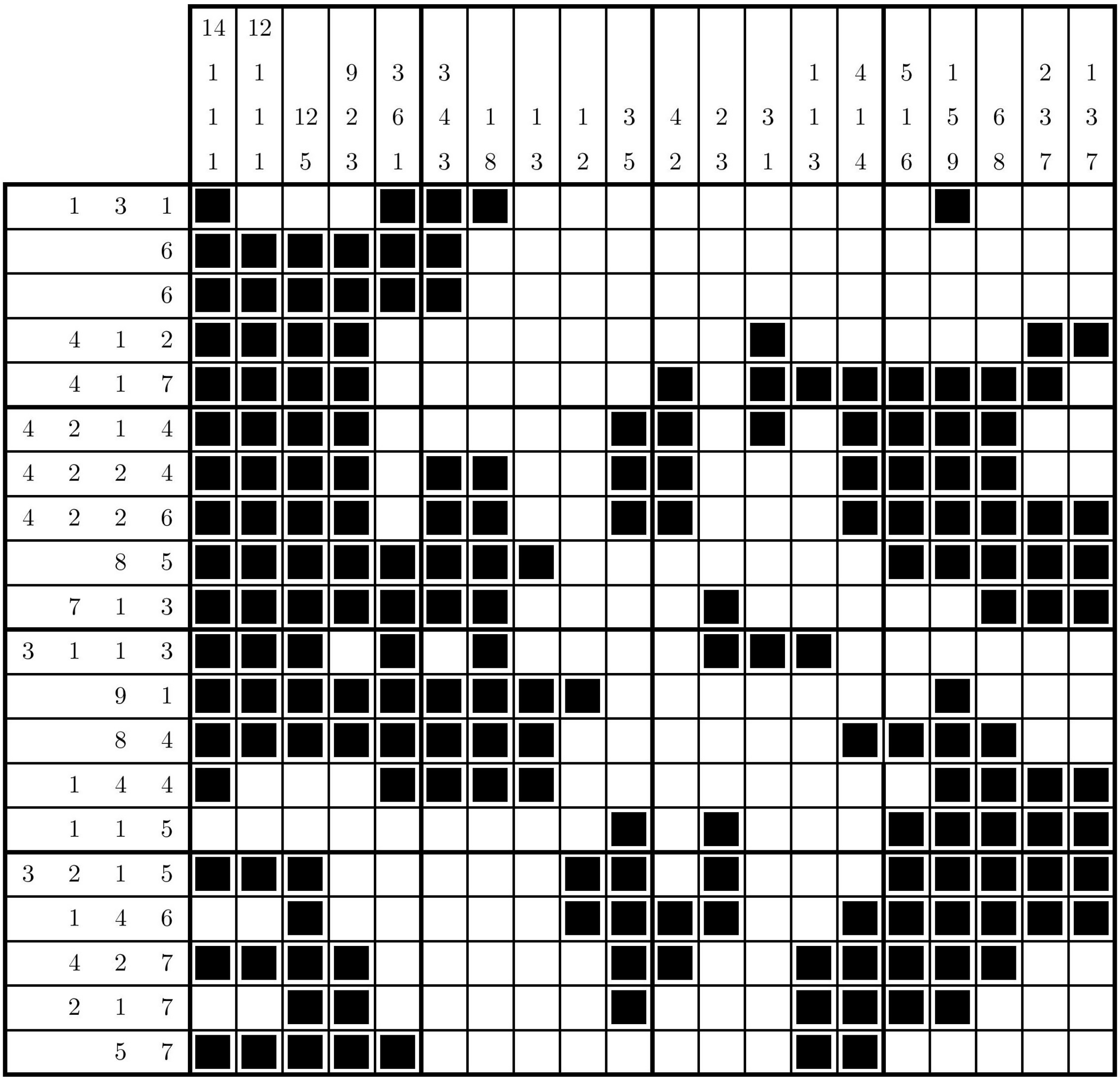
Slika 4.10.15: Peti korak u rješavanju zadane logičke zagonetke nonogram.

Sada, nakon razmatranja po recima, slijedi razmatranje po stupcima u koje smo upravo upisali crna polja, pa ponovo po recima. Dobivamo:



Slika 4.10.16: Šesti korak u rješavanju zadane logičke zagonetke nonogram.

Sada uočavamo 1 4 6 u četvrtom redu odozdo i nakon toga 3 5 u desetom stupcu. Dalje neprestano pregledavamo redove pa stupce kako bismo na kraju dobili



Slika 4.10.17: Konačno rješenje zadane logičke zagonetke nonogram.

Za kraj dodajemo i dva teža (vrlo teška) nonograma koji se ne mogu riješiti uobičajenim jednostavnim trikovima. Čitatelja svakako pozivamo da ih pokuša riješiti. Vjerujemo da će to biti dodatna motivacija za izradu računalnog programa za rješavanje nonograma.

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

(a)

								2		
	1					1		1		1
	2		2	1	1	2	1	1		1
	1	1	2	2	2	1	1	1	1	1
1 3 1										
1 1 1										
1 1										
1 2										
1 2										
1 1 1										
1 1 1										
1 1 1										
1										
3 1										

(b)

Slika 4.10.18: Dva teža nonograma.

Zadaci za vježbu

Zadatak 4.10.1. Riješi nonogram

	2	1	3		4	5	5	2		
	3	4	1	9	2	2	2	2	1	2
2 4										
1 5										
4										
4										
4 2										
4 2										
4 1										
1 1										
5										
6										

Slika 4.10.19: Zadana logička zagonetka nonogram.

Zadatak 4.10.2. Napravi računalni program koji će riješiti cijeli uneseni nonogram, tj. ispuniti sva polja (npr. brute force metodom). Onda napravi program koji će na brz i jednostavan način riješiti bar neka polja zadanog nonograma, tj. koji će raditi na osnovu brzog heurističkog algoritma.

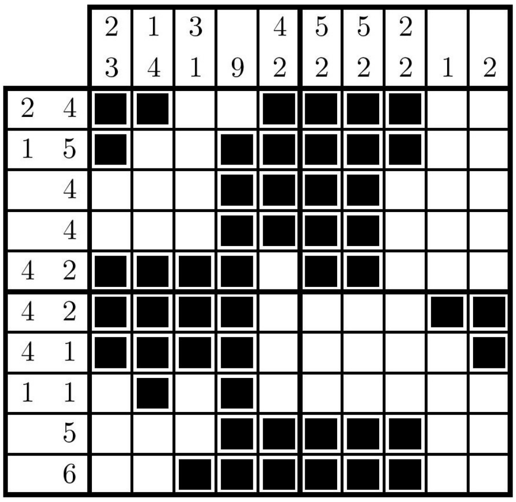
RJEŠENJA

4.10.1. Opišimo rješenje u koracima:

1. Upišimo osam crnih polja u 4. stupcu u kojem je zadan broj 9.
2. Upišimo dva crna polja u zadnji red u kojem je zadan broj 6.
3. Upišimo zadnja dva crna polja u 5. stupac te iznad tih dvaju crnih polja postavimo $\times$.
4. Također, upišimo zadnja dva crna polja u 6. stupac za kojeg je zadano 5, 2 te iznad ta dva crna polja postavimo $\times$.
5. U zadnja tri polja trećeg i četvrtog reda koji su zadani s brojem 4 upišimo tri znaka $\times$.

   Dalje neprestanim istraživanjem po redovima pa po stupcima, s obzirom na već upisana polja, lako dobivamo konačno rješenje.

Konačno je rješenje



Slika 4.10.20: Konačno rješenje zadane logičke zagonetke nonogram.

Prilozi

Prilog 1: Prijedlog izvedbe kolegija po nastavnim satima

Predavanja po blokovima od dvaju školskih sati	Vježbe po blokovima od dva školska sata
1. **Uvod u kolegij (predstavljanje nastavnika i kolegija)** Dati sadržaj kolegija i prokomentirati koja su gradiva važnija, teža ili više vezana uz pismeni ili usmeni ispit. Dati kod svakog poglavlja literaturu za to poglavlje (ili, druga opcija, na kraju svakog bloka od dvaju ili četiriju školskih sati dati literaturu za na tom bloku obrađeno gradivo). Dogovoriti se koji su uvjeti polaganja ispita i obaveznih dolazaka na predavanja i vježbe. **Trajanje: 10 minuta** **Tradicionalna logika** Izložiti kratko osnove povijesti logike te važnost Grčke i Aristotela. Povezati logiku, znanstveno razmišljanje i matematiku na primjeru kategorija, podjele pojmova i sudova i zaključaka. Obraditi definiciju (viši rodni pojam i vrsna razlika) i razliku induktivnog i deduktivnog zaključka. **Obavezno:** početke logike vezati uz početke matematike i znanosti općenito zbog sustavnosti, analize i sinteze znanosti. **Trajanje: 80 minuta** **Ukupno: 90 minuta**	1. **Zadaci s definicijom i kategoričkim silogizmom** Obraditi primjere definicija. Rješavati kategorički silogizam pomoću rečenica iz svakodnevnog života te pomoću slike, tj. dijagrama odnosa subjekta, predikata i raspodijeljenog pojma. **Trajanje: 45 minuta** **Šah** Dati "definiciju" šaha, tj. objasniti u što kraćem naputku sva pravila šaha (kao nastavak prethodnog gradiva o definiciji). Napraviti zadatke sa šahom iz poglavlja 4. Za programerske smjerove zadati programerske zadatke s kretanjem figura u šahu te slobodnim i napadnutim poljima. Prokomentirati uvjete napada raznih figura. **Trajanje: 45 minuta** **Ukupno: 90 minuta**

Predavanja po blokovima od dvaju školskih sati	Vježbe po blokovima od dva školska sata
2. **Matematička logika** Dati uvod o važnosti matematike i logike kao "sigurnih" i nepogrešivih znanosti čije alate koriste i ostale znanosti i važnija istraživanja. Prokomentirati vrste logika. Definirati alfabet, riječ i formulu logike sudova. Definirati interpretaciju varijabli i formule. Detaljno opravdati definiciju interpretacije veznika *i*, *ili*, *kondicionala*, *bikondicionala* i *negacije*. (U početnim nastavnim satima ne pisati npr. $A = 0$, nego $I(A) = 0$.) **Obavezno:** Polazeći od alfabeta, definirati strogo sve nove pojmove, sve do interpretacije formule. **Ukupno: 90 minuta**	2. **Matematička logika** Vježbati ispitivanje formule te zadatke 1.2.1, 1.2.2, 1.2.3, 1.2.5, 1.2.7, 1.2.8 i 1.2.9. **Trajanje: 60 minuta** **Rekurzivne logičke zagonetke** **Trajanje: 30 minuta** **Ukupno 90: minuta**
3. **Konjunktivna i disjunktivna normalna forma** Definirati i dati primjere za literal, elementaru konjunkciju i disjunkciju, KNF i DNF. Pokazati kako se nalaze KNF i DNF zadane formule i obrazložiti postupke. **Veznici** Dati definiciju baze veznika i paralelu s bazom vektorskog prostora. Uvesti Lukasiewiczevu i Shefferovu operaciju. Detaljno obraditi De Morganove formule. Dati primjere izražavanja jednog veznika pomoću ostalih zadanih. Dati primjer sudovne jednadžbe (npr. primjer 1.4.1 na str. 47.) i detaljno ju riješiti. **Ukupno: 90 minuta**	3. **Konjunktivna i disjunktivna normalna forma** Vježbati traženje KNF-a i DNF-a. Vježbati izražavanje zadanog veznika pomoću zadanog skupa veznika. **Trajanje: 60 minuta** **Logička zagonetka rasvjeta** Prokomentirati i zadati kao programerski zadatak implementaciju ove (i ostalih zagonetki tipa križaljka) na računalu (početak programa, tj. samo oblikovanje križaljke na računalu). **Trajanje: 30 minuta** **Ukupno: 90 minuta**

Predavanja po blokovima od dvaju školskih sati	Vježbe po blokovima od dva školska sata
4. **Prirodna dedukcija** Detaljno objasniti važnost tautologija i sustava za dobivanje tautologija. Dati objašnjenja i primjere teorema, lema, korolara, propozicija i dokaza. Navesti i prokomentirati svako od pravila prirodne dedukcije. Riješiti bar dva primjera dokaza koristeći samo prirodna pravila i bar dva s hipotetskim pravilima. Dati i detaljno obrazložiti formalnu definiciju teorema i dokaza. Obraditi teoreme konzistentnosti, adekvatnosti i potpunosti sustava prirodne dedukcije. **Obavezno:** Obraditi formalni dokaz i prokomentirati matematiku i logiku kao "sigurne" znanosti. **Ukupno: 90 minuta**	4. **Prirodna dedukcija** Vježbati dokazivanje u sustavu prirodne dedukcije. **Trajanje: 60 minuta** **Logička zagonetka neboderi** Prokomentirati i zadati za zadaću ili kraći seminarski rad konstrukciju programa za rješavanje nebodera. Osvrnuti se na sigurni upis elementa reda i stupca ako je moguće upisati samo jedan broj. **Trajanje: 30 minuta** **Ukupno: 90 minuta**
5. **Osnove teorije skupova** Dati uvod o skupu i elementu zajedno s povijesnim pregledom teorije skupova. Obraditi skup, element i primjere skupova. Definirati i kroz primjere obraditi podskup, pravi podskup, jednakost skupova, partitivni skup i prazan skup. Definirati i na primjeru pokazati operacije sa skupovima. **Ukupno: 90 minuta**	5. **Osnove teorije skupova** Rješavati zadatke iz osnova teorije skupova (obavezno zadatke 2.1.1, 2.1.2 i 2.1.3). Uvesti Vennove dijagrame za jedan, dva i tri skupa i koristiti ih u zadacima. Za domaću zadaću dati konstrukciju Vennovog dijagrama za četiri skupa. Pokazati zašto se ne može prikazati pomoću kružnica. **Obavezno:** Detaljno obraditi zadatke 2.2.1, 2.2.2, 2.2.3 i 2.2.4. **Ukupno: 90 minuta**

Predavanja po blokovima od dvaju školskih sati	Vježbe po blokovima od dva školska sata
6. **Relacije** Redom obraditi Kartezijev produkt $A \times B$, A^2, relaciju i svojstva relacija (refleksivnost, irefleksivnost, simetričnost, antisimetričnost, tranzitivnost i linearnost). Dati primjere relacija među kojima obavezno i relacije koje su prazan skup te na tome ponoviti tablicu implikacije. **Ukupno: 90 minuta**	6. **Ispitivanje relacija** Vježbati ispitivanje relacije. **Trajanje: 45 minuta** **Logička zagonetka integram** Obraditi logičku zagonetku integram i povezati ju s relacijama. Prokomentirati i dati kao npr. seminarski rad zadatak s računalnim programom koji će na osnovu unesenih poznatih podataka u poljima križaljke integrama ispisati ostale podatke koje je moguće iz njih dobiti. **Trajanje: 45 minuta** **Ukupno: 90 minuta**
7. **Klase ekvivalencije** Ponoviti na jednom primjeru svojstva relacija. Dati primjer i definiciju particije skupa. Definirati relaciju ekvivalencije i na primjerima pokazati kako svaka particija skupa prirodno generira relaciju ekvivalencije na tom skupu i obrnuto. Definirati klase elemenata, klase ekvivalencije i kvocijentni skup. Dati primjer kako relacija uređaja poreda elemente nekog (konačnog) skupa. Definirati relaciju uređaja, minimum, minimalni element, maksimum i maksimalni element. Na primjerima pokazati traženje tih elemenata. Definirati lanac u skupu s obzirom na relaciju uređaja. **Ukupno: 90 minuta**	7. **Ispitivanje relacija i traženje kvocijentnog skupa** Vježbati ispitivanje relacija koje su zadane tako da se pokaže da su to ili relacije ekvivalencije ili relacije uređaja. U slučaju relacije ekvivalencije, odrediti kvocijentni skup, a u slučaju relacije uređaja, odrediti minimume, maksimume, minimalne elemente i maksimalne elemente. **Ukupno: 90 minuta**

Predavanja po blokovima od dvaju školskih sati	Vježbe po blokovima od dva školska sata
8. **Kardinalni brojevi** Definirati funkciju, injekciju, surjekciju i bijekciju i napraviti primjere na konačnim skupovima. Raspraviti o načinima klasifikacije skupova (kako u sve skupove uvesti neki "red") (početak cjeline 2.4.). Definirati ekvipotentnost skupova i napraviti primjere. Uvesti klase ekvivalencije i kardinalne brojeve. Definirati 1, 2, 3, ... Napraviti primjere od 2.4.3 do 2.4.7. Objasniti bijektivnost $\mathbb{N}$, $2\mathbb{N}$, $\mathbb{Z}$ i $\mathbb{Q}$. U sklopu primjera 2.4.4, detaljno raspraviti o odnosu prirodnih i parnih brojeva i pokazati razliku u zakonitostima u konačnim i beskonačnim skupovima. **Ukupno: 90 minuta**	8. **Bijektivnost skupova** Zadavati po dva skupa i na njima pokušavati napraviti injekcije, surjekcije i bijekcije. (Svakako prvo detaljno obraditi konačne skupove.) Vježbati zbrajanje i množenje manjih brojeva i uspoređivanje skupova. **Trajanje: 60 minuta** **Logička zagonetka sudoku** Obraditi logičku zagonetku sudoku. Objasniti na konkretnom primjeru i prokomentirati programsku implementaciju "backtracking" algoritma. **Trajanje: 30 minuta** **Ukupno: 90 minuta**
9. **Kardinalni brojevi** Pokazati da $\mathbb{R}$ nije prebrojiv, tj. iskazati i skicirati dokaz Cantorovog teorema. Definirati zbrajanje i množenje kardinalnih brojeva te pokazati kako se kardinalni brojevi uspoređuju, tj. kako se uvodi relacija $\leq$ na klasu svih kardinalnih brojeva. Pročitati i prokomentirati neke dijelove knjige Priče o skupovima (*N. J. Vilenkin, Priče o skupovima, Školska knjiga, Zagreb, 1975.*). **Ukupno: 90 minuta**	9. **Zbrajanje i množenje kardinalnih brojeva** Vježbati zbrajanje i množenje manjih brojeva i uspoređivanje skupova. **Trajanje: 45 minuta** **Logička zagonetka kakuro** Obraditi logičku zagonetku kakuro. Prokomentirati programsku implementacije traženje broja presjekom vodoravnih i okomitih mogućnosi i implementaciju "backtracking" algoritma. **Trajanje: 45 minuta** **Ukupno: 90 minuta**

Predavanja po blokovima od dvaju školskih sati	Vježbe po blokovima od dva školska sata
10. **Teorija brojeva. Djeljivost. Prosti brojevi.** Objasniti što je teorija brojeva i čime se bavi. Dati definiciju djeljivosti i osnovna svojstva relacije “biti djeljiv s/sa”. Definirati proste brojeve , navesti ih sve do 100 i dati osnovna svojstva i osnovne teoreme. Hipoteze objasniti detaljno i zadati ih za domaći uradak na računalu. Dati osnovni teorem aritmetike i objasniti zapis u bazi prostih brojeva. Heurističkom metodom izvesti formulu za broj djelitelja prirodnog broja. **Ukupno: 90 minuta**	10. **Prosti brojevi i djeljivost** Navesti pravila djeljivosti sa svim brojevima od 2 do 12. Objasniti pravila djeljivosti s nekim većim brojevima. Zadati veliki prirodni broj i ispitivati je li prost. Rješavati zadatke s djeljivosti. **Trajanje: 45 minuta** **Što mogu 1, 2, 3, 4 i 5?** Podijeliti studente u grupe i organizirati natjecanje u prikazu prirodnih brojeva pomoću brojeva 1, 2, 3, 4 i 5 (poglavlje 4.9.). Rješavati redom prikaz brojeva od 1 na dalje pomoću 1, 2, 3 i 4 (poglavlje 4.9.). **Trajanje: 45 minuta** **Ukupno: 90 minuta**
11. **Djeljivost. Najveća zajednička mjera (nzm) i najmanji zajednički višekratnik (nzv).** Dati definiciju i načine traženja nzm-a i nzv. Objasniti i na brojevima i polinomima vježbati Euklidov algoritam za traženje nzm. Dati i provježbati na primjeru Osnovni teorem o djeljivosti cijelog broja prirodnim brojem. **Ukupno: 90 minuta**	11. **Prosti brojevi i djeljivost** Zadaci s prostim brojevima i s djeljivošću te s nzm-om i nzv-om. **Trajanje: 45 minuta** **Logička zagonetka mostovi** Na primjeru riješiti lakšu zagonetku mostovi. Zadati pravila rješavanja zagonetke mostovi. Raspraviti o načinima implementacije otoka i veza među otocima na računalu. **Trajanje: 45 minuta** **Ukupno: 90 minuta**

Predavanja po blokovima od dvaju školskih sati	Vježbe po blokovima od dva školska sata
12. **Primjena djeljivosti u zadacima s matematičkih natjecanja** Vježbati zadatke s matematičkih natjecanja osnovnih i srednjih škola iz područja teorije brojeva koji su vezani uz djeljivost. **Ukupno: 90 minuta**	12. **Primjena djeljivosti u zadacima s matematičkih natjecanja** Vježbati zadatke s matematičkih natjecanja osnovnih i srednjih škola iz područja teorije brojeva koji su vezani uz djeljivost. **Ukupno: 90 minuta**
13. **Kongruencije** Objasniti na primjerima računalnu funkciju mod (funkciju %). Dati definiciju kongruentnosti i što više primjera s pozitivnim i negativnim brojevima. Rješavati jednadžbe $ax \equiv b \pmod{c}$ i $a \equiv b \pmod{x}$ za neke cijele brojeve a, b i c. Dati svojstva kongruencija i konkretne primjere za svako od devet svojstava. Sada ponovo riješiti jednadžbe $ax \equiv b \pmod{c}$ i $a \equiv b \pmod{x}$ za neke cijele brojeve a, b i c. **Ukupno: 90 minuta**	13. **Kongruencije** Rješavati zadatke s kongruencijama tipa: - odredi zadnju znamenku, - odredi zadnje dvije znamenke ili zadnje tri znamenke broja, - odredi ostatak pri dijeljenju broja s brojem (npr. odredi ostatak pri dijeljenju broja $22 \cdot 33^{44} - 55^{66} \cdot 77^{88}$ s 9). Svakako napraviti zadatak: Odredi zadnje dvije znamenke broja 2^{2222}. **Trajanje: 45 minuta** **Logička ispunjaljka** Na primjeru riješiti lakšu logičku ispunjaljku. Dati pravila rješavanja logičke ispunjaljke. Raspraviti o načinima implementacije logičke ispunjaljke na računalu i za domaći uradak (seminar) zadati kreiranje programa za rješavanje logičke ispunjaljke računalom. **Trajanje: 45 minuta** **Ukupno: 90 minuta**

Predavanja po blokovima od dvaju školskih sati	Vježbe po blokovima od dva školska sata
14. **Kongruencije. Eulerov teorem i mali Fermatov teorem.** Obraditi Eulerovu funkciju. Izložiti Eulerov teorem o kongruencijama i mali Fermatov teorem te ih na primjerima naučiti upotrebljavati. **Ukupno: 90 minuta**	14. **Kongruencije. Eulerov teorem i mali Fermatov teorem.** Rješavati razne zadatke s kongruencijama, posebno zadatke koji se rješavaju primjenom Eulerovog teorema i malog Fermatovog teorema. **Ukupno: 90 minuta**
15. **Diofantske jednadžbe** Izložiti osnove i kratku povijest diofantskih jednadžbi. Proraditi redom: - Nelinearne diofantske jednadžbe (bar metodu rastava na faktore), - Pitagorine trojke, - Fermatove trojke, - Bealovu hipotezu, - linearne diofantske jednadžbe (obraditi linearne diofantske jednadžbe s dvjema nepoznanicama metodom pogađanja jednog rješenja i gotovom formulom te Eulerovom metodom). **Ukupno: 90 minuta**	15. **Diofantske jednadžbe** Rješavati razne zadatke iz područja Diofantskih jednadžbi, posebno zadatke s matematičkih natjecanja osnovnih i srednjih škola u čijem se rješavanju koriste algoritmi za rješavanje diofantskih jednadžbi. **Ukupno: 90 minuta**

Kazalo

A
afirmativni sud, 5
alfabet logike sudova, 16
antisimetrična relacija, 99
antitautologija, 21
atomarna formula, 65

B
baza veznika, 42
bijekcija, 69
bikondicional, 16
binarna relacija, 96

D
De Morganov zakon, 24, 42
deduktivni zaključak, 8
definicija, 6
diofantska jednadžba, 173
disjunkcija, 16
disjunktivna normalna forma, 39
disjunktivni sud, 6
disjunktni skupovi, 80
djelitelj, 128
domena, 66
dvojna negacija, 24
dvopogodba, 16

E
ekvipotentni skupovi, 118
ekvivalencija, 16
elementarna disjunkcija, 39
elementarna konjunkcija, 39
Euklidov algoritam, 136
Eulerov teorem o kongruencijama, 170
Eulerova funkcija, 169

F
fuzzy logika, 16

G
Goldbachova hipoteza, 131

H
hipotetički sud, 6

I
implikacija, 16
individualne varijable, 64
induktivan zaključak, 7
induktivna definicija, 17
injekcija, 69
integram, 231
interpretacija, 18, 66
irefleksivna relacija, 99
ispunjiva formula, 21

K
kakuro, 223
Kartezijev produkt, 79
kategorički silogizam, 8
kategorički sud, 6
klasa ekvivalencije, 103
komplement, 79
konačan skup, 122
kondicional, 16
kongruencije, 157
konjunkcija, 16
konjunktivna normalna forma, 39
konkatenacija, 17
konkluzija, 7
kvantifikator egzistencije, 64
kvocijentni skup, 106

L
limitativni sud, 5
linearna diofantska jednadžba, 177
linearna relacija, 99
literal, 39
logika sudova, 15
logička ispunjaljka, 255
logičke slike, 255
logički ekvivalentne formule, 22
Lukasiewiczeva operacija, 44

M
maksimalni element, 109
maksimum, 108
mali Fermatov teorem, 170

medijalni pojam, 8
minimalni element, 109
minimum, 108
mjesnost relacije, 64
modalna logika, 16
model, 67
modul, 158
mostovi, 215

N

nadskup, 77
najmanji zajednički višekratnik, 137
najveći zajednički djelitelj, 135
neboderi, 207
negacija, 16
negativni sud, 5
neproturječnost, 24
nonogram, 255
nosač, 66

O

oboriva formula, 21
osnovni teorem aritmetike, 131

P

parcijalna interpretacija, 19
parcijalni uređaj, 78, 107
particija, 103
partikularni sud, 5
partikularno rješenje diofantske jednadžbe, 178
partitivni skup, 78
Peirceova strijela, 44
Pitagorin teorem, 54
Pitagorina trojka, 175
podskup, 77
pogodba, 16
pojam, 5
pomoćni simboli, 16
potpun skup veznika, 42
pravi podskup, 77
prazan skup, 78
prebrojiv skup, 123
predikat, 8
predikatna logika, 61
premisa, 7
presjek, 79
princip isključenja trećeg, 24
propozicionalna logika, 15
propozicionalne varijable, 16
prost broj, 130
prosti brojevi blizanci, 130

Q

Quineov bodež, 44

R

rasvjeta, 198
razredba, 103
refleksivna relacija, 98
refleksivnost bikondicionala, 24
refleksivnost kondicionala, 24
rekurzivne logičke igre, 193
relacija ekvivalencije, 102
riječ, 17, 64

S

Shefferova operacija, 43
signatura, 64
simetrična razlika, 79
simetrična relacija, 99
singularni sud, 5
složen broj, 130
subjekt, 8
sud, 5
sudoku, 243
surjekcija, 69
sustav prirodne dedukcije, 55
svijet, 66

T

tautologija, 21
temeljna Pitagorina trojka, 175
teorem adekvatnosti za sustav prirodne dedukcije, 59
teorem konzistentnosti za sustav prirodne dedukcije, 59
teorem o dijeljenju s ostatkom, 137
teorem potpunosti za sustav prirodne dedukcije, 59
teorem sustava prirodne dedukcije, 59
teorija brojeva, 127
term, 65
tornjevi, 207
tranzitivna relacija, 99

U

unija, 79

univerzalni kvantifikator, 64
univerzalni skup, 79
univerzalni sud, 5
univerzum, 66

V

valjana formula, 21
valuacija, 62, 66
varijable, 64
Vennov dijagram, 84
veznici, 16
višekratnik, 128

Z

zaključak, 7