Elementarna matematika 1

Vježbe

Akademska godina 2024./2025.

Predgovor

Ova skripta nastala je tijekom akademske godine 2024./2025. kao nadopuna vježbama iz kolegija Elementarna matematika 1. Sadrži važne definicije i iskaze teorema obrađene na predavanjima te zadatke koji će se rješavati na vježbama. Svrha skripte nije da zamijeni redovito pohađanje i aktivno praćenje vježbi, već da studentima omogući da sami pogledaju nešto što na nastavi nisu stigli zapisati ili žele ponoviti.

Kako bi imali najviše koristi od nastave i ove skripte, preporuka studentima je da barem neke zadatake pokušaju samostalno riješiti *prije* dolaska na vježbe. Na kraju svakog poglavlja nalaze se upute za rješavanje nekih zadataka te rješenja. Napominjemo da je čitanje rješenja zadataka gotovo beskorisno ukoliko prije toga niste dobro razmislili o zadatku i pokušali ga riješiti, makar i bezuspješno.

Budući da je skripta tijekom cijelog semestra u procesu nastajanja, gotovo sigurno će sadržavati gramatičke, sintaksne ili matematičke greške. Bit ćemo iznimno zahvalni svakome tko nam ukaže na neku grešku ili sumnju na istu.

Posljednja izmjena napravljena je 22. siječnja 2025.

Matea Čelar, Ivan Novak i Ivan Puljiz

Sadržaj

Poglavlje 1

Logika

1.1 Logički veznici

Definicija 1.1. Sud je svaka izjavna (matematička) rečenica (zapisana riječima ili simbolima) za koju se može utvrditi je li istinita ili lažna.

Primjer 1.2. Promotrimo sljedeće izjave:

1. Izjava *"Broj* 13 *je jednak broju* 7*"* je sud, i to lažan.
2. Izjava "$1+1+1=2$" je sud, i to lažan.
3. Izjava "$x+1=2$" nije sud, jer nije moguće jednoznačno utvrditi je li istint ili lažan. Za $x=1$ to bi bio istinit sud, a za npr. $x=2$ to bi bio lažan sud.
4. Izjava *"Za sve prirodne brojeve* x *vrijedi* $x+0=x$*"* je sud, i to istinit.
5. Izjava *"Svaki polinom stupnja većeg ili jednakog* 1 *ima nultočku u skupu kompleksnih brojeva"* jest sud. Iako u ovom trenutku nemamo dokaz te tvrdnje, jasno je da se njena istinitost može jednoznačno utvrditi. Tvdrnje za koje nemamo dokaz nazivamo **hipotezama**.

   Dokaz ove tvrdnje napravit će se na trećoj godini studija, na kolegiju *Kompleksna analiza*. Dakle, ovaj sud je istinit.
6. Izjava *"Ova izjava je lažna"* nije sud, jer nije moguće jednoznačno utvrditi njenu istinitost. Kad bi ona bila istinita, onda bi vrijedilo *"Ova izjava je lažna"*, tj. izjava bi bila lažna. Slično, kad bi ta izjava bila lažna, onda ne bi vrijedilo *"Ova izjava je lažna"*, tj. izjava bi bila istinita. Sud ne može istovremeno biti i istinit i lažan, pa ova izjava nije sud.

Od jednostavnih sudova gradimo složene sudove pomoću **logičkih veznika**. Radi kraćeg zapisa, sudove pritom simbolički označavamo velikim slovima, npr.

$$A \equiv \text{“}1+2=3\text{”}, \qquad B \equiv \text{“}3^2=9\text{”}.$$

Definicija 1.3. (Logički veznici)

- **Negacija** suda A je sud koji je istinit točno onda kada je sud A lažan. Negaciju suda A označavamo sa $\neg A$ ili $\overline{A}$ te čitamo *“ne A”* ili *“nije A”*.

A	$\neg A$
1	0
0	1

- **Konjunkcija** sudova A i B je složeni sud koji je istinit točno onda kada su istiniti i sud A i sud B. Konjunkciju sudova A i B označavamo sa $A \wedge B$, $A\&B$ ili $A \cdot B$, te čitamo *“A i B”*.

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

- **Disjunkcija** sudova A i B je složeni sud koji je lažan točno onda kada su lažni i sud A i sud B. Disjunkciju sudova A i B označavamo sa $A \vee B$, $A \mid B$ ili $A+B$, te čitamo *“A ili B”*.

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

- **Implikacija** sudova A i B je složeni sud koji je lažan samo onda kada je sud A istinit, a sud B lažan. Implikaciju sudova A i B označavamo sa $A \Rightarrow B$ ili $A \rightarrow B$, te čitamo *“A povlači B”*, *‘‘A implicira B”*, *“Ako A, onda B”*, *“Iz A slijedi B”*, *“B je **nužan uvjet** za A”* ili *“A je **dovoljan uvjet** za B”*.

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

- **Ekvivalencija** sudova A i B je složeni sud koji je istinit točno onda kada su i sud A i sud B oba istiniti ili oba lažni. Ekvivalenciju sudova A i B označavamo sa $A \Leftrightarrow B$ ili $A \leftrightarrow B$, te čitamo *“A vrijedi ako i samo ako vrijedi B”* (kraći zapis *“A akko B”*) ili *“A je **nužan i dovoljan uvjet** za B”*.

A	B	$A \Leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

Zadatak 1.1 Neka je $A \equiv 2^3 = 8$ i $B \equiv 7 > 5$. Zapišite sljedeće sudove:

(a) $A \Rightarrow \neg B$

(b) $A \vee \neg B$

(c) $\neg A \Leftrightarrow B$

(d) $\neg(\neg A)$

(e) $(A \wedge \neg B) \Rightarrow A$

Zadatak 1.2 Odredite istinitost sljedećih sudova:

(a) *"Ako je* $3+2=7$*, onda je* $4+4=8$*."*

(b) *"Nije istina da je* $6^2 = 32$ *ako i samo ako je* $4 \geq 10$*."*

(c) *"Nije istina da je* $\log_2 16 = 3$ *ili* $\cos 0 = 1$*."*

(d) *"Nije istina da, ako je* 10 *djeljiv s* 3*, onda je* $\sqrt{9} = 4$*."*

Napomena 1.4. Uvodimo prioritet logičkih veznika:

1. Najviši prioritet ima negacija.
2. Srednji prioritet ima konjunkcija.
3. Najniži prioritet imaju disjunkcija, implikacija i ekvivalencija. Ta tri veznika imaju jednak prioritet.

Definicija 1.5. Kažemo da je složeni sud **tautologija** ako se njegov pripadni stupac u tablici istinitosti sastoji samo od oznaka 1.

Definicija 1.6. Kažemo da su složeni sudovi A i B **semantički jednaki** ili **logički ekvivalentni** ako i samo ako je sud $A \Leftrightarrow B$ tautologija, tj. ako sudovi A i B imaju identične stupce u tablici istinitosti. Tada pišemo $A \equiv B$.

Oznakom $\top$ označavamo tautologiju, tj. sud koji je uvijek istinit. Oznakom $\bot$ označavamo sud čija negacija je tautologija, tj. sud koji je uvijek lažan.

Zadatak 1.3 Provjerite zakone **asocijativnosti** i **distributivnosti** za konjunkciju i disjunkciju:

(a) $A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C$

(b) $A \vee (B \vee C) \equiv (A \vee B) \vee C$

(c) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

(d) $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$

Zadatak 1.4 Dokažite da su sljedeći složeni sudovi tautologije.

(a) $(A \wedge (A \Rightarrow B)) \Rightarrow B$

(b) $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$

(c) $((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$

Negiranje složenih sudova

Primjer 1.7.

1. Negacija suda *"Broj* 18 *je djeljiv s* 3 *i s* 4*"* je *"Broj* 18 *nije djeljiv s* 3 *ili nije djeljiv s* 4*"*. Uz oznake $A \equiv$ *"Broj* 18 *je djeljiv s* 3*"* i $B \equiv$ *"Broj* 18 *je djeljiv s* 4*"* vidimo da je

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

2. Negacija suda *"Broj* 9 *je prost ili je paran"* je *"Broj* 9 *nije prost i nije paran"*. Uz oznake $A \equiv$ *"Broj* 9 *je prost"* i $B \equiv$ *"Broj* 9 *je paran"* vidimo da je

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

3. Negacija suda *"Ako je* 6^2 *djeljiv s* 4*, onda je* 6 *djeljiv s* 4*"* je *"*6^2 *je djeljiv s* 4 *i* 6 *nije djeljiv s* 4*"*. Uz oznake $A \equiv$ *"*6^2 *je djeljiv s* 4*"* i $B \equiv$ *"*6 *je djeljiv s* 4*"* vidimo da je

$$\neg(A \Rightarrow B) \equiv A \wedge \neg B.$$

Zadatak 1.5 Dokažite sljedeće identitete:

(a) $\neg(\neg A) \equiv A$

(b) $A \Rightarrow B \equiv \neg A \vee B$

(c) $\neg(A \wedge B) \equiv \neg A \vee \neg B$

(d) $\neg(A \vee B) \equiv \neg A \wedge \neg B$

(e) $\neg(A \Rightarrow B) \equiv A \wedge \neg B$

(f) $\neg(A \Leftrightarrow B) \equiv (A \wedge \neg B) \vee (\neg A \wedge B)$

Definicija 1.8. Neka je $A \Rightarrow B$ sud. Tada kažemo:

- Sud $B \Rightarrow A$ je **obrat** suda $A \Rightarrow B$;
- Sud $\neg B \Rightarrow \neg A$ je **obrat po kontrapoziciji** suda $A \Rightarrow B$.

Promotrimo tablicu istinitosti za navedene sudove:

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

Vidimo da je sud $A \Rightarrow B$ semantički jednak svom obratu po kontrapoziciji, a nije općenito jednak svom obratu.

Zadatak 1.6 Odredite sud F takav da sud

$$\big((A \Leftrightarrow \neg B) \wedge C\big) \Rightarrow \big((A \vee B) \wedge (\neg C \vee F)\big)$$

bude tautologija.

1.2 Predikati i kvantifikatori

Jednomjesni predikat je izjavna (matematička) rečenica koja sadrži varijablu i čija istinitost ovisi o vrijednosti te varijable. Uvrštavanjem konkretne vrijednosti za tu varijablu predikat postaje sud. Općenito, n**-mjesni predikat** je izjavna rečenica koja sadrži n varijabli te koja postaje sud uvrštavanjem konkretnih vrijednosti za te varijable.

Definicija 1.9. Neka je $P(x)$ predikat.

- Sud
$$(\forall x)P(x)$$
je istinit točno onda kada je $P(x)$ istinit za sve (dozvoljene) vrijednosti varijable x. Čitamo *"Za svaki x vrijedi $P(x)$"*, a oznaku $\forall$ zovemo **univerzalni kvantifiktor**.

- Sud
$$(\exists x)P(x)$$
je istinit točno onda kada postoji barem jedna vrijednost varijable x za koju je sud $P(x)$ istinit. Čitamo *"Postoji x za koji vrijedi $P(x)$"*, a oznaku $\exists$ zovemo **egzistencijalni kvantifiktor**.

U većini slučajeva potrebno je eksplicitno navesti iz kojeg skupa dolaze vrijednosti neke varijable. To možemo učiniti na sljedeći način:

$$(\forall x)(x \in S \Rightarrow P(x)) \quad \text{i} \quad (\exists x)(x \in S \wedge P(x)).$$

Ove sudove kraće zapisujemo kao

$$(\forall x \in S)P(x) \quad \text{i} \quad (\exists x \in S)P(x).$$

Ako želimo izjaviti da postoji točno jedna vrijednost varijable za koju je sud istinit (a ne više njih!), onda koristimo **kvantifikator jedinstvene egzistencije**, u oznaci $\exists!$.

Primjer 1.10.

1. Sud *"Svaki cijeli broj k djeljiv je s 1"* možemo zapisati kao $(\forall k \in \mathbb{Z})(k$ je djeljiv s 1) ili $(\forall k \in \mathbb{Z})(1 \mid k)$.

2. Sud *"Postoji realan broj koji nije racionalan"* možemo zapisati kao $(\exists x \in \mathbb{R})(x \notin \mathbb{Q})$.

3. Sud *"Postoji jedinstven prirodan broj čiji kvadrat je jednak 9"* možemo zapisati kao $(\exists! n \in \mathbb{N})(n^2 = 9)$.

Zadatak 1.7 Zapišite simbolima sljedeće sudove:

(a) "Za svaki realan broj postoji prirodan broj koji je veći od njega"

(b) "Postoji prirodan broj koji je djelitelj svakog prirodnog broja"

Zadatak 1.8 Zapišite sljedeće sudove riječima i provjerite njihovu istinitost:

(a) $(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(n < m)$

(b) $(\exists m \in \mathbb{N})(\forall n \in \mathbb{N})(n < m)$

Što možete zaključiti o redoslijedu kvantifikatora?

Zadatak 1.9 Odredite istinitost sljedećih sudova:

(a) $(\forall x \in \mathbb{R})(x = x^2)$

(b) $(\exists x \in \mathbb{R})(x = x^2)$

(c) $(\forall x \in \mathbb{R})(x + 1 > x)$

(d) $(\exists x \in \mathbb{R})(x + 2 = x)$

(e) $(\exists x \in \mathbb{R})(|x| = 0)$

(f) $(\forall y \in \mathbb{N})(\exists x \in \mathbb{N})(y \geq x)$

(g) $(\exists x \in \mathbb{N})(\forall y \in \mathbb{N})(y \geq x)$

(h) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(y \geq x)$

(i) $(\forall y \in \mathbb{R}_+)(\exists x \in \mathbb{R}_+)(xy = 1)$

Zadatak 1.10 Zapišite sljedeće sudove simbolima:

(a) “Svaki prirodan broj manji je od nekog prirodnog broja”

(b) “Postoji pridodan broj veći od svakog prirodnog broja”

(c) “Svaki prirodan broj koji je djeljiv s 14 je djeljiv s 2 i sa 7”

(d) “Svaki prirodan broj koji je kvadrat parnog broja je djeljiv s 4”

(e) “Za svaka dva prirodna broja vrijedi: ako je njihov produkt djeljiv nekim prostim brojem, onda je istim prostim brojem djeljiv barem jedan od njih”

Negiranje sudova s kvantifikatorima

Primjer 1.11.

1. Negacija suda "Svaki prirodan broj je paran" je "Postoji prirodan broj koji nije paran". Zapisano simbolima:

$$\neg(\forall n \in \mathbb{N})(2 \mid n) \equiv (\exists n \in \mathbb{N})(2 \nmid n).$$

   Uočavamo: negacija suda $\forall x P(x)$ je $\exists x(\neg P(x))$.

2. Negacija suda "Postoji prirodan broj koji je negativan" je "Svaki prirodan broj je nenegativan". Simbolima:

$$\neg(\exists n \in \mathbb{N})(n < 0) \equiv (\forall n \in \mathbb{N})(n \geq 0).$$

   Uočavamo: negacija suda $\exists x P(x)$ je $\forall x(\neg P(x))$.

3. Odredimo negaciju suda "Svaki pozitivan broj veći je od recipročne vrijednosti nekog prirodnog broja". Najprije zapišimo taj sud simbolima:

$$(\forall x \in \mathbb{R}_+)(\exists n \in \mathbb{N})\left(x > \tfrac{1}{n}\right).$$

   Koristeći pravila iz prethodna dva primjera, sada možemo zapisati negaciju:

$$(\exists x \in \mathbb{R}_+)(\forall n \in \mathbb{N})\left(x \leq \tfrac{1}{n}\right),$$

   tj. "Postoji pozitivan broj koji je manji ili jednak od recipročnih vrijednosti svih prirodnih brojeva".

Zadatak 1.11 Zapišite negacije sljedećih sudova:

(a) $(\exists x \in \mathbb{N})(x + 1 = 8)$

(b) $(\forall x \in \mathbb{N})(x < 8)$

(c) $(\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(x^2 + y^2 \geq 4)$

(d) $(\forall x \in \mathbb{R})(x > 0 \vee x < 0)$

(e) $(\forall x \in \mathbb{Q})(x \cdot 0 = 0 \wedge x \cdot 1 = x)$

(f) $(\exists a \in \mathbb{R}_+)(a \neq -1 \Rightarrow a = -2)$

(g) $(\forall x \in \mathbb{R})(x^2 - x \geq 0 \Leftrightarrow (x < 0 \vee x \geq 1))$

(h) $\big((\exists x \in \mathbb{Q})(x^2 = 2)\big) \Rightarrow \big((\forall y \in \mathbb{Q})(y + \sqrt{2} \in \mathbb{Q})\big)$

Zadatak 1.12 Napišite obrat po kontrapoziciji sljedećih implikacija:

(a) $(\forall x \in \mathbb{R})(x^2 - 7x + 12 > 0 \Rightarrow x < 3)$

(b) $(\forall x \in \mathbb{R})(x^2 - 2x > 0 \Rightarrow (x > 2 \vee x < 0))$

(c) $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})\big((x > 0 \wedge y > 0) \Rightarrow xy > 0\big)$

(d) $(\forall n \in \mathbb{N})\,(2 \mid n \Rightarrow (\exists k \in \mathbb{Z})(n = 4k \vee n = 4k + 2))$

Zadatak 1.13 Označimo $P(x) \equiv$ *"x je prost broj"*. Zadana je tvrdnja:

"Postoji prirodan broj manji od svakog prostog broja manjeg od 100*."*

Napišite simbolima zadanu tvrdnju te njenu negaciju, obrat i obrat po kontrapoziciji. Odredite istinitost zadane i svih dobivenih tvrdnji.

Zadatak 1.14 Zadana je tvrdnja:

"Za svaka dva prirodna broja vrijedi: ako je jedan od njih veći od drugog,
onda postoji paran broj manji od njihovog zbroja."

Napišite simbolima zadanu tvrdnju te njenu negaciju, obrat i obrat po kontrapoziciji. Odredite istinitost zadane i svih dobivenih tvrdnji.

1.3 Tehnike dokazivanja

Vrste matematičkih tvrdnji

Aksiom je tvrdnja koja se smatra istinitom i koja se ne dokazuje.

Definicija je izjava kojom se na jednoznačan način, nabrajanjem njegovih nužnih i dovoljnih svojstava, opisuje neki matematički pojam.

Teorem je matematička tvrdnja čiju istinitost je potrebno utvrditi dokazom, tj. logičkim zaključivanjem iz aksioma i već ranije dokazanih tvrdnji. Teoremi tipično imaju oblik implikacije $P \Rightarrow Q$, pri čemu sud P zovemo **pretpostavkom** teorema, a sud Q **tvrdnjom** teorema.

Primjer 1.12. Razdvojimo pretpostavke od tvrdnji sljedećih teorema:

1. Neka je funkcija $f : I \to \mathbb{R}$ strogo monotona na skupu $I \subseteq \mathbb{R}$. Tada je ona injekcija.

PRETPOSTAVKA $f : I \to \mathbb{R}$ je strogo monotana funkcija na skupu $I \subseteq \mathbb{R}$

TVRDNJA f je injekcija

2. Apsolutna vrijednost zbroja realnih brojeva je manja ili jednaka od zbroja apsolutnih vrijednosti pribrojnika.

PRETPOSTAVKA a i b su realni brojevi

TVRDNJA $|a+b| \leq |a| + |b|$

3. Podskup linearno nezavisnog skupa je linearno nezavisan.

PRETPOSTAVKA S je linearno nezavisan skup i $S' \subseteq S$ je njegov podskup

TVRDNJA S' je linearno nezavisan

Tehnike dokazivanja

Napraviti **direktan dokaz** tvrdnje $P \Rightarrow Q$ znači, uz pretpostavku da je tvrdnja P istinita, logičkim zaključivanjem pronaći tvrdnje $Q_1, Q_2, \ldots, Q_n$ takve da vrijedi

$$P \Rightarrow Q_1 \Rightarrow Q_2 \Rightarrow \ldots \Rightarrow Q_n \Rightarrow Q.$$

Zbog tranzitivnosti implikacije tada vrijedi $P \Rightarrow Q$.

Slično, napraviti direktan dokaz tvrdnje P znači pronaći tvrdnje $Q_1, Q_2, \ldots, Q_n$ takve da je

$$Q_1 \Rightarrow Q_2 \Rightarrow \ldots \Rightarrow Q_n \Rightarrow P,$$

pri čemu je Q_1 aksiom teorije ili neka očito istinita tvrdnja.

Zadatak 1.15 Dokažite da za svaka dva pozitivna realna broja a i b vrijedi **AG nejednakost**:

$$\frac{a+b}{2} \geq \sqrt{ab}.$$

Napraviti dokaz tvrdnje $P \Rightarrow Q$ **obratom po kontrapoziciji** znači dokazati tvrdnju $\neg Q \Rightarrow \neg P$. Kako je taj sud semantički jednak sudu $P \Rightarrow Q$, time smo ujedno dokazali i $P \Rightarrow Q$.

Zadatak 1.16 Dokažite da za svaki cijeli broj x vrijedi: ako je broj $x^2 - 6x + 5$ paran, onda je x neparan.

Napraviti dokaz tvrdnje P **svođenjem na kontradikciju** znači dokazati $\neg P \Rightarrow \bot$, pri čemu je $\bot$ neka očito lažna tvrdnja. Tada $\neg P$ mora biti laž, pa P mora biti istina.

Zadatak 1.17 Dokažite da ne postoje cijeli brojevi x, y i z takvi da je

$$x^2 + y^2 - z^2 + 2xy = 90.$$

Upute za rješavanje zadataka

Uputa za Z1.2 Uvedite oznake za jednostavne sudove i odredite im istinitost. Zatim zapišite složene sudove simbolima i promotrite odgovarajući redak u tablici istinitosti.

Uputa za Z1.3 Napišite tablice istinitosti i uvjerite se da su odgovarajući stupci jednaki.

Uputa za Z1.4 Napišite tablice istinitosti i uvjerite se da se odgovarajući stupci sastoje samo od jedinica.

Uputa za Z1.5 Tvrdnje (a), (b), (c) i (d) dokažite koristeći tablice istinitosti. Zatim iskoristite te tvrdnje za dokaz tvrdnji (e) i (f).

Uputa za Z1.6 Implikacija $P \Rightarrow Q$ je lažna samo ako je sud P istinit, a sud Q lažan. Odredite za koje vrijednosti sudova A, B i C je sud P istinit, i odaberite F tako da u tom slučaju sud Q mora također biti istinit.

Uputa za Z1.14 Izjava *"jedan od brojeva m i n je veći od drugog"* ne specificira redoslijed, pa treba obuhvatiti obje mogućnosti pri zapisu tog suda simbolima. Zapisujemo ga $n > m \vee m > n$.

Rješenja zadataka

Rješenje 1.1

(a) Ako je $2^3 = 8$, onda je $7 \leq 5$.

(b) $2^3 = 8$ ili je $7 \leq 5$.

(c) $2^3 \neq 8$ ako i samo ako je $7 > 5$.

(d) Nije istina da je $2^3 \neq 8$

(e) Ako je $2^3 = 8$ i $7 \leq 5$, onda je $2^3 = 8$.

Rješenje 1.2

(a) Označimo $A \equiv 3+2=7$ i $B \equiv 4+4=8$. Tada je zadani sud $A \Rightarrow B$. Imamo tablicu istinitosti:

A	B	$A \Rightarrow B$
0	1	1

Zadani sud je istinit.

(b) Označimo $A \equiv 6^2 = 32$ i $B \equiv 4 \geq 10$. Tada je zadani sud $\neg(A \Leftrightarrow B)$. Imamo tablicu istinitosti:

A	B	$A \Leftrightarrow B$	$\neg(A \Leftrightarrow B)$
0	0	1	0

Zadani sud je lažan.

(c) Označimo $A \equiv \log_2 16 = 3$ i $B \equiv \cos 0 = 1$. Tada je zadani sud $\neg(A \vee B)$. Imamo tablicu istinitosti:

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

Zadani sud je lažan.

(d) Označimo $A \equiv$ "10 je djeljiv s 3" i $B \equiv \sqrt{9} = 4$. Zadani sud je $\neg(A \Rightarrow B)$. Imamo tablicu istinitosti:

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

Zadani sud je lažan.

Rješenje 1.3 Semantičku jednakost sudova provjeravamo tablicom istinitosti.

(a)

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

(b)

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

(c)

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

(d)

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

Vidimo da zadani sudovi imaju jednake stupce u tablici istinitosti, pa su semantički jednaki.

Rješenje 1.4 Pokažimo da se stupci u tablici istinitosti koji odgovara zadanim sudovima sastoje samo od jedinica:

(a)

A	B	$A \Rightarrow B$	$A \wedge (A \Rightarrow B)$	$(A \wedge (A \Rightarrow B)) \Rightarrow A$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	1	1	1

(b)

A	B	$A \Rightarrow B$	$\neg B$	$\neg A$	$\neg A \Rightarrow \neg B$	$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
0	0	1	1	1	1	1
0	1	1	0	1	1	1
1	0	0	1	0	0	1
1	1	1	0	0	1	1

(c)

A	B	C	$A \Rightarrow B$	$B \Rightarrow C$	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$A \Rightarrow C$	$((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

Rješenje 1.5

(a)

A	$\neg A$	$\neg(\neg A)$
0	1	0
1	0	1

(b)

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

(c)

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

(d)

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

(e) $\neg(A \Rightarrow B) \equiv \neg(\neg A \vee B) \equiv \neg(\neg A) \wedge \neg B \equiv A \wedge \neg B$

(f) $\neg(A \Leftrightarrow B) \equiv \neg((A \Rightarrow B) \wedge (B \Rightarrow A)) \equiv \neg(A \Rightarrow B) \vee \neg(B \Rightarrow A) \equiv (A \wedge \neg B) \vee (B \wedge \neg A)$

Rješenje 1.6 Implikacija $P \Rightarrow Q$ je lažna samo onda kad je sud P istinit, a sud Q lažan. Prema tome, moramo osigurati da sud $(A \vee B) \wedge (\neg C \vee F)$ bude istinit kad god je sud $(A \Leftrightarrow \neg B) \wedge C$ istinit.
Ako je sud $(A \Leftrightarrow \neg B) \wedge C$ istinit, onda su oba konjunkta istinita. Dakle, C i $A \Leftrightarrow \neg B$ su istiniti. Ako je sud $A \Leftrightarrow \neg B$ istinit, onda su A i $\neg B$ ili oba istiniti, ili oba lažni. U svakom slučaju, ti sudovi imaju iste vrijednosti, pa sudovi A i B imaju različite vrijednosti, tj. točno jedan je istinit, a drugi je lažan.
Sada treba osigurati da sud $\big((A \vee B) \wedge (\neg C \vee F)\big)$ bude istinit u slučaju kad je C istinit, a A i B imaju različite vrijednosti. Sud $A \vee B$ je svakako istinit, jer je istinit ili A, ili B. Još treba

postići da sud $\neg C \vee F$ bude istinit. To možemo npr. za $F \equiv C$, jer znamo da je $\neg C \vee C$ tautologija.
Provjerimo tablicom istinitosti da je sud $\big((A \Leftrightarrow \neg B) \wedge C\big) \Rightarrow \big((A \vee B) \wedge (\neg C \vee C)\big)$ zaista tautologija:

A	B	C	$(A \Leftrightarrow \neg B) \wedge C$	$(A \vee B) \wedge (\neg C \vee C)$	$\big((A \Leftrightarrow \neg B) \wedge C\big) \Rightarrow \big((A \vee B) \wedge (\neg C \vee C)\big)$
0	0	0	0	0	1
0	0	1	0	0	1
0	1	0	0	1	1
0	1	1	1	1	1
1	0	0	0	1	1
1	0	1	1	1	1
1	1	0	0	1	1
1	1	1	0	1	1

Rješenje 1.7

(a) $(\forall x \in \mathbb{R})(\exists n \in \mathbb{N})(n > x)$

(b) $(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n \mid m)$

Rješenje 1.8

(a) "Za svaki prirodan broj postoji prirodan broj koji je veći od njega."
Ovaj sud je istinit.

(b) "Postoji prirodan broj koji je veći od svakog prirodnog broja"
Ovaj sud je lažan.

Budući da je sud pod (a) istinit, a sud pod (b) lažan, vidimo da je redoslijed kvantifikatora bitan. U suprotnom bi ova dva suda bila ekvivalentna, što očito ne vrijedi.

Rješenje 1.9

(a) Sud je lažan jer $x^2 = x$ ne vrijedi za sve realne brojeve x; npr. $2^2 \neq 2$.

(b) Sud je istinit jer postoji realan broj x koji je jednak svom kvadratu; takvi su brojevi 0 i 1.

(c) Sud je istinit jer je $x+1$ strogo veće od x za sve realne brojeve x.

(d) Sud je lažan, ne postoji realan broj x takav da je $x+2=x$ jer bi u tom slučaju vrijedilo $2=0$.

(e) Sud je istinit, postoji realan broj x čija apsolutna vrijednost je jednaka 0, to je 0.

(f) Sud je istinit, za svaki prirodan broj y postoji neki prirodan broj koji je manji ili jednak y, npr. sam y.

(g) Sud je istinit, postoji prirodan broj koji je manji ili jednak od svakog prirodnog broja; to je broj 1.

(h) Sud je lažan, ne postoji realan broj koji je manji ili jednak od svakog realnog broja; za svaki $x \in \mathbb{R}$ je npr. $x-1<x$.

(i) Sud je istinit, za svaki pozitivan realni broj y postoji pozitivan realni broj $\frac{1}{y}$ takav da je $y \cdot \frac{1}{y} = 1$.

Rješenje 1.10

(a) $(\forall n \in \mathbb{N})(n$ je manji od nekog prirodnog broja$) = (\forall n \in \mathbb{N})(\exists m \in \mathbb{N})(n < m)$

(b) $(\exists n \in \mathbb{N})(n$ je veći od svakog prirodnog broja$) = (\exists n \in \mathbb{N})(\forall m \in \mathbb{N})(n > m)$

(c) $(\forall n \in \mathbb{N})$(ako je n djeljiv s 14, onda je n djeljiv s 2 i sa 7)
$= (\forall n \in \mathbb{N})(14 \mid n \Rightarrow 2 \mid n \wedge 7 \mid n)$

(d) $(\forall n \in \mathbb{N})$(ako je n kvadrat nekog parnog broja, onda je n djeljiv s 4)
$= (\forall n \in \mathbb{N})($(postoji parni broj čiji kvadrat je $n) \Rightarrow 4 \mid n)$
$= (\forall n \in \mathbb{N})((\exists k \in \mathbb{N})(2 \mid k \wedge n = k^2) \Rightarrow 4 \mid n)$

(e) $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})$(ako neki prost broj p dijeli mn, onda p dijeli m ili p dijeli n)
$= (\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(\forall p \in \mathbb{N})((p$ prost $\wedge\ p \mid mn) \Rightarrow (p \mid m \vee p \mid n))$

Rješenje 1.11

(a) $(\forall x \in \mathbb{N})(x+1 \neq 8)$

(b) $\exists x \in \mathbb{N})(x \geq 8)$

(c) $(\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(x^2+y^2 < 4)$

(d) $(\exists x \in \mathbb{R})(x \leq 0 \wedge x \geq 0)$

(e) $(\exists x \in \mathbb{Q})(x \cdot 0 \neq 0 \vee x \cdot 1 \neq x)$

(f) $(\forall a \in \mathbb{R}_+)(a = -1 \wedge a \neq -2)$

(g) $(\exists x \in \mathbb{R})\big((x^2 - x \geq 0 \wedge (x > 0 \wedge x < 1)) \vee (x^2 - x < 0 \wedge (x \leq 0 \vee x \geq 1))\big)$

(h) $\big((\exists x \in \mathbb{Q})(x^2 = 2)\big) \wedge \big((\exists y \in \mathbb{Q})(y + \sqrt{2} \notin \mathbb{Q})\big)$

Rješenje 1.12

(a) $(\forall x \in \mathbb{R})(x \geq 3 \Rightarrow x^2 - 7x + 12 \leq 0)$

(b) $(\forall x \in \mathbb{R})\big((x \leq 2 \wedge x \geq 0) \Rightarrow x^2 - 2x \leq 0\big)$

(c) $(\forall x \in \mathbb{R})(\forall y \in \mathbb{R})\big(xy \leq 0 \Rightarrow (x \leq 0 \vee y \leq 0)\big)$

(d) $(\forall n \in \mathbb{N})\big((\forall k \in \mathbb{Z})(n \neq 4k \wedge n \neq 4k+2) \Rightarrow 2 \nmid n\big)$

Rješenje 1.13
Zadana tvrdnja:

$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})\big((P(m) \wedge m < 100) \Rightarrow n < m\big)$$

Negacija:

$$(\forall n \in \mathbb{N})(\exists m \in \mathbb{N})\big((P(m) \wedge m < 100) \wedge n \geq m\big)$$

Obrat:

$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})\big(n < m \Rightarrow (P(m) \wedge m < 100)\big)$$

Obrat po kontrapoziciji:

$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})\big(n \geq m \Rightarrow (\neg P(m) \vee m \geq 100)\big)$$

Zadana tvrdnja je istinita: broj 1 je manji od svakog prostog broja manjeg od 100. Negacija tvrdnje je lažna, a obrat po kontrapoziciji je istinit.
Obrat nije istinit: ne postoji prirodan broj takav da je svaki prirodan broj koji je veći od njega prost i manji od 100.

Rješenje 1.14
Zadana tvrdnja:

$$(\forall m, n \in \mathbb{N})\big((m > n \vee n > m) \Rightarrow (\exists k \in \mathbb{N})(2 \mid k \wedge k < m + n)\big)$$

Negacija:

$$(\exists m,n\in\mathbb{N})\big((m>n\vee n>m)\wedge(\forall k\in\mathbb{N})(2\nmid k\vee k\geq m+n)\big)$$

Obrat:

$$(\forall m,n\in\mathbb{N})\big((\exists k\in\mathbb{N})(2\mid k\wedge k<m+n)\Rightarrow(m>n\vee n>m)\big)$$

Obrat po kontrapoziciji:

$$(\forall m,n\in\mathbb{N})\big((\forall k\in\mathbb{N})(2\nmid k\vee k\geq m+n)\Rightarrow(m\leq n\wedge n\leq m)\big)$$

Zadana tvrdnja je istinita: ako je jedan broj strogo veći od drugog, onda ti brojevi mogu biti najmanje 1 i 2, pa je njihov zbroj najmanje 3. Tada je 2 paran broj koji je sigurno manji od njihovog zbroja. Negacija tvrdnje je lažna, a obrat po kontrapoziciji je istinit.

Obrat nije istinit: za $n=3$ i $m=3$ postoji paran broj strogo manji od njihovog zbroja (npr. 4), ali vrijedi $n=m$, tj. nijedan od ta dva broja nije strogo veći od drugog.

Rješenje 1.15 Dokazujemo implikaciju

$$a \text{ i } b \text{ su pozitivni realni brojevi} \quad\Longrightarrow\quad \frac{a+b}{2}\geq\sqrt{ab}.$$

Tvrdnju ćemo dokazati direktno, tj. pretpostavit ćemo da vrijedi lijeva strana implikacije i zaključiti da tada vrijedi i desna strana.

Pretpostavimo da su a i b pozitivni realni brojevi. Tada su $\sqrt{a}$ i $\sqrt{b}$ (pozitivni) realni brojevi, pa je njihova razlika realni broj. Stoga je

$$(\sqrt{a}-\sqrt{b})^2\geq 0.$$

Odavde slijedi

$$a-2\sqrt{ab}+b\geq 0,$$

odnosno

$$a+b\geq 2\sqrt{ab}.$$

Dijeljenjem s 2 dobivamo zadanu nejednakost.

Rješenje 1.16 Neka je x proizvoljan cijeli broj.
Pretpostavimo da je x paran. Tada je $x = 2k$ za neki $k \in \mathbb{Z}$, pa imamo

$$x^2 - 6x + 5 = 4k^2 - 12k + 5 = 2\underbrace{(2k^2 - 6k + 2)}_{\in\mathbb{Z}} + 1.$$

Dakle, dokazali smo

$$x \text{ paran} \quad \Rightarrow \quad x^2 - 6x + 5 \text{ neparan},$$

što je ekvivalentno s

$$x^2 - 6x + 5 \text{ paran} \quad \Rightarrow \quad x \text{ neparan}.$$

Rješenje 1.17 Dokazujemo da ne postoje cijeli brojevi za koje vrijedi gornja jednakost. Tvrdnju ćemo dokazati svođenjem na kontradikciju.

Pretpostavimo suprotno, da postoje cijeli brojevi x, y i z za koje vrijedi

$$x^2 + y^2 - z^2 + 2xy = 90.$$

Tada je

$$(x + y)^2 - z^2 = 90,$$

odnosno

$$(x + y + z)(x + y - z) = 90.$$

Uočimo: razlika brojeva $x+y+z$ i $x+y-z$ je paran broj $(2z)$, pa su ti brojevi iste parnosti.

1°) $x + y + z$ i $x + y - z$ su oba neparni. No, tada je i njihov umnožak neparan, pa ne može biti jednak 90.

2°) $x + y + z$ i $x + y - z$ su oba parni. Tada je njihov umnožak djeljiv s 4. No, 90 nije djeljiv s 4, pa umnožak ne može biti 90.

U oba slučaja dobili smo kontradikciju s pretpostavkom da je $x^2 + y^2 - z^2 + 2xy = 90$. Dakle, pretpostavka ne vrijedi, tj. ne postoje cijeli brojevi x, y i z za koje vrijedi $x^2 + y^2 - z^2 + 2xy = 90$.

Poglavlje 2

Skupovi

2.1 Skupovne operacije

Neformalno, **skup** shvaćamo kao neuređenu kolekciju različitih objekata.

Pišemo $x \in S$ ako x pripada kolekciji objekata koji čine S. U protivnom pišemo $x \notin S$.

Primjer 2.1. Neki primjeri skupova:

1. $S = \{1,2,3\}$ je skup čiji elementi su prirodni brojevi 1, 2 i 3. Vrijedi
$$S = \{1,3,2\} = \{2,1,3\} = \{2,3,1\} = \{3,1,2\} = \{3,2,1\}.$$
2. Skup prirodnih brojeva $\mathbb{N} = \{1,2,3,\ldots\}$ je primjer beskonačnog skupa. Također poznajemo skupove brojeva $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$.
3. Skup parnih prirodnih brojeva $P = \{2,4,6,8,\ldots\}$ možemo zapisati kao
$$P = \{n \in \mathbb{N} \mid n \text{ je paran}\} = \{n \in \mathbb{N} \mid 2 \mid n\}$$
ili, alternativno, kao skup svih višekratnika broja 2:
$$P = \{2n \mid n \in \mathbb{N}\}.$$
4. **Prazan skup** $\emptyset$ ne sadrži niti jedan element. Drugim riječima, za svaki objekt x vrijedi $x \notin \emptyset$.

Napomena 2.2. $\emptyset$ je *oznaka* za prazan skup, tj. skup $\{\,\}$ (skup bez elemenata), jednako kao što je $\mathbb{N}$ oznaka za skup $\{1,2,3,\ldots\}$. Bilo bi pogrešno pisati $\{\emptyset\}$ za prazan skup, jednako kao što bi bilo pogrešno pisati $\{\mathbb{N}\}$ za skup prirodnih brojeva.

Definicija 2.3. Neka su A i B skupovi. Kažemo da je A **podskup** skupa B i pišemo $A \subseteq B$ ako je svaki element skupa A ujedno i element skupa B, tj. ako vrijedi

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

Kažemo da su skupovi A i B **jednaki** i pišemo $A = B$ ako vrijedi $A \subseteq B$ i $B \subseteq A$, tj.

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

Kažemo da je skup A **pravi podskup** skupa B i pišemo $A \subsetneq B$ ako vrijedi $A \subseteq B$ i $B \nsubseteq A$.

Napomena 2.4. Prazan skup je podskup svakog skupa. Zaista, za bilo koji skup S tvrdnja

$$\forall x(x \in \emptyset \Rightarrow x \in S)$$

je istinita jer je za svaki objekt x sud $x \in \emptyset$ lažan, pa je implikacija $x \in \emptyset \Rightarrow x \in S$ istinita. Također, za svaki skup S vrijedi $S \subseteq S$: sud

$$\forall x(x \in S \Rightarrow x \in S)$$

je očito istinit.

Primjer 2.5. Zapišimo sve podskupove skupa $\{1,2,3\}$.

- Prazan skup $\emptyset$.
- Jednočlani podskupovi su $\{1\}$, $\{2\}$ i $\{3\}$.
- Dvočlani podskupovi su $\{1,2\}$, $\{2,3\}$ i $\{1,3\}$.
- Jedini tročlani podskup je $\{1,2,3\}$.

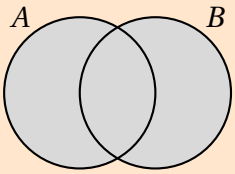
Definicija 2.6. Neka je S skup. Skup svih podskupova od S zovemo **partitivni skup** skupa S i označavamo sa $\mathscr{P}(S)$.

Zadatak 2.1 Dokažite da vrijedi $\mathscr{P}(A) = \mathscr{P}(B)$ ako i samo ako je $A = B$.

Operacije nad skupovima. Neka su A i B skupovi.

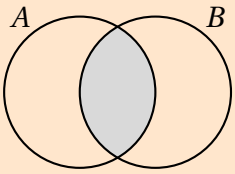
- **Unija** skupova A i B je skup čiji elementi su svi objekti koji pripadaju ili skupu A, ili skupu B. Uniju skupova A i B označavamo sa $A \cup B$.
  Vrijedi

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B.$$



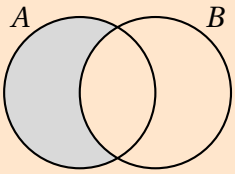
- **Presjek** skupova A i B je skup čiji elementi su svi objekti koji pripadaju i skupu A i skupu B. Presjek skupova A i B označavamo sa $A \cap B$.
  Vrijedi

$$x \in A \cap B \Leftrightarrow x \in A \wedge x \in B.$$



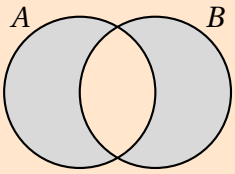
- **Razlika** skupova A i B je skup čiji elementi su svi objekti koji pripadaju skupu A, a ne pripadaju skupu B. Razliku skupova A i B označavamo sa $A \setminus B$.
  Vrijedi

$$x \in A \setminus B \Leftrightarrow x \in A \wedge x \notin B.$$

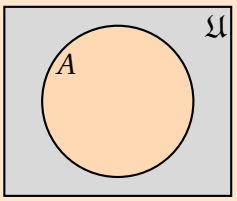


- **Simetrična razlika** skupova A i B je skup čiji elementi su svi objekti koji pripadaju jednom od skupova A i B, a ne pripadaju drugom. Simetričnu razliku skupova A i B označavamo sa $A \triangle B$.
  Vrijedi

$$x \in A \triangle B \Leftrightarrow (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B).$$

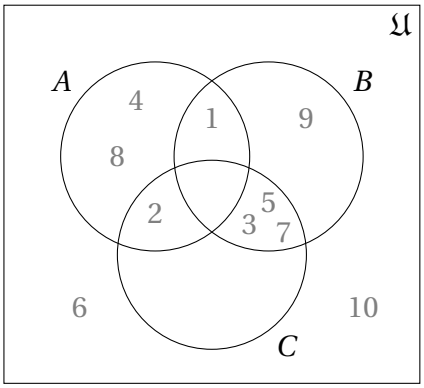


- Ako je $A \subseteq \mathfrak{U}$ za neki skup $\mathfrak{U}$, skup $\mathfrak{U} \setminus A$ označavamo još sa A^c i zovemo **komplement skupa** A u odnosu na $\mathfrak{U}$. Ovdje $\mathfrak{U}$ ima ulogu *univerzalnog skupa.*



Primjer 2.7. Neka je $\mathfrak{U} = \{1,2,3,4,5,6,7,8,9,10\}$ i

$$A = \{1,2,4,8\}, \quad B = \{1,3,5,7,9\}, \quad C = \{2,3,5,7\}.$$



Imamo

$$A \cup B = \{1,2,3,4,5,7,8,9\} \qquad B \cap C = \{3,5,7\} \qquad A \setminus C = \{1,4,8\}$$
$$C \setminus A = \{3,5,7\} \qquad (A \cup B)^c = \{6,10\} \qquad C \setminus (A \cup B) = \emptyset$$

Zadatak 2.2 Neka su A i B podskupovi univerzalnog skupa $\mathfrak{U}$. Dokažite da je

$$A \setminus B = A \cap B^c.$$

Zadatak 2.3 Neka je $\mathfrak{U} = \mathbb{N}$. Ako postoji, navedite primjer skupa $A \subseteq \mathbb{N}$ takvog da:

(a) A je konačan i A^c je beskonačan;

(b) A je beskonačan i A^c je konačan;

(c) A i A^c su oba beskonačni;

(d) A i A^c su oba konačan;

Definicija 2.8. Za skupove A i B takve da vrijedi $A \cap B = \emptyset$ kažemo da su **disjunktni**.

Zadatak 2.4 Neka su A i B podskupovi univerzalnog skupa $\mathfrak{U}$. Dokažite da su A i B disjunktni ako i samo ako je $A \subseteq B^c$.

Zadatak 2.5 Neka su A, B i C skupovi. Dokažite da vrijedi

$$A \subseteq C \text{ i } B \subseteq C \quad \text{ako i samo ako} \quad A \cup B \subseteq C.$$

Zadatak 2.6 Neka su A i B skupovi. Dokažite da vrijedi

$$(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

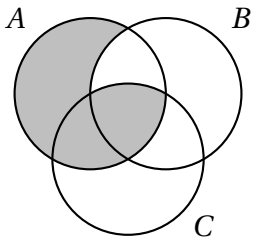
Napomena 2.9. Primijetimo da je skup iz prethodnog zadatka upravo simetrična razlika $A \triangle B$.

Zadatak 2.7 Neka su A, B i C skupovi. Dokažite

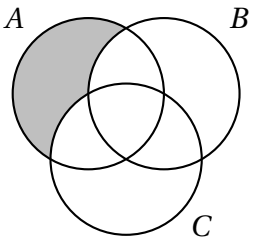
$$A \setminus (B \cup C) = (A \setminus B) \setminus C.$$

Napomena 2.10. Skupovna razlika nije asocijativna aperacija, tj. vrijedi

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



$A \setminus (B \setminus C)$



$(A \setminus B) \setminus C$

Primjerice, za skupove $A = \{1,2,3\}$, $B = \{2\}$ i $C = \{2,3\}$ vrijedi

$$A \setminus (B \setminus C) = \{1,2,3\} \setminus (\{2\} \setminus \{2,3\}) = \{1,2,3\} \setminus \emptyset = \{1,2,3\}$$

i

$$(A \setminus B) \setminus C = (\{1,2,3\} \setminus \{2\}) \setminus \{2,3\} = \{1,3\} \setminus \{2,3\} = \{1\},$$

a očito $\{1,2,3\} \neq \{1\}$.

Ispitati odnos skupova S i T znači provjeriti vrijedi li neka od inkluzija $S \subseteq T$ i $T \subseteq S$. Inkluziju koja vrijedi potrebno je dokazati, a za onu koja ne vrijedi potrebno je naći *kontraprimjer*.

Zadatak 2.8 Neka su A, B i C skupovi. Ispitajte odnos skupova

$$(A \setminus B) \cup C \qquad \text{i} \qquad (A \cup C) \setminus B.$$

Zadatak 2.9 Neka su A, B, C i D skupovi. Ispitajte odnos skupova

$$(A \setminus B) \cup (C \setminus D) \qquad \text{i} \qquad (A \cup C) \setminus (B \cup D).$$

Zadatak 2.10 Neka su A, B, C skupovi. Ispitajte odnos skupova

$$(A \cup B) \triangle C \quad \text{i} \quad (A \triangle C) \cup B.$$

Zadatak 2.11 Neka su A, B, C skupovi. Dokažite da je $A \triangle (B \triangle C) = (A \triangle B) \triangle C$, odnosno da je operacija $\triangle$ asocijativna.

2.2 Kartezijev produkt

Definicija 2.11. Neka su A i B skupovi te $a \in A$, $b \in B$. Objekt (a, b) zovemo **uređeni par**, pri čemu a zovemo **prvi član** para, a b zovemo **drugi član** para.

Za dva uređena para (a_1, b_1) i (a_2, b_2) vrijedi

$$(a_1, b_1) = (a_2, b_2) \quad \Leftrightarrow \quad a_1 = a_2 \ \wedge \ b_1 = b_2.$$

Poredak elemenata u uređenom paru je bitan. Na primjer, ako je $A = B = \{1, 2\}$, onda je $(1, 2) \neq (2, 1)$ iako za pripadne skupove vrijedi $\{1, 2\} = \{2, 1\}$.

Definicija 2.12. Kartezijev produkt skupova A i B je skup

$$A \times B := \{(a, b) \mid a \in A \wedge b \in B\}.$$

Napomena 2.13. Kartezijev produkt nije komutativan, odnosno ako je $A \neq B$, onda je $A \times B \neq B \times A$.

Napomena 2.14. Primijetimo da su formalno $(A \times B) \times C$ i $A \times (B \times C)$ različiti skupovi. Naime, elementi prvog su oblika $((a,b),c)$ a elementi drugog su oblika $(a,(b,c))$ za neke $a \in A$, $b \in B$, $c \in C$. Međutim, dogovorno ih u većini situacija smatramo jednakima, i pišemo $A \times B \times C$ za bilo koji od tih skupova, a elemente zapisujemo kao uređene trojke (a,b,c).

Slično možemo definirati Kartezijev produkt n skupova $A_1, A_2, \ldots, A_n$ kao skup svih uređenih n-torki:

$$A_1 \times A_2 \times \ldots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1 \wedge a_2 \in A_2 \wedge \cdots \wedge a_n \in A_n\}.$$

Zadatak 2.12 Neka su A, B i C skupovi. Dokažite da je $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Napomena 2.15. Vrijede i sljedeća svojstva:

$$A \times (B \setminus C) = (A \times B) \setminus (A \times C),$$
$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

Dokazi su slični prethodnom i ostavljamo ih za zadaću.

Zadatak 2.13 Neka su A, B, C i D skupovi. Ispitajte odnos skupova

$$((A \setminus C) \times (B \setminus D)) \cup ((C \setminus A) \times (D \setminus B)) \quad \text{i} \quad (A \times B) \triangle (C \times D).$$

Upute za rješavanje zadataka

Uputa za Z2.1 Za dokaz $\mathscr{P}(A) = \mathscr{P}(B) \Rightarrow A = B$ iskoristite $A \in \mathscr{P}(A)$, odnosno $B \in \mathscr{P}(B)$ i činjenicu $A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$.

Uputa za Z2.2 Dokažite da je $x \in A \setminus B$ logički ekvivalentno s $x \in A \cap B^c$. Pritom koristite formule iz definicija skupovnih operacija.

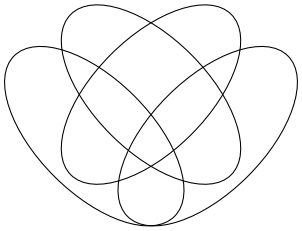
Uputa za Z2.4 Koristite svođenje na kontradikciju! Konkretno, za smjer $\boxed{\Leftarrow}$, pretpostavite da postoji neki element skupa $A \cap B$ i pokušajte iz toga dobiti neku lažnu tvrdnju.

Uputa za Z2.5 Iskoristite $S \subseteq S \cup T$ i $T \subseteq S \cup T$.

Uputa za Z2.7 Dokažite da je $x \in A \setminus (B \cup C)$ logički ekvivalentno s $x \in (A \setminus B) \setminus C$.

Uputa za Z2.8 Najprije skicirajte Vennove dijagrame i uočite $(A \setminus B) \cup C \supsetneq (A \cup C) \setminus B$. Treba dokazati inkluziju $\boxed{\supseteq}$ i naći kontraprimjer za $\boxed{\not\subseteq}$.

Uputa za Z2.9 Kao u zadatku 2.8, skicirajte Vennove dijagrame kako biste ustanovili koju inkluziju treba dokazati, a koju opovrgnuti. Vennov dijagram za četiri skupa izgleda ovako:



Uputa za Z2.11 Pomoću semantičke tablice dokažite da su sudovi $x \in A \triangle (B \triangle C)$ i $x \in (A \triangle B) \triangle C$ logički ekvivalentni.

Rješenja zadataka

Rješenje 2.1 Dokazujemo ekvivalenciju

$$\mathscr{P}(A) = \mathscr{P}(B) \Leftrightarrow A = B.$$

$\boxed{\Rightarrow}$ Pretpostavimo da je $\mathscr{P}(A) = \mathscr{P}(B)$. Treba dokazati $A = B$. Dokazat ćemo $A \subseteq B$ i $B \subseteq A$.

Kako je $A \subseteq A$, vrijedi $A \in \mathscr{P}(A)$. Zbog pretpostavke $\mathscr{P}(A) = \mathscr{P}(B)$ odavde slijedi $A \in \mathscr{P}(B)$, tj. $A \subseteq B$.
Analogno, vrijedi $B \subseteq B$ pa je $B \in \mathscr{P}(B)$ i zbog pretpostavke imamo $B \in \mathscr{P}(A)$, odnosno $B \subseteq A$.

Dakle, vrijedi $A \subseteq B$ i $B \subseteq A$, tj. $A = B$.

$\boxed{\Leftarrow}$ Pretpostavimo da vrijedi $A = B$. Tada očito vrijedi $\mathscr{P}(A) = \mathscr{P}(B)$: svaki podskup od A je ujedno i podskup od B i obratno, pa $\mathscr{P}(A)$ i $\mathscr{P}(B)$ sadrže iste elemente, tj. jednaki su.

Rješenje 2.2 Neka je $x \in \mathfrak{U}$ proizvoljan. Vrijedi:

$$\begin{aligned} x \in A \setminus B &\Leftrightarrow x \in A \wedge x \notin B \\ &\Leftrightarrow (x \in A \wedge x \in \mathfrak{U}) \wedge x \notin B \\ &\Leftrightarrow x \in A \wedge (x \in \mathfrak{U} \wedge x \notin B) \\ &\Leftrightarrow x \in A \wedge x \in B^c \\ &\Leftrightarrow x \in A \cap B^c. \end{aligned}$$

Dakle, vrijedi $\forall x (x \in A \setminus B \Leftrightarrow x \in A \cap B^c)$, tj. $A \setminus B = A \cap B^c$.

Rješenje 2.3

(a) Skup $A = \{1,2\}$ je konačan. Njegov komplement $A^c = \{3,4,5,\ldots\}$ je beskonačan.

(b) Skup $A = \{2,3,4,\ldots\}$ je beskonačan. Njegov komplement $A^c = \{1\}$ je konačan.

(c) Skup parnih brojeva $A = \{2n \mid n \in \mathbb{N}\}$ je beskonačan. Njegov komplement je skup neparnih brojeva $A^c = \{2n-1 \mid n \in \mathbb{N}\}$ koji je također beskonačan.

(d) Takav skup ne postoji; u suprotnom bi skup prirodnih brojeva $\mathbb{N} = A \cup A^c$ bio unija dva konačna skupa, pa bi i sam bio konačan.

Rješenje 2.4

$\boxed{\Rightarrow}$ Pretpostavimo da su A i B disjunktni, tj. $A \cap B = \emptyset$. Treba dokazati $A \subseteq B^c$.

Neka je $x \in \mathfrak{U}$ proizvoljan. Pretpostavimo $x \in A$.

Kada bi vrijedilo $x \in B$, imali bismo $x \in A \cap B$, tj. $x \in \emptyset$ što je nemoguće. Dakle, vrijedi $x \notin B$.

Imamo $x \in \mathfrak{U}$ i $x \notin B$, pa je $x \in B^c$.

Dakle, vrijedi $(\forall x)(x \in A \Rightarrow x \in B^c)$, odnosno $A \subseteq B^c$.

$\boxed{\Leftarrow}$ Pretpostavimo da je $A \subseteq B^c$. Dokazujemo $A \cap B = \emptyset$ svođenjem na kontradikciju.

Pretpostavimo da vrijedi $A \cap B \neq \emptyset$. Tada postoji $x \in A \cap B$, tj. imamo $x \in A$ i $x \in B$. Iz činjenice $x \in A$ koristeći pretpostavku $A \subseteq B^c$ dobivamo $x \in B^c$. No, vrijedi i $x \in B$. Kako x ne može istovremeno biti element i skupa B i njegovog komplementa, došli smo do kontradikcije. Dakle, vrijedi $A \cap B = \emptyset$.

Rješenje 2.5

$\boxed{\Rightarrow}$ Pretpostavimo da je $A \subseteq C$ i $B \subseteq C$.

Neka je $x \in A \cup B$. Ako je $x \in A$, zbog $A \subseteq C$ slijedi $x \in C$. Analogno, ako je $x \in B$, zbog $B \subseteq C$ slijedi $x \in C$. U svakom slučaju, vrijedi $x \in C$.

Dakle, vrijedi $(\forall x)(x \in A \cup B \Rightarrow x \in C)$, tj. $A \cup B \subseteq C$.

$\boxed{\Leftarrow}$ Pretpostavimo da je $A \cup B \subseteq C$. Vrijedi:

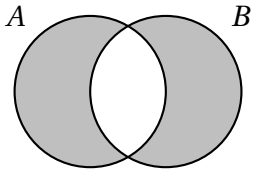
$$x \in A \Rightarrow x \in A \vee x \in B \Rightarrow x \in A \cup B \Rightarrow x \in C$$

i

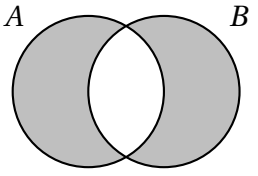
$$x \in B \Rightarrow x \in A \vee x \in B \Rightarrow x \in A \cup B \Rightarrow x \in C.$$

Dakle, vrijedi $(\forall x)(x \in A \Rightarrow x \in C)$ i $(\forall x)(x \in B \Rightarrow x \in C)$, odnosno $A \subseteq C$ i $B \subseteq C$.

Rješenje 2.6 Za početak, skicirajmo Vennove dijagrame za ove skupove.



$(A \setminus B) \cup (B \setminus A)$



$(A \cup B) \setminus (A \cap B)$

Podsjetimo se: kako bismo dokazali $S = T$, treba dokazati $S \subseteq T$ i $T \subseteq S$.

$\boxed{\subseteq}$ Neka je $x \in (A \setminus B) \cup (B \setminus A)$. Imamo:

$$\begin{aligned} x \in (A \setminus B) \cup (B \setminus A) &\Leftrightarrow (x \in A \setminus B) \vee (x \in B \setminus A) \\ &\Leftrightarrow \underbrace{(x \in A \wedge x \notin B)}_{1^\circ} \vee \underbrace{(x \in B \wedge x \notin A)}_{2^\circ} \end{aligned}$$

1°) Iz $x \in A$ slijedi $x \in A \cup B$, a iz $x \notin B$ slijedi $x \notin A \cap B$. Prema tome, vrijedi $x \in (A \cup B) \setminus (A \cap B)$.

2°) Iz $x \in B$ slijedi $x \in A \cup B$, a iz $x \notin A$ slijedi $x \notin A \cap B$. Stoga i u ovom slučaju vrijedi $x \in (A \cup B) \setminus (A \cap B)$.

Dokazali smo $(A \setminus B) \cup (B \setminus A) \subseteq (A \cup B) \setminus (A \cap B)$.

$\boxed{\supseteq}$ Neka je $x \in (A \cup B) \setminus (A \cap B)$. Imamo:

$$\begin{aligned} x \in (A \cup B) \setminus (A \cap B) &\Leftrightarrow (x \in A \cup B) \wedge (x \notin A \cap B) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge x \notin A \cap B \\ &\Leftrightarrow \underbrace{(x \in A \wedge x \notin A \cap B)}_{1^\circ} \vee \underbrace{(x \in B \wedge x \notin A \cap B)}_{2^\circ} \end{aligned}$$

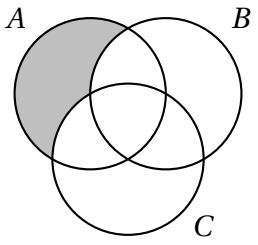
1°) Ako je $x \in A$ i $x \notin A \cap B$, onda je nužno $x \notin B$. Dakle, imamo $x \in A$ i $x \notin B$, tj. $x \in A \setminus B$.

2°) Ako je $x \in B$ i $x \notin A \cap B$, onda vrijedi $x \notin A$. Imamo $x \in B$ i $x \notin A$, tj. $x \in B \setminus A$.

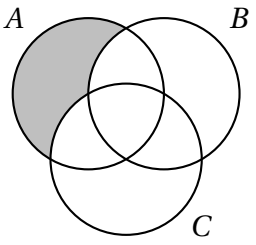
Kako mora vrijediti jedan od ova dva slučaja, zaključujemo $(x \in A \setminus B) \vee (x \in B \setminus A)$, odnosno $x \in (A \setminus B) \cup (B \setminus A)$.

Ovime smo dokazali $(A \cup B) \setminus (A \cap B) \subseteq (A \setminus B) \cup (B \setminus A)$ i dokaz je završen.

Rješenje 2.7 Skicirajmo Vennove dijagrame:



$A \setminus (B \cup C)$



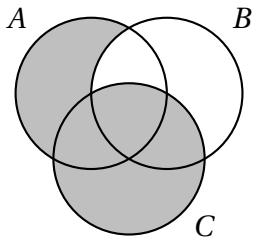
$(A \setminus B) \setminus C$

Imamo

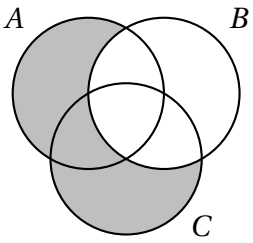
$$\begin{aligned} x \in A \setminus (B \cup C) &\Leftrightarrow x \in A \wedge x \notin B \cup C \\ &\Leftrightarrow x \in A \wedge (x \notin B \wedge x \notin C) \\ &\Leftrightarrow (x \in A \wedge x \notin B) \wedge x \notin C \\ &\Leftrightarrow (x \in A \setminus B) \wedge x \notin C \\ &\Leftrightarrow x \in (A \setminus B) \setminus C. \end{aligned}$$

Dakle, vrijedi $(\forall x)(x \in A \setminus (B \cup C) \Leftrightarrow x \in (A \setminus B) \setminus C)$, odnosno $A \setminus (B \cup B) = (A \setminus B) \setminus C$.

Rješenje 2.8 Za početak, skicirajmo Vennove dijagrame za ova dva skupa.



$(A \setminus B) \cup C$



$(A \cup C) \setminus B$

Sa slike naslućujemo da vrijedi $(A \setminus B) \cup C \not\subseteq (A \cup C) \setminus B$ i $(A \cup C) \setminus B \subseteq (A \setminus B) \cup C$.

$\boxed{\not\subseteq}$ Neka je $A = \emptyset$ i $B = C = \{1\}$. Tada je

$$(A \setminus B) \cup C = (\emptyset \setminus \{1\}) \cup \{1\} = \emptyset \cup \{1\} = \{1\}$$

i

$$(A \cup C) \setminus B = (\emptyset \cup \{1\}) \setminus \{1\} = \{1\} \setminus \{1\} = \emptyset.$$

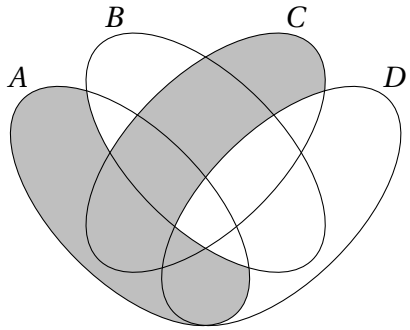
Kako očito vrijedi $\{1\} \not\subseteq \emptyset$, ovime smo pokazali $(A \setminus B) \cup C \not\subseteq (A \cup C) \setminus B$.

$\boxed{\supseteq}$ Imamo

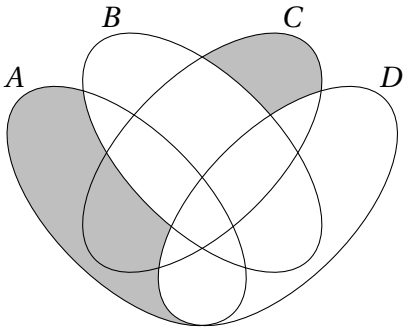
$$\begin{aligned} x \in (A \cup C) \setminus B &\Leftrightarrow (x \in A \cup C) \wedge x \notin B \\ &\Leftrightarrow (x \in A \vee x \in C) \wedge x \notin B \\ &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in C \wedge x \notin B) \\ &\Rightarrow (x \in A \setminus B) \vee x \in C \qquad (\text{zbog } P \wedge Q \Rightarrow P) \\ &\Leftrightarrow x \in (A \setminus B) \cup C. \end{aligned}$$

Dakle, $(A \cup C) \setminus B \subseteq (A \setminus B) \cup C$.

Rješenje 2.9 Skicirajmo Vennove dijagrame:



$(A \setminus B) \cup (C \setminus D)$



$(A \cup C) \setminus (B \cup D)$

Sa slike naslućujemo da vrijedi $(A \setminus B) \cup (C \setminus D) \supsetneq (A \cup C) \setminus (B \cup D)$.

$\boxed{\not\subseteq}$ Neka je

$$A = B = C = \{1\} \qquad \text{i} \qquad D = \emptyset.$$

Imamo

$$(A \setminus B) \cup (C \setminus D) = (\{1\} \setminus \{1\}) \cup (\{1\} \setminus \emptyset) = \emptyset \cup \{1\} = \{1\}$$

i

$$(A \cup C) \setminus (B \cup D) = (\{1\} \cup \{1\}) \setminus (\{1\} \cup \emptyset) = \{1\} \setminus \{1\} = \emptyset.$$

Očito $\{1\} \not\subseteq \emptyset$.

$\boxed{\supseteq}$ Vrijedi

$$\begin{aligned}
x \in (A \cup C) \setminus (B \cup D) &\Leftrightarrow (x \in A \cup C) \wedge (x \notin B \cup D) \\
&\Leftrightarrow (x \in A \vee x \in C) \wedge (x \notin B \wedge x \notin D) \\
&\Leftrightarrow (x \in A \wedge x \notin B \wedge x \notin D) \vee (x \in C \wedge x \notin B \wedge x \notin D) \\
&\Rightarrow (x \in A \wedge x \notin B) \vee (x \in C \wedge x \notin D) \\
&\Leftrightarrow (x \in A \setminus B) \vee (x \in C \setminus D) \\
&\Leftrightarrow x \in (A \setminus B) \cup (C \setminus D),
\end{aligned}$$

Dakle $(A \cup C) \setminus (B \cup D) \subseteq (A \setminus B) \cup (C \setminus D)$.

Rješenje 2.10

$\boxed{\subseteq}$ Pretpostavimo da je $x \in (A \cup B) \triangle C$. Razlikujemo dva slučaja:

1°) Ako je $x \in C$, tada $x \notin A \cup B$, pa $x \notin A$, pa je $x \in A \triangle C$. Dakle, $x \in (A \triangle C) \cup B$.

2°) Ako $x \notin C$, onda je $x \in A \cup B$. Ako je $x \in B$, onda je $x \in (A \triangle C) \cup B$. Ako $x \notin B$, onda je $x \in A$, pa je $x \in A \triangle C$, pa je $x \in (A \triangle C) \cup B$.

U oba slučaja došli smo do zaključka $x \in (A \triangle C) \cup B$, pa zaključujemo $(A \cup B) \triangle C \subseteq (A \triangle C) \cup B$.

$\boxed{\not\supseteq}$ Iz Vennovih dijagrama (nacrtajte ih sami) vidimo da regija koja pripada $(B \cap C) \setminus A$ leži u skupu $(A \triangle C) \cup B$ i ne leži u skupu $(A \cup B) \triangle C$. Stoga, da bismo našli protuprimjer, trebamo naći skupove A, B, C za koje je ta regija neprazna. Na primjer, to vrijedi za izbor skupova $A = \emptyset$, $B = C = \{1\}$. Lako izračunamo da vrijedi $(A \cup B) \triangle C = \emptyset$, $(A \triangle C) \cup B = \{1\} \neq \emptyset$. Dakle, ova inkluzija ne vrijedi općenito.

Rješenje 2.11 Najjednostavniji (i najnaporniji) način za dokazati ovu tvrdnju je da promotrimo 8 slučajeva, ovisno o tome u kojoj se "regiji" u Vennovom dijagramu nalazi x. To možemo prikazati tablično.

$x \in A$	$x \in B$	$x \in C$	$x \in A \triangle B$	$x \in (A \triangle B) \triangle C$	$x \in B \triangle C$	$x \in A \triangle (B \triangle C)$
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	1	1
0	1	1	1	0	0	0
1	0	0	1	1	0	1
1	0	1	1	0	1	0
1	1	0	0	0	1	0
1	1	1	0	1	0	1

Iz tablice vidimo da su sudovi $x \in (A \triangle B) \triangle C$ i $x \in A \triangle (B \triangle C)$ logički ekvivalentni, tj. vrijedi $A \triangle (B \triangle C) = (A \triangle B) \triangle C$.
Istu tabličnu metodu možemo primijeniti i inače, ali često je jednostavnije do zaključka doći bez promatranja svih 8 slučajeva (ili 2^n slučajeva ako imamo n varijabli).

Rješenje 2.12 Vrijedi

$$\begin{aligned}(x, y) \in A \times (B \cup C) &\Leftrightarrow x \in A \wedge y \in B \cup C \\ &\Leftrightarrow x \in A \wedge (y \in B \vee y \in C) \\ &\Leftrightarrow (x \in A \wedge y \in B) \vee (x \in A \wedge y \in C) \\ &\Leftrightarrow (x, y) \in (A \times B) \cup (A \times C).\end{aligned}$$

U trećem redu smo koristili svojstvo distributivnosti za logičke veznike $\wedge$ i $\vee$:

$$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R).$$

Rješenje 2.13 Neka je $(x,y) \in ((A \setminus C) \times (B \setminus D)) \cup ((C \setminus A) \times (D \setminus B))$. Tada imamo dva slučaja.

1. $(x,y) \in ((A \setminus C) \times (B \setminus D)$. Tada je $x \in A \setminus C$, $y \in B \setminus D$. Onda je $(x,y) \in A \times B$ i $(x,y) \notin C \times D$, pa je $(x,y) \in (A \times B) \triangle (C \times D)$.

2. $(x,y) \in (C \setminus A) \times (D \setminus B)$. Tada je $x \in C \setminus A$, $y \in D \setminus B$. Onda je $(x,y) \in C \times D$, $(x,y) \notin A \times B$, pa je $(x,y) \in (A \times B) \triangle (C \times D)$.

Zaključujemo da vrijedi inkluzija

$$((A \setminus C) \times (B \setminus D)) \cup ((C \setminus A) \times (D \setminus B)) \subseteq (A \times B) \triangle (C \times D)\,.$$

Neka je sada $(x,y) \in (A \times B) \triangle (C \times D)$. Tada je ili $(x,y) \in A \times B$ ili u $C \times D$.
Ako je $(x,y) \in A \times B$, onda $(x,y) \notin C \times D$. To znači da ili $x \notin C$ ili $x \notin D$. Međutim, jedno od tog dvoje može biti istina. Pa neka je $(x,y) \in A \times B$, $x \in C$, $y \notin D$.
Vidimo da je tada $(x,y) \in (A \times B) \triangle (C \times D)$, ali $(x,y) \notin (A \setminus C) \times (B \setminus D)$ te $(x,y) \notin (C \setminus A) \times (D \setminus B)$, jer x nije ni u $A \setminus C$ ni u $C \setminus A$. Dakle, naslućujemo da obratna inkluzija ne vrijedi, a dobili smo i ideju za protuprimjer.
Stavimo da je $A = C = \{1\}$, $B = \{2\}$, $D = \{3\}$. Promotrimo element $(1,2)$. On se nalazi u $A \times B$ i ne nalazi se u $C \times D$, pa se nalazi u skupu s desne strane. Međutim, skup s lijeve strane je prazan.
Zaključujemo da inkluzija

$$((A \setminus C) \times (B \setminus D)) \cup ((C \setminus A) \times (D \setminus B)) \supseteq (A \times B) \triangle (C \times D)\,.$$

ne vrijedi općenito.

Poglavlje 3

Relacije

3.1 Svojstva relacija

Definicija 3.1. Neka su A i B skupovi. Podskup $\rho \subseteq A \times B$ zovemo **relacija**.
Ako je $(a,b) \in \rho$, kažemo da je a u relaciji ρ sa b i pišemo $a \,\rho\, b$.
Ako $(a,b) \notin \rho$, kažemo da a nije u relaciji ρ sa b i pišemo $a \not\rho\, b$.

Relacije služe da iskažemo vezu koja postoji između elemenata.

Primjer 3.2.

1. Neki primjeri relacija na $\mathbb{R}$ su $\leq, <, \geq$ i $>$.
2. Ako je S skup, onda je $\subseteq$ relacija na $\mathscr{P}(S)$.
3. Na skupu prirodnih brojeva imamo relaciju djeljivosti.

Primjer 3.3.

1. Neka je S bilo koji skup. Tada je $=$ relacija na S.
2. Neka je $\mathscr{L}$ skup svih pravaca u ravnini. Definiramo relaciju paralelnosti $\sim$ sa
$$p \sim q \iff p \text{ i } q \text{ su paralelni.}$$
3. Na skupu $\mathbb{Z} \times \mathbb{N}$ definiramo relaciju $\sim$ sa
$$(a,b) \sim (c,d) \iff ad - bc = 0.$$

Definicija 3.4. Neka je ρ relacija na skupu A. Kažemo da je ρ:

- **refleksivna** ako za svaki $a \in A$ vrijedi $a \rho a$,
- **simetrična** ako za sve $a, b \in A$ takve da je $a \rho b$ vrijedi $b \rho a$,
- **antisimetrična** ako za sve različite $a, b \in A$ vrijedi $a \not\rho b$ ili $b \not\rho a$,
- **tranzitivna** ako za sve $a, b, c \in A$ takve da je $a \rho b$ i $b \rho c$ vrijedi $a \rho c$,
- **irefleksivna** ako za svaki $a \in A$ vrijedi $a \not\rho a$.

Napomena 3.5. Primijetimo da ako je A neprazan, relacija na A ne može istovremeno biti refleksivna i irefleksivna.

Zadatak 3.1 Za svaku od sljedećih relacija odredite je li refleksivna, simetrična, antisimetrična, tranzitivna, irefleksivna:

a) relacija $\leq$ na $\mathbb{R}$,

b) relacija $>$ na $\mathbb{R}$,

c) relacija paralelnosti na skupu pravaca u ravnini,

d) relacija djeljivosti na $\mathbb{N}$,

e) relacija djeljivosti na $\mathbb{Z} \setminus \{0\}$,

f) prazna relacija na skupu $\{1,2,3\}$,

g) relacija $A \times A$ na proizvoljnom skupu A koji ima barem dva elementa.

Zadatak 3.2 Na skupu $\{1,2,3,4\}$ dana je relacija

$$\rho = \{(1,2),(2,3),(3,4),(1,3),(2,4),(4,4),(1,4)\}.$$

Odredite je li ρ refleksivna, simetrična, antisimetrična, tranzitivna, irefleksivna.
U narednim zadacima, 'ispitati svojstva relacije' znači provjeriti je li relacija refleksivna, simetrična, antisimetrična, tranzitivna, irefleksivna.

Zadatak 3.3 Na skupu prirodnih brojeva definirana je relacija ρ sa

$$m \rho n \iff 3m \text{ i } 5n \text{ daju isti ostatak pri dijeljenju sa } 7.$$

Ispitajte svojstva ove relacije.

Definicija 3.6. Neka je ρ relacija. **Suprotna relacija** od ρ je relacija

$$\rho^{-1} := \{(y,x) \mid (x,y) \in \rho\}.$$

Primjer 3.7. $<$ je suprotna od $>$, $\leq$ je suprotna od $\geq$.

Zadatak 3.4 Neka je ρ relacija na A.

a) $\rho = \rho^{-1} \iff \rho$ je simetrična,

b) ρ je tranzitivna $\iff \rho^{-1}$ je tranzitivna,

c) ρ je antisimetrična $\iff \rho \cap \rho^{-1} \subseteq \{(x,x) \mid x \in A\}$.

Zadatak 3.5 Za svaku od sljedećih relacija na skupu realnih brojeva odredite njena svojstva:

(a) $x \lozenge y \iff x \cdot y = 0$,

(b) $x \,\delta\, y \iff x \cdot y \neq 0$,

(c) $x \otimes y \iff |x - y| < 5$,

(d) $x \circledcirc y \iff x^2 + y^2 = 1$,

(e) $x \,\rho\, y \iff x^2 + y^2 = 0$.

3.2 Relacije ekvivalencije

Definicija 3.8. Binarna relacija koja je refleksivna, simetrična i tranzitivna zove se **relacija ekvivalencije**.

Primjer 3.9. Relacije iz primjera 3.3 su relacije ekvivalencije.

Definicija 3.10. Neka je $\sim$ relacija ekvivalencije na nepraznom skupu A, te neka je $x \in A$. Skup

$$[x] := \{y \in A \mid x \sim y\}$$

zovemo **klasa ekvivalencije** elementa x. Nadalje, kažemo da je x **reprezentant** klase $[x]$.

Skup svih klasa ekvivalencije zovemo **kvocijentni skup** od $\sim$ i označavamo ga sa

$$A/_\sim := \{[x] \mid x \in A\}.$$

Teorem 3.11. Neka je $\sim$ relacija ekvivalencije na skupu A, te neka su $x, y \in A$ proizvoljni. Tada:

(a) $x \in [x]$;

(b) ako $x \not\sim y$, onda $[x] \cap [y] = \emptyset$;

(c) ako $x \sim y$, onda $[x] = [y]$.

Dokaz teorema 3.11.

(a) Kako je $\sim$ refleksivna, vrijedi $x \sim x$, pa je $x \in [x]$.

(b) Neka je $x \not\sim y$. Pretpostavimo suprotno, tj. $[x] \cap [y] \neq \emptyset$ i uzmimo $z \in [x] \cap [y]$. Tada je $x \sim z$ i $y \sim z$. Zbog simetričnosti od $\sim$ iz $y \sim z$ slijedi $z \sim y$. Sada imamo $x \sim z$ i $z \sim y$, pa zbog tranzitivnosti slijedi $x \sim y$. Kontradikcija. Dakle, vrijedi $[x] \cap [y] = \emptyset$.

(c) Neka je $x \sim y$ i $z \in [x]$. Iz $x \sim y$ zbog simetričnosti slijedi $y \sim x$, a iz $z \in [x]$ slijedi $x \sim z$. Zbog tranzitivnosti je tada $y \sim z$, tj. $z \in [y]$. Ako je $z \in [y]$, analogno iz $x \sim y$ i $y \sim z$ zaključujemo $x \sim z$, tj. $z \in [x]$. Dakle, vrijedi $[x] = [y]$. □

Napomena 3.12. Vrijede i obrati tvrdnji (b) i (c) iz teorema 3.11. Dokažite to!

Zadatak 3.6 Na skupu $\mathbb{N}$ zadana je relacija $\sim$ sa

$$m \sim n \iff m - n \text{ je paran cijeli broj.}$$

Dokažite da je $\sim$ relacija ekvivalencije i odredite klase ekvivalencije.

Zadatak 3.7 Odredite relaciju ekvivalencije $\sim$ na skupu A čije klase su $A/_\sim$, ako je:

(a) $A = \{1,2,3,4,5\}$, $A/_\sim = \big\{\{1,4,5\},\ \{2,3\}\big\}$;

(b) $A = \mathbb{N}$, $A/_\sim = \big\{\{n\} \mid n \in \mathbb{N}\big\}$;

(c) $A = \mathbb{R}$, $A/_\sim = \big\{[k, k+1\rangle \mid k \in \mathbb{Z}\big\}$.

Definicija 3.13. Neka je A skup. **Particija skupa** A je bilo koja familija skupova $\mathscr{F} \subseteq \mathscr{P}(A)$ sa sljedećim svojstvima:

(i) Za sve $X \in \mathscr{F}$ vrijedi $X \neq \emptyset$;

(ii) Za sve $X, Y \in \mathscr{F}$ vrijedi $X = Y$ ili $X \cap Y = \emptyset$;

(iii) $\bigcup_{X \in \mathscr{F}} X = A$.

Primjer 3.14.

1. $\mathscr{F}_1 = \{\{1,4,5\}, \{2,3\}\}$ je particija skupa $\{1,2,3,4,5\}$.

2. $\mathscr{F}_2 = \{\{2k \mid k \in \mathbb{N}\}, \{2k+1 \mid k \in \mathbb{N}\}\}$ je particija skupa prirodnih brojeva.
   $\mathscr{F}_3 = \{\{n\} \mid n \in \mathbb{N}\}$ je također particija skupa prirodnih brojeva.

3. $\mathscr{F}_4 = \{[k, k+1\rangle \mid k \in \mathbb{Z}\}$ je particija skupa $\mathbb{R}$.

Uočimo da su ovo točno kvocijentni skupovi iz zadataka 3.6 i 3.7!

Korolar 3.15. Neka je A neprazan skup i $\sim$ relacija ekvivalencije na A. Tada je kvocijentni skup $A/_\sim$ particija skupa A.

Dokaz korolara 3.15. Dokazujemo svojstva (i)-(iii) iz definicije 3.13 za familiju

$$\mathscr{F} = A/_\sim = \{[x] \mid x \in A\}.$$

Kako je $\sim$ refleksivna, za svaki $x \in A$ je $x \in [x]$, pa je $[x] \neq \emptyset$. Iz teorema 3.11 slijedi da za svake dvije klase $[x]$ i $[y]$ vrijedi $[x] = [y]$ ili $[x] \cap [y] = \emptyset$. Konačno, očito je $[x] \subseteq A$ za svaki $x \in A$, pa je i $\bigcup_{x \in A} [x] \subseteq A$. Obratno, za svaki $x \in A$ vrijedi $x \in [x] \subseteq \bigcup_{x \in A} [x]$, pa je $A \subseteq \bigcup_{x \in A} [x]$. □

Zadatak 3.8 Neka je A skup i neka je $\mathscr{F}$ particija skupa A. Definirajmo relaciju $\sim$ na skupu A sa

$$a \sim b \iff (\exists X \in \mathscr{F})(a \in X \wedge b \in X).$$

Dokažite da je $\sim$ relacija ekvivalencije na A i da vrijedi $A/_\sim = \mathscr{F}$.

Zadatak 3.9 Na skupu $\mathbb{N}$ zadana je relacija ρ sa

$$a \,\rho\, b \iff (\exists p \in \mathbb{P})(p \mid a \wedge p \mid b),$$

gdje je $\mathbb{P}$ skup prostih brojeva.

(a) Ispitajte svojstva relacije ρ. Je li ρ relacija ekvivalencije?

(b) Odredite najmanju relaciju ekvivalencije koja sadrži ρ.

Zadatak 3.10 Na skupu $\mathbb{Z} \times \mathbb{Z}$ zadana je relacija ρ na sljedeći način:

$$(a,b)\,\rho\,(c,d) \iff 2 \mid a-c \vee 3 \mid b-d.$$

(a) Ispitajte svojstva relacije ρ. Je li ρ relacija ekvivalencije?

(b) Odredite sve načine na koje se ρ može nadopuniti do relacije ekvivalencije.

Lema 3.16. Neka su A i B skupovi te $f\colon A \to B$ funkcija. Neka je $\sim$ relacija na A zadana s

$$x \sim y \iff f(x) = f(y).$$

Tada je $\sim$ relacija ekvivalencije.

Dokaz. Relacija je simetrična jer je $f(x) = f(y)$ ako i samo ako je $f(y) = f(x)$. Relacija je refleksivna jer $f(x) = f(x)$ vrijedi za svaki $x \in A$. Relacija je tranzitivna jer ako je $f(x) = f(y)$ i $f(y) = f(z)$, tada je i $f(x) = f(z)$. □

Zadatak 3.11 Neka je $S \neq \emptyset$ skup i $T \subseteq S$. Na skupu $\mathscr{P}(S)$ zadana je relacija ρ sa

$$A \,\rho\, B \iff A \cap T = B \cap T.$$

(a) Dokažite da je ρ relacija ekvivalencije.

(b) Za $S = \{1,2,3,4,5\}$ i $T = \{2,3,4\}$ odredite $[\{2,5\}]$.

Dokaz.

(a) Neka je $f : \mathscr{P}(S) \to \mathscr{P}(T)$ definirana s $f(A) = A \cap T$. Tada prema lemi 3.16 slijedi da je ρ relacija ekvivalencije, jer je $A \,\rho\, B$ ako i samo ako je $f(A) = f(B)$.

(b) Klasa $[\{2,5\}]$ sastoji se od svih podskupova A od S za koje je $A \cap \{2,3,4\} = \{2,5\} \cap \{2,3,4\} = \{2\}$. Dakle, klasa od $\{2,5\}$ se sastoji od svih skupova koji sadrže 2, a ne sadrže 3 i 4. Popišimo sve te skupove:

$$[\{2,5\}] = \{\{2\}, \{1,2\}, \{1,2,5\}, \{2,5\}\}.$$

□

3.3 Relacije parcijalnog uređaja

Definicija 3.17. Relacija ρ na skupu A koja je refleksivna, antisimetrična i tranzitivna zove se **relacija parcijalnog uređaja** ili jednostavno **parcijalni uređaj**.
Ako još vrijedi

$$(\forall x, y \in A)(x \rho y \vee y \rho x),$$

onda ρ zovemo **relacija totalnog uređaja** ili **totalni uređaj**.

Primjer 3.18. Relacije $\leq$, $\geq$, $\subseteq$ i $\mid$ iz primjera 3.2 su parcijalni uređaji. Pri tome su $\leq$ i $\geq$ totalni uređaji, a $\subseteq$ i $\mid$ nisu totalni uređaji.

Definicija 3.19. Relacija koja je irefleksivna i tranzitivna zove se **relacija strogog parcijalnog uređaja** ili jednostavno **strogi parcijalni uređaj**.

Primjer 3.20. Relacije $<$ i $>$ su strogi parcijalni uređaji.

Napomena 3.21. Svaka relacija koja je irefleksivna i tranzitivna je automatski i antisimetrična. Zaista, neka je ρ irefleksivna i tranzitivna relacija na skupu A. Ako su $x, y \in A$ različiti, onda mora vrijediti ili $x \not\rho y$ ili $y \not\rho x$; u suprotnom zbog tranzitivnosti slijedi $x \rho x$, što je nemoguće zbog irefleksivnosti od ρ.
Posebno, svaka relacija strogog parcijalnog uređaja je antisimetrična.

Zadatak 3.12 Neka su $\leq_1$ i $\leq_2$ parcijalni uređaji na nekom skupu A. Jesu li relacije $\leq_\cup$ definirana s $\leq_1 \cup \leq_2$ i $\leq_\cap$ definirana s $\leq_1 \cap \leq_2$ nužno parcijalni uređaji?

Zadatak 3.13

(a) Neka je ρ relacija strogog parcijalnog uređaja na skupu A. Neka je σ relacija na skupu A definirana s

$$x \sigma y \iff x = y \vee x \rho y.$$

Dokažite da je σ relacija parcijalnog uređaja.

(b) Neka je σ relacija parcijalnog uređaja na skupu A. Neka je ρ relacija na skupu A definirana s

$$x \rho y \iff x \sigma y \wedge x \neq y.$$

Dokažite da je ρ relacija strogog parcijalnog uređaja.

Definicija 3.22. Neka je ρ relacija parcijalnog uređaja na skupu A i neka je $B \subseteq A$. Kažemo da je $a \in A$ **donja međa** skupa B ako

$$(\forall b \in B)(a \,\rho\, b).$$

Kažemo da je element $a \in A$ **najveća donja međa** ili **infimum** skupa B i pišemo $a = \inf B$ ako vrijedi

(i) a je donja međa skupa B;

(ii) za svaku donju među $x \in A$ skupa B vrijedi $x \,\rho\, a$.

Ako vrijedi i $\inf B \in B$, kažemo da je $\inf B$ **najmanji element** skupa B.

Definicija 3.23. Neka je ρ relacija parcijalnog uređaja na skupu A i neka je $B \subseteq A$. Kažemo da je $a \in A$ **gornja međa** skupa B ako

$$(\forall b \in B)(b \,\rho\, a).$$

Kažemo da je element $a \in A$ **najmanja gornja međa** ili **supremum** skupa B i pišemo $a = \sup B$ ako vrijedi

(i) a je gornja međa skupa B;

(ii) za svaku gornju među $x \in A$ skupa B vrijedi $a \,\rho\, x$.

Ako vrijedi i $\sup B \in B$, kažemo da je $\sup B$ **najveći element** skupa B.

Zadatak 3.14 Na skupu $\mathbb{N} \times \mathbb{N}$ definirana je relacija ρ sa

$$(a,b) \,\rho\, (c,d) \iff a \mid c \,\wedge\, b \leq d.$$

(a) Dokažite da je ρ relacija parcijalnog uređaja.

(b) Ima li skup $\{(6,16),(9,12),(15,8)\}$ donju među (s obzirom na uređaj ρ)? Ima li infimum?

Zadatak 3.15 Na skupu $A = \{1,2,3,4\}$ dana je relacija ρ s

$$\rho = \{(1,1),(1,2),(1,3),(1,4),(2,2),(3,3),(3,4),(4,4)\}.$$

(a) Dokažite da je ρ relacija parcijalnog uređaja.

(b) Odredite sve donje međe skupa $\{3,4\}$. Ima li taj skup infimum?

(c) Odredite sve gornje međe skupa $\{2,3\}$. Ima li taj skup supremum?

(d) Odredite sve gornje međe skupa $\{1\}$. Ima li taj skup supremum?

Zadatak 3.16 Neka je A proizvoljan neprazan skup. Na skupu $\mathscr{A}$ svih particija od A definirana je relacija ρ s

$$\mathscr{F}_1 \rho \mathscr{F}_2 \iff (\forall X \in \mathscr{F}_1)(\exists Y \in \mathscr{F}_2)\, X \subseteq Y.$$

(a) Dokažite da je ρ relacija parcijalnog uređaja. Je li totalan uređaj?

(b) Postoje li u $(\mathscr{A}, \rho)$ najmanji i najveći element?

(c) U slučaju kada je $A = \{1,2,3,4\}$ odredite supremum i infimum skupa $\{\mathscr{F}_1, \mathscr{F}_2\}$ gdje su $\mathscr{F}_1 = \{\{1\},\{2\},\{3,4\}\}$ i $\mathscr{F}_2 = \{\{1\},\{2,3\},\{4\}\}$.

Upute za rješavanje zadataka

Uputa za Z3.2 Prikažite ρ grafički: tablično ili u koordinatnom sustavu.

Uputa za Z3.3 Pokušajte naći neke parove brojeva koji jesu u relaciji i iz toga zaključiti je li relacija refleksivna, irefleksivna, simetrična i tranzitivna. Uočite da su svi brojevi oblika $7n$ međusobno u relaciji.

Uputa za Z3.6 Refleksivnost, simetričnost i tranzitivnost dokažite direktno po definiciji. Možete iskoristiti činjenicu da, ako su p i q parni brojevi, onda su i $-p$ te $p+q$ parni.

Za određivanje klasa, uočite da su dva broja u relaciji akko su iste parnosti.

Uputa za Z3.7 Za (c), uočite da vrijedi $x, y \in [k, k+1\rangle$ akko je $\lfloor x \rfloor = \lfloor y \rfloor = k$.

Uputa za Z3.8 Dokažite refleksivnost, simetričnosti i tranzitivnost po definiciji. Iskoristite svojstva (i)-(iii) familije $\mathscr{F}$ iz definicije particije!

Uputa za Z3.9 Uočite da vrijedi $a \;\rho\; b$ akko a i b imaju zajednički prosti faktor. Za (b) podzadatak, provjerite koje parove brojeva treba dodati u ρ da bi ona bila refleksivna i tranzitivna. Možete iskoristiti činjenicu da za svaka dva prirodna broja $a, b > 1$ vrijedi (objasnite zašto!) $a \;\rho\; ab$ i $ab \;\rho\; b$.

Uputa za Z3.10 Za (b) podzadatak, možete iskoristiti činjenicu da za svaka dva uređena para (a,b) i (c,d) vrijedi (objasnite zašto!) $(a,b)\;\rho\;(a,d)$ i $(a,d)\;\rho\;(c,d)$.

Uputa za Z3.11 Za (a) podzadatak, iskoristite lemu 3.16. Za (b) podzadatak, iskoristite $\{2,5\}\;\rho\;A \iff A \cap \{2,3,4\} = \{2\}$.

Uputa za Z3.12 Za $\leq_\cup$: promotrite $\leq \cup \geq$ (uniju standardnih uređaja na $\mathbb{N}$). Je li to parcijalni uređaj?

Za $\leq_\cap$: dokažite po definiciji da je ova relacija refleksivna, tranzitivna i antisimetrična.

Uputa za Z3.14 Za (b) podzadatak: raspišite što znači da je (a,b) donja međa zadanog skupa. Koja donja međa je najveća?

Rješenja zadataka

Rješenje 3.1

a) Vrijedi $a \leq a$ za svaki a, pa je relacija refleksivna i nije irefleksivna. Ne postoje različiti $a, b \in \mathbb{R}$ takvi da je $a \leq b$ i $b \leq a$ pa je relacija antisimetrična. Vrijedi $1 \leq 2$ i $2 \not\leq 1$ pa relacija nije simetrična.

b) Slično kao i a), jedina razlika je da je ova relacija irefleksivna i da nije refleksivna.

c) Svaki pravac je paralelan sam sa sobom, pa je relacija refleksivna, i nije irefleksivna. Ako su p i q paralelni, tada su q i p paralelni, pa je relacija simetrična. Ako su p i q paralelni te su q i r paralelni, onda su p i r također paralelni, pa je relacija tranzitivna. Postoje dva različita paralelna pravca, pa relacija nije antisimetrična.

d) Svaki prirodan broj dijeli sam sebe, pa je relacija refleksivna i nije irefleksivna. Vrijedi $2 \mid 4$ i $4 \nmid 2$, pa relacija nije simetrična. Ako $a \mid b$ i $b \mid a$, tada je $a = b$ pa je relacija antisimetrična. Za tranzitivnost, prisjetimo se definicije djeljivosti:

$$a \mid b \text{ ako postoji cijeli broj } k \text{ takav da je } b = ka.$$

Neka su a, b, c takvi da $a \mid b$ i $b \mid c$. Tada postoje k, ℓ takvi da je $b = ka$, $c = \ell b$, pa je $c = k\ell a$ i $a \mid c$. Dakle, relacija jest tranzitivna.

e) Objašnjenja za sva svojstva osim antisimetričnosti su ista kao i u d) dijelu. Antisimetričnost ovdje ne vrijedi: $a \mid -a$ i $-a \mid a$ za svaki cijeli broj $a \neq 0$, pa relacija nije antisimetrična.

f) Označimo relaciju s ρ. Vrijedi $a \not\rho a$ za sve $a \in \{1, 2, 3\}$, pa je relacija irefleksivna, pa nije refleksivna. Kako ni ne postoje a, b, c takvi da je $a \rho b$ i $b \rho c$, relacija je trivijalno tranzitivna. Slično, kako ne postoje a, b takvi da je $a \rho b$, relacija je trivijalno simetrična.

Kako ne postoje različiti a, b takvi da je $a \rho b$, relacija je i antisimetrična.

g) Označimo s R ovu relaciju. Vrijedi aRa za svaki $a \in A$, pa je relacija refleksivna i nije irefleksivna. Ako je aRb. tada je i bRa, pa je relacija simetrična. Ako je aRb i bRc, onda je i aRc pa je relacija tranzitivna. Ako su $a \neq b$ elementi skupa A, tada je aRb i bRa, pa relacija nije antisimetrična.

Rješenje 3.2 Prikažimo ρ grafički na sljedeći način.

	1	2	3	4
1				
2				
3				
4				

Tablica 3.1: Relacija ρ

Interpretirajmo sada svojstva relacija u terminima tablica.

- relacija je refleksivna ako i samo ako je dijagonala cijela osjenčana,
- relacija je irefleksivna ako i samo ako je dijagonala cijela neosjenčana,
- relacija je simetrična ako i samo ako je tablica simetrična u odnosu na dijagonalu,
- relacija je antisimetrična ako i samo ako ne postoje dva polja u tablici koja su simetrična u odnosu na dijagonalu i oba osjenčana.

Za tranzitivnost nažalost nemamo vizualnu interpretaciju, već ju trebamo provjeriti direktno.
To znači da za sve a, b, c takve da je $a \rho b$ i $b \rho c$ treba provjeriti je li $a \rho c$. Provjerimo to u konkretnom slučaju:

- $1 \rho 2$ i $2 \rho 3$, te je $1 \rho 3$. ✓
- $1 \rho 2$ i $2 \rho 4$, te je $1 \rho 4$. ✓
- $1 \rho 3$ i $3 \rho 4$, te je $1 \rho 4$. ✓
- $1 \rho 4$ i $4 \rho 4$, te je $1 \rho 4$. ✓
- $2 \rho 3$ i $3 \rho 4$, te je $2 \rho 4$. ✓
- $3 \rho 4$ i $4 \rho 4$, te je $3 \rho 3$. ✓
- $4 \rho 4$ i $4 \rho 4$, te je $4 \rho 4$. ✓

Dakle, relacija jest tranzitivna.
Provjerimo sada ostala svojstva. Kako dijagonala nije cijela osjenčana i nije cijela neosjenčana, relacija nije ni refleksivna niti irefleksivna. Kako tablica nije simetrična u odnosu na dijagonalu (npr. $1 \rho 2$ i $2 \not\rho 1$), relacija nije simetrična. Kako ne postoje dva polja simetrična u odnosu na dijagonalu koja su oba obojena, relacija jest antisimetrična.

Rješenje 3.3 Ova relacija se na prvi pogled čini kompliciranа, pa je najbolji prvi korak u ovakvim zadacima izračunati za nekoliko parova jesu li u relaciji.
Za početak, vidimo $1 \not\rho\, 1$, $1\ \rho\ 2$, $2 \not\rho\, 1$, $2 \not\rho\, 2$. Iz toga odmah vidimo da ρ nije simetrična jer je $1\ \rho\ 2$ i $2 \not\rho\, 1$. Također, ρ nije refleksivna jer $1 \not\rho\, 1$.
Pokušajmo sada naći neki element koji je u relaciji s 2. Vidimo $2\ \rho\ 4$ jer $5 \cdot 4$ daje ostatak $6 = 2 \cdot 3$ pri dijeljenju sa 7. Sada imamo $1\ \rho\ 2$ i $2\ \rho\ 4$, ali $1 \not\rho\, 4$; naime, $3 \cdot 1$ i $5 \cdot 4$ ne daju isti ostatak pri dijeljenju sa 7. Dakle, ρ nije tranzitivna.
Preostaje provjeriti irefleksivnost i antisimetričnost. Za to, primijetimo da ako su m i n djeljivi sa 7, onda $3m$ i $5n$ daju ostatak 0 pri dijeljenju sa 7, pa je $m\ \rho\ n$. Dakle, svaka dva elementa djeljiva sa 7 su u relaciji.
Onda posebno imamo $7\ \rho\ 7$, pa relacija nije irefleksivna, te $7\ \rho\ 14$ i $14\ \rho\ 7$, pa relacija nije antisimetrična.

Rješenje 3.4 Primijetimo prvo da vrijedi $(\rho^{-1})^{-1} = \rho$. To je jasno iz definicije suprotne relacije.

a) $\boxed{\Rightarrow}$ Pretpostavimo da je $\rho = \rho^{-1}$. Dokažimo da je ρ simetrična.
Neka je $(x, y) \in \rho$. Tada je prema pretpostavci $(x, y) \in \rho^{-1}$, pa je $(y, x) \in \rho$. Dakle, ρ je simetrična.

$\boxed{\Leftarrow}$ Pretpostavimo da je ρ simetrična. Treba dokazati da je $\rho^{-1} = \rho$.
Neka je $(x, y) \in \rho^{-1}$. Tada je $(y, x) \in \rho$, pa je $(x, y) \in \rho$ jer je ρ simetrična. Dakle, $\rho^{-1} \subseteq \rho$.
Neka je $(x, y) \in \rho$. Tada je $(y, x) \in \rho$ jer je ρ simetrična, pa je $(x, y) \in \rho^{-1}$. Dakle, $\rho \subseteq \rho^{-1}$. Kako smo dokazali obje inkuzije, zaključujemo $\rho = \rho^{-1}$.

b) Primijetimo prvo da vrijedi $(\rho^{-1})^{-1} = \rho$. To je jasno iz definicije suprotne relacije. Stoga je samo dovoljno dokazati da ako je ρ tranzitivna, onda je ρ^{-1} tranzitivna, jer drugi smjer slijedi primjenom prvog smjera na relaciju ρ^{-1}.

Neka je ρ tranzitivna. Neka su a, b, c takvi da je $(a, b) \in \rho^{-1}$, $(b, c) \in \rho^{-1}$. Treba dokazati da je $(a, c) \in \rho^{-1}$.

Iz $(a, b) \in \rho^{-1}, (b, c) \in \rho^{-1}$ slijedi $(c, b) \in \rho$, $(b, a) \in \rho$. Primjenom tranzitivnosti od ρ slijedi $(c, a) \in \rho$, odnosno $(a, c) \in \rho^{-1}$, pa je tranzitivnost od ρ^{-1} dokazana.

c) $\boxed{\Rightarrow}$ Pretpostavimo da je ρ antisimetrična.
Neka je $(x, y) \in \rho \cap \rho^{-1}$. Treba dokazati da je $(x, y) \in \{(a, a) \mid a \in A\}$, odnosno da je $x = y$.
Pretpostavimo suprotno, da je $x \neq y$. Imamo $(x, y) \in \rho$, $(x, y) \in \rho^{-1}$, odnosno $(x, y) \in \rho$, $(y, x) \in \rho$, kontradikcija s antisimetričnošću od ρ. Dakle, $x = y$.

$\boxed{\Leftarrow}$ Pretpostavimo da je $\rho \cap \rho^{-1}$ sadržano u $\{(a,a) \mid a \in A\}$. Treba dokazati da je ρ antisimetrična.

Pretpostavimo suprotno. Tada postoje različiti x, y takvi da je $(x,y) \in \rho$ i $(y,x) \in \rho$. Onda je $(x,y) \in \rho$ i $(x,y) \in \rho^{-1}$, pa je $(x,y) \in \{(a,a) \mid a \in A\}$, odnosno $x = y$, kontradikcija. Stoga, ρ je antisimetrična.

Rješenje 3.5 Primijetimo prvo da su sve relacije simetrične, jer zamjena x i y u definiciji bilo koje relacije ne mijenja relaciju.
Provjerimo sada refleksivnost i irefleksivnost. Vrijedi $1 \cdot 1 \neq 0$, pa $\diamondsuit$ nije refleksivna. Slično, $0 \cdot 0 = 0$, pa δ nije refleksivna. Iz istih razloga vidimo da $\diamondsuit$ i δ nisu irefleksivne.
Relacija $\otimes$ je refleksivna (te onda nije irefleksivna) jer je $|x - x| = 0 < 5$ za svaki $x \in \mathbb{R}$.
Relacija $\circledcirc$ nije refleksivna i nije irefleksivna, jer je $1^2 + 1^2 \neq 1$ i

$$\left(\frac{1}{\sqrt{2}}\right)^2 + \left(\frac{1}{\sqrt{2}}\right)^2 = 1.$$

Relacija ρ nije refleksivna jer je $1^2 + 1^2 \neq 0$, i nije irefleksivna jer je $0^2 + 0^2 = 0$.
Provjerimo sada tranzitivnost. Relacija $\diamondsuit$ nije tranzitivna, jer je $1 \cdot 0 = 0$ i $0 \cdot 1$ ali $1 \cdot 1 \neq 0$.
Relacija δ jest tranzitivna, jer ako su $a, b, c \in \mathbb{R}$ brojevi takvi da je $a \cdot b \neq 0$, $b \cdot c \neq 0$, tada je i $a \cdot c \neq 0$. Relacija $\otimes$ nije tranzitivna. Naime, $|5-1| < 5$, $|1-0| < 5$ ali $|5-0| \geq 5$.
Relacija $\circledcirc$ također nije tranzitivna, jer je $0^2 + 1^2 = 1$, $1^2 + 0^2 = 1$ ali $0^2 + 0^2 \neq 1$. Konačno, relacija ρ jest tranzitivna. Naime, ako su $a, b, c \in \mathbb{R}$ takvi da je $a^2 + b^2 = b^2 + c^2 = 0$, onda je $a = b = c = 0$, pa je i $a^2 + c^2 = 0$.
Još treba provjeriti antisimetričnost. Relacija ρ jest antisimetrična, jer je jedini par koji je u relaciji $(0,0)$, pa ne postoje različiti $a, b \in \mathbb{R}$ u relaciji ρ.
Za ostale relacije, možemo naći različite a, b koji su u relaciji. Kako je svaka od tih relacija simetrična, onda su i b, a u relaciji. Dakle, relacije nisu antisimetrične.
Ovdje smo zapravo koristili sljedeći princip koji slijedi iz prethodnog zadatka: neprazna simetrična relacija koja nije sadržana u relaciji jednakosti nije antisimetrična.

Rješenje 3.6 Za svaki $n \in \mathbb{N}$ vrijedi da je $n - n = 0$ paran, tj. $n \sim n$. Dakle, relacija $\sim$ je refleksivna. Ako vrijedi $m \sim n$, tj. $m - n$ je paran, onda je i $-(m-n) = n - m$ paran, pa vrijedi $n \sim m$. Dakle, relacija $\sim$ je simetrična. Konačno, ako vrijedi $m \sim n$ i $n \sim p$, onda su brojevi $m-n$ i $n-p$ parni, pa je i njihov zbroj $(m-n)+(n-p) = m-p$ paran, tj. vrijedi $m \sim p$. Dakle, relacija $\sim$ je tranzitivna.
Odredimo sada klase ekvivalencije. Uočimo da za bilo koja dva parna broja $2k$ i $2l$ vrijedi $2k - 2l = 2(k-l)$, odnosno $2k \sim 2l$. Dakle, svi parni brojevi su međusobno u relaciji $\sim$. Imamo

$$[2] = [4] = [6] = \ldots = \{2k \mid k \in \mathbb{N}\}.$$

Nadalje, za bilo koja dva neparna broja $2k+1$ i $2l+1$ vrijedi $(2k+1)-(2l+1)=2(k-l)$, tj. $2k+1 \sim 2l+1$. Dakle, svi neparni brojevi su međusobno u relaciji $\sim$. Imamo

$$[1] = [3] = [5] = \ldots = \{2k+1 \mid k \in \mathbb{N}\}.$$

Možemo pisati

$$\mathbb{N}/_\sim = \big\{\{2k \mid k \in \mathbb{N}\},\ \{2k+1 \mid k \in \mathbb{N}\}\big\}$$

Rješenje 3.7

(a) Imamo $[1] = [4] = [5] = \{1,4,5\}$ i $[2] = [3] = \{2,3\}$. Tražena relacija je

$$\sim = \big\{(1,1),(1,4),(1,5),(4,1),(4,4),(4,5),(5,1),(5,4)(5,5),(2,2),(2,3),(3,2),(3,3)\big\}.$$

(b) Kvocijentni skup je $A/_\sim = \{\{1\},\{2\},\{3\},\ldots\}$, pa imamo $[1] = \{1\}$, $[2] = \{2\}$, $[3] = \{3\}$ itd. Vidimo da je svaki prirodan broj jedini element svoje klase, tj. svaki broj je u relaciji jedino sam sa sobom. Dakle, tražena relacija je

$$\sim = \{(n,n) \mid n \in \mathbb{N}\},$$

tj. relacija jednakosti $\mathbb{N}$.

(c) Kvocijentni skup je $A/_\sim = \{\ldots,[-1,0\rangle,[0,1\rangle,[1,2\rangle,\ldots\}$. Uočimo: ako je $x \in [k,k+1\rangle$, onda je k najveći cijeli broj koji je manji ili jednak od x, tj. $k = \lfloor x \rfloor$. Isto vrijedi za sve elemente intervala $[k,k+1\rangle$. Dva realna broja x i y su u relaciji $\sim$ ako i samo ako su elementi istog intervala, tj. ako i samo ako je $\lfloor x \rfloor = \lfloor y \rfloor$. Tražena relacija je

$$\sim = \{(x,y) \mid \lfloor x \rfloor = \lfloor y \rfloor\}.$$

Rješenje 3.8 Neka je $a \in A$. Kako je $\bigcup_{X \in \mathscr{F}} X = A$, postoji $X \in \mathscr{F}$ takav da je $a \in X$. Vrijedi

$$(\exists X \in \mathscr{F})(a \in X \wedge a \in X),$$

tj. $a \sim a$. Dakle, $\sim$ je refleksivna.
Pretpostavimo da vrijedi $a \sim b$. Tada postoji $X \in \mathscr{F}$ takav da je $a \in X$ i $b \in X$. Zbog komutativnosti konjunkcije automatski vrijedi i

$$(\exists X \in \mathscr{F})(b \in X \wedge a \in X),$$

tj. $b \sim a$. Dakle, $\sim$ je simetrična.

Pretpostavimo da vrijedi $a \sim b$ i $b \sim c$. Zbog $a \sim b$ postoji $X \in \mathscr{F}$ takav da je $a \in X$ i $b \in X$. Nadalje, zbog $b \sim c$ postoji $Y \in \mathscr{F}$ takav da je $b \in Y$ i $c \in Y$. Kako je $b \in X \cap Y$, skup $X \cap Y$ je neprazan, pa prema svojstvu (ii) iz definicije 3.13 slijedi $X = Y$. Sada imamo

$$(\exists X \in \mathscr{F})(a \in X \wedge c \in X),$$

tj. $a \sim c$. Dakle, $\sim$ je tranzitivna.
Neka je $X \in \mathscr{F}$. Kako je X neprazan, postoji $a \in X$. Budući da je $a \sim b \Leftrightarrow b \in X$, vrijedi $X = [a]$. Obratno, svaki $a \in A$ se mora nalaziti u nekom skupu $X \in \mathscr{F}$, i tada vrijedi $[a] = X$. Dakle, klase ekvivalencije su točno elementi od $\mathscr{F}$, tj. $A/_\sim = \mathscr{F}$.

Rješenje 3.9 Uočimo: vrijedi $a \rho b$ akko postoji prost broj koji dijeli i a i b, tj. akko a i b imaju zajednički prosti faktor.

(a) Relacija nije refleksivna jer $1 \not\rho 1$. Samim time nije relacija ekvivalencije.

Relacija nije irefleksivna jer $2 \rho 2$.

Relacija nije tranzitivna jer 2 i 6 imaju zajednički prosti faktor, 6 i 3 imaju zajednički prosti faktor, ali 2 i 3 nemaju zajednički prosti faktor.

Relacija jest simetrična jer zamjena uloga a i b ne utječe na definiciju relacije.

Relacija nije antisimetrična, jer je $2 \rho 6$ i $6 \rho 2$.

(b) Trebamo naći najmanju relaciju koja je nadskup od ρ i koja je relacija ekvivalencije. To možemo ekvivalentno opisati kao presjek svih relacija koje sadrže ρ i koje su relacije ekvivalencije, jer je presjek relacija ekvivalencije također relacija ekvivalencije.

Neka je $\sim$ bilo koja relacija ekvivalencije koja je nadskup od ρ. Relacija $\sim$ je refleksivna, pa je $1 \sim 1$.

Nadalje, neka su a i b prirodni brojevi veći od 1. Primijetimo sljedeće: $a \rho ab$ i $ab \rho b$. Onda vrijedi i $a \sim ab$, $ab \sim b$, pa zaključujemo $a \sim b$.

Dakle, za sada smo dokazali sljedeće: svaka relacija ekvivalencije koja sadrži ρ sadrži i skup (relaciju)

$$R = \{(1,1)\} \cup \{(a,b) \mid a,b \in \mathbb{N}, a,b > 1\}.$$

Sada primijetimo da je R relacija ekvivalencije na $\mathbb{N}$ čije klase su $\{1\}$ i $\mathbb{N} \setminus \{1\}$, pa je R tražena relacija ekvivalencije.

Rješenje 3.10

(a) Relacija je refleksivna jer $2 \mid a-a$, pa je $(a,b)\ \rho\ (a,b)$ za sve $(a,b) \in \mathbb{Z}\times\mathbb{Z}$. Odmah slijedi da nije irefleksivna.

Relacija nije tranzitivna. Naime, $(0,0)\ \rho\ (0,1)$ jer $2 \mid 0-0$ i $(0,1)\ \rho\ (1,1)$ jer $3 \mid 1-1$, ali $(0,0) \not\rho (1,1)$. Dakle, nije ni relacija ekvivalencije.

Relacija je simetrična jer $2 \mid a-c$ ako i samo ako $2 \mid c-a$ te $3 \mid b-d$ ako i samo ako $3 \mid d-b$.

Relacija nije antisimetrična jer je $(0,0)\ \rho\ (0,1)$ i $(0,1)\ \rho\ (0,0)$.

(b) Neka su (a,b) i (c,d) parovi cijelih brojeva. Tada je $(a,b)\ \rho\ (a,d)$ i $(a,d)\ \rho\ (c,d)$. Ako je $\sim$ bilo koja relacija ekvivalencije koja je nadskup od ρ, vrijedi $(a,b)\sim(a,d)$ i $(a,d)\sim(c,d)$, pa zbog tranzitivnosti vrijedi $(a,b)\sim(c,d)$. Dakle, $\sim$ je nužno jednaka cijelom Kartezijevom produktu $\mathbb{Z}\times\mathbb{Z}$.

Kako je $\mathbb{Z}\times\mathbb{Z}$ relacija ekvivalencije, zaključujemo da se ρ na jedinstven način može proširiti do relacije ekvivalencije.

Rješenje 3.12 Unija dva parcijalna uređaja svakako ne mora biti parcijalni uređaj. Na primjer, uzmimo uređaje " $\leq$ " i " $\geq$ " na $\mathbb{N}$. Tada je njihova unija cijeli Kartezijev produkt $\mathbb{N}\times\mathbb{N}$, što nije antisimetrična relacija.
Dokažimo da presjek dva parcijalna uređaja $\leq_1$ i $\leq_2$ jest parcijalan uređaj. Primijetimo $a \leq_\cap b$ ako i samo ako je $a \leq_1 b$ i $a \leq_2 b$.
Refleksivnost je sada jasna jer $a \leq_1 a$ i $a \leq_2 a$ vrijedi za svaki $a \in A$.
Dokažimo antisimetričnost. Ako je $a \leq_\cap b$ i $b \leq_\cap a$, onda je $a \leq_1 b$ i $b \leq_1 a$, pa je $a = b$ jer je $\leq_1$ antisimetrična.
Konačno, provjerimo tranzitivnost. Neka su a,b,c takvi da je $a \leq_\cap b$, $b \leq_\cap c$. Tada je $a \leq_i b$, $b \leq_i c$ za $i = 1,2$, pa je $a \leq_i c$ za $i = 1,2$ odnosno $a \leq_\cap c$.

Rješenje 3.13

(a) Relacija ρ je po pretpostavci zadatka irefleksivna i tranzitivna. Treba dokazati da je relacija σ refleksivna, antisimetrična i tranzitivna.

Za svaki $x \in A$ vrijedi $x = x$, pa onda vrijedi i $x = x \ \vee\ x\ \rho\ x$, tj. $x\ \sigma\ x$. Dakle, relacija σ je refleksivna.

Pretpostavimo da su $x, y \in A$ takvi da je $x \neq y$ i $x\ \sigma\ y$. Tada nužno vrijedi $x\ \rho\ y$. Kad bi vrijedilo $y\ \sigma\ x$, na isti način bismo mogli zaključiti $y\ \rho\ x$. Zbog tranzitivnosti od ρ bi tada vrijedilo $x\ \rho\ x$, što je nemoguće jer je ρ irefleksivna. Dakle, za različite $x, y \in A$ vrijedi ili $x \not\sigma\ y$ ili $y \not\sigma\ x$, tj. σ je antisimetrična.

Pretpostavimo da su $x, y, z \in A$ takvi da vrijedi $x \sigma y$ i $y \sigma z$. Ako je $x = y$ ili $y = z$, automatski vrijedi i $x \sigma z$. U suprotnom vrijedi $x \rho y$ i $y \rho z$, pa zbog tranzitivnosti od ρ slijedi $x \rho z$, što povlači $x \sigma z$. Dakle, σ je tranzitivna.

(b) Relacija σ je po pretpostavci zadatka refleksivna, antisimetrična i tranzitivna. Treba dokazati da je ρ irefleksivna i tranzitivna.

Irefleksivnost je očita: niti za jedan $x \in A$ ne vrijedi $x \neq x$, pa ne može vrijediti $x \rho x$.

Pretpostavimo da su $x, y, z \in A$ takvi da vrijedi $x \rho y$ i $y \rho z$. Tada je $x \sigma y$ i $x \neq y$ te $y \sigma z$ i $y \neq z$. Kad bi vrijedilo $x = z$, imali bismo $x \sigma y$ i $y \sigma x$, što je nemoguće jer je $x \neq y$ i σ je antisimetrična. Dakle, vrijedi $x \neq z$. Nadalje, $x \sigma z$ slijedi iz $x \sigma y$ i $y \sigma z$ zbog tranzitivnosti od σ. Dakle, vrijedi $x \rho z$, pa je ρ tranzitivna.

Rješenje 3.14

(a) Treba dokazati da je ρ refleksivna, antisimetrična i tranzitivna.

Neka je $(a, b) \in \mathbb{N} \times \mathbb{N}$. Budući da vrijedi $a \mid a$ i $b \leq b$, vrijedi $(a, b)\ \rho\ (a, b)$. Dakle, ρ je refleksivna.

Pretpostavimo da za neke $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ vrijedi $(a, b)\ \rho\ (c, d)$ i $(c, d)\ \rho\ (a, b)$. Tada imamo $a \mid c$, $b \leq d$, $c \mid a$ i $d \leq b$. Zbog antisimetričnosti relacija $\mid$ i $\leq$ vrijedi $a = c$ i $b = d$, tj. $(a, b) = (c, d)$. Dakle, ρ je antisimetrična.

Pretpostavimo da za neke $(a, b), (c, d), (e, f) \in \mathbb{N} \times \mathbb{N}$ vrijedi $(a, b)\ \rho\ (c, d)$ i $(c, d)\ \rho\ (e, f)$. Tada imamo $a \mid c$, $b \leq d$, $c \mid e$ i $d \leq f$. Zbog tranzitivnosti relacija $\mid$ i $\leq$ vrijedi $a \mid e$ i $b \leq f$, tj. $(a, b)\ \rho\ (e, f)$. Dakle, ρ je tranzitivna.

(b) Element (a, b) je donja međa skupa $\{(6, 16), (9, 12), (15, 8)\}$ ako i samo ako vrijedi

$$(a, b)\ \rho\ (6, 16), \qquad (a, b)\ \rho\ (9, 12) \quad \text{i} \quad (a, b)\ \rho\ (15, 8),$$

odnosno ako i samo ako vrijedi

$$a \mid 6, \quad b \leq 16, \quad a \mid 9, \quad b \leq 12, \quad a \mid 15 \quad \text{i} \quad b \leq 8.$$

To će vrijediti za bilo koji $a \in \{1, 3\}$ i $b \leq 8$. Npr. $(1, 1)$ je jedna donja međa zadanog skupa.

Tvrdimo da je $(3, 8)$ infimum zadanog skupa. Zaista, $(3, 8)$ prema gore navedenim uvjetima jest donja međa, te za bilo koju drugu donju među (a, b) vrijedi $a \mid 3$ i $b \leq 8$, tj. $(a, b)\ \rho\ (3, 8)$. Dakle, $(3, 8)$ je najveća donja međa skupa $\{(6, 16), (9, 12), (15, 8)\}$.

Rješenje 3.15

(a) Pokažite po definiciji da je ρ refleksivna, antisimetrična i tranzitivna. (DZ)

(b) Ako je $a \in A$ donja međa od $\{3,4\}$ mora vrijediti $a\rho 3$ i $a\rho 4$. Vidimo da to svojstvo imaju $a = 1$ i $a = 3$. Pokažimo da je 3 najveća donja međa. Trebamo provjeriti da za sve donje međe a danog skupa vrijedi $a\rho 3$. To očito vrijedi jer je $1\rho 3$ i $3\rho 3$.

(c) Ako je $a \in A$ gornja međa od $\{2,3\}$ mora vrijediti $2\rho a$ i $3\rho a$. Takav element ne postoji pa je skup gornjih međa prazan te skup nema supremum.

(d) Za svaki $a \in A$ vrijedi $1\rho a$ pa je svaki element u A gornja međa za $\{1\}$. Kada bi neki $a \in A$ bio supremum moralo bi vrijediti $a\rho x$ za svaki $x \in A$. Vidimo da $a = 1$ ima to svojstvo pa je to supremum danog skupa.

Rješenje 3.16

(a) Treba dokazati da je ρ refleksivna, antisimetrična i tranzitivna.

Neka je $\mathscr{F} \in \mathscr{A}$. Za bilo koji $X \in \mathscr{A}$ možemo uzeti $Y = X$ pa je $\mathscr{F}\rho\mathscr{F}$. Dakle, ρ je refleksivna.

Pretpostavimo da za neke $\mathscr{F}_1, \mathscr{F}_2 \in \mathscr{A}$ vrijedi $\mathscr{F}_1\rho\mathscr{F}_2$ i $\mathscr{F}_2\rho\mathscr{F}_1$. Uzmimo $X \in \mathscr{F}_1$. Tada postoji $Y \in \mathscr{F}_2$ takav da je $X \subseteq Y$. Za taj Y postoji $Z \in \mathscr{F}_1$ takav da je $Y \subseteq Z$ pa je i $X \subseteq Y \subseteq Z$. Kako je $\mathscr{F}_1$ particija mora biti $X = Z$ pa je i $X = Y \in \mathscr{F}_2$. Zaključujemo $\mathscr{F}_1 \subseteq \mathscr{F}_2$ i analogno dobijemo $\mathscr{F}_2 \subseteq \mathscr{F}_1$. Dakle, $\mathscr{F}_1 = \mathscr{F}_2$ pa je ρ antisimetrična.

Pretpostavimo da za neke $\mathscr{F}_1, \mathscr{F}_2, \mathscr{F}_3 \in \mathscr{A}$ imamo $\mathscr{F}_1\rho\mathscr{F}_2$ i $\mathscr{F}_2\rho\mathscr{F}_3$. Za $X \in \mathscr{F}_1$ postoji $Y \in \mathscr{F}_2$ takav da $X \subseteq Y$, a za taj Y postoji $Z \in \mathscr{F}_3$ takav da je $Y \subseteq Z$. Slijedi $X \subseteq Z$ pa je $\mathscr{F}_1\rho\mathscr{F}_3$.

Ako je A jednočlan, $A = \{a\}$ jedina particija je $\{\{a\}\}$ pa je tada uređaj očito totalan. Ako je A dvočlan, $A = \{a,b\}$ particije su $\mathscr{F}_1 = \{\{a\},\{b\}\}$ i $\mathscr{F}_2 = \{\{a,b\}\}$ te tada očito vrijedi $\mathscr{F}_1\rho\mathscr{F}_2$ pa je i u ovom slučaju uređaj totalan.

Promotrimo sada slučaj kada A ima neka tri različita elementa a,b,c. Uzmimo particije $\mathscr{F}_1 = \{\{a\},\{b,c\}, A \setminus \{a,b,c\}\}$ i $\mathscr{F}_2 = \{\{a,b\},\{c\}, A \setminus \{a,b,c\}\}$. Tada ne postoji $Y \in \mathscr{F}_2$ takav da je $\{b,c\} \subseteq Y$ pa $\mathscr{F}_1 \not\mathscr{F}_2$. Slično, ne postoji $Y \in \mathscr{F}_1$ takav da je $\{a,b\} \subseteq Y$ pa $\mathscr{F}_2 \not\mathscr{F}_1$. Dakle, u ovom slučaju uređaj nije totalan.

(b) Pokažimo da je $\mathscr{F} = \{\{a\} : a \in A\}$ najmanji element u $(\mathscr{A}, \rho)$. Primijetimo prvo da je očito $\mathscr{F} \in \mathscr{A}$. Pokažimo da je $\mathscr{F} = \inf\mathscr{A}$.

Pokažimo prvo da je $\mathscr{F}$ donja međa. Neka je $\mathscr{H} \in \mathscr{A}$ proizvoljna particija. Tada je $\mathscr{F}\rho\mathscr{H}$. Zaista, ako je $X = \{a\}$ za neki $a \in A$, kako je $\mathscr{H}$ particija mora postojati $Y \in \mathscr{H}$ takav da je $a \in Y$, tj. $\{a\} \subseteq Y$.

Pokažimo da je $\mathscr{F}$ najveća donja međa. Neka je $\mathscr{H} \in \mathscr{A}$ proizvoljna donja međa za $\mathscr{A}$. Kako je $\mathscr{F} \in \mathscr{A}$ posebno imamo $\mathscr{H}\rho\mathscr{F}$. Slijedi tvrdnja.

Slično se pokaže da je $\mathscr{G} = \{A\}$ najveći element (DZ).

(c) Pokažimo da je $\sup\{\mathscr{F}_1, \mathscr{F}_2\} = \{\{1\}, \{2,3,4\}\} = \mathscr{F}$. Primijetimo da je $\mathscr{F}_1\rho\mathscr{F}$ i $\mathscr{F}_2\rho\mathscr{F}$ pa je $\mathscr{F}$ jedna gornja međa za $\{\mathscr{F}_1, \mathscr{F}_2\}$. Pokažimo da je ujedno i najmanja gornja međa, odnosno supremum. Neka je $\mathscr{H}$ proizvoljna gornja međa. Tada je $\mathscr{F}_1\rho\mathscr{H}$ i $\mathscr{F}_2\rho\mathscr{H}$. Trebamo pokazati da je $\mathscr{F}\rho\mathscr{H}$. Kako je $\mathscr{H}$ particija jasno je da postoji $Y \in \mathscr{H}$ takav da je $\{1\} \subseteq Y$. Kako je $\mathscr{F}_1\rho\mathscr{H}$ postoji $Y \in \mathscr{H}$ takav da je $\{3,4\} \subseteq Y$, a kako je $\mathscr{F}_2\rho\mathscr{H}$ postoji $Z \in \mathscr{H}$ takav da je $\{2,3\} \subseteq Z$. Tada je $Y \cap Z \neq \emptyset$ pa kako je $\mathscr{H}$ particija mora biti $Y = Z$. Dakle, $\{2,3,4\} \subseteq Y$. Slijedi tvrdnja.

Slično se pokaže da je $\mathscr{G} = \{\{1\}, \{2\}, \{3\}, \{4\}\}$ infimum (DZ).

Poglavlje 4

Matematička indukcija

Aksiom matematičke indukcije. Neka je $S \subseteq \mathbb{N}$ takav da:

(i) $1 \in S$;

(ii) $(\forall n \in \mathbb{N})(n \in S \implies n+1 \in S)$.

Tada je $S = \mathbb{N}$.

Aksiom matematičke indukcije koristit ćemo kada želimo dokazati da neka tvrdnja vrijedi za sve prirodne brojeve. Najčešće ćemo ga koristiti u sljedećem obliku:

Teorem 4.1 (Princip matematičke indukcije)**.** Neka je $P(n)$ predikat koji ovisi o prirodnom broju $n \in \mathbb{N}$. Neka vrijedi:

BAZA: $P(1)$ je istina.

KORAK: Ako je $P(n)$ istina za neki $n \in \mathbb{N}$, onda je i $P(n+1)$ istina.

Tada je $P(n)$ istina za sve prirodne brojeve n, tj. vrijedi $(\forall n \in \mathbb{N})P(n)$.

Dokaz. Definirajmo skup $S := \{n \in \mathbb{N} \mid P(n) \text{ je istina}\}$. Tada iz BAZE slijedi $1 \in S$, a iz KORAKA slijedi $(\forall n \in \mathbb{N})(n \in S \implies n+1 \in S)$. Prema aksiomu matematičke indukcije tada vrijedi $S = \mathbb{N}$, što je upravo tvrdnja teorema. □

Zadatak 4.1 Dokažite da za sve prirodne brojeve n vrijedi

$$\sum_{i=1}^{n} i = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Zadatak 4.2 Dokažite da za sve prirodne brojeve n vrijedi

$$\sum_{i=1}^{n}(2i-1) = 1+3+\ldots+(2n-1) = n^2.$$

Zadatak 4.3 Dokažite da za sve prirodne brojeve n vrijedi

$$\sum_{i=1}^{n} i^2 = 1^2+2^2+\ldots+n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Zadatak 4.4 Dokažite da je broj $3^{2n+2}-8n-9$ djeljiv sa 64 za svaki cijeli broj $n \geq 0$.

Zadatak 4.5 Dokažite da je broj $11^{n+2}+12^{2n+1}$ djeljiv sa 133 za svaki cijeli broj $n \geq 0$.

Zadatak 4.6 Dokažite da je broj $37^{n+2}+16^{n+1}+23^n$ djeljiv sa 7 za svaki cijeli broj $n \geq 0$.

Varijante principa matematičke indukcije

Neka je $P(n)$ predikat koji ovisi o prirodnom broju n.

(1) Neka je $m \in \mathbb{Z}$. Ako vrijedi:

BAZA: $P(m)$ je istina.

KORAK: Ako je $P(n)$ istina za neki $n \geq m$, onda je i $P(n+1)$ istina.

Tada je $P(n)$ istina za sve cijele brojeve brojeve $n \geq m$.

(2) Neka vrijedi:

BAZA: $P(1)$ i $P(2)$ je istina.

KORAK: Ako je $P(n)$ istina za neki $n \in \mathbb{N}$, onda je i $P(n+2)$ istina.

Tada je $P(n)$ istina za sve prirodne brojeve n.

(3) (**Potpuna** ili **jaka indukcija**) Neka vrijedi:

BAZA: $P(1)$ je istina.

KORAK: Ako je $P(k)$ istina za sve prirodne brojeve k manje ili jednake od nekog $n \in \mathbb{N}$, onda je i $P(n+1)$ istina.

Tada je $P(n)$ istina za sve prirodne brojeve n.

Zadatak 4.7 U nekom restoranu brze hrane, pileći medaljoni prodaju se u pakiranjama od 3 ili od 5 komada. Dokažite da se za svaki prirodan broj $n \geq 8$ može naručiti točno n medaljona.

Zadatak 4.8 Dokažite da je $2^n > 10n^2$ za svaki prirodan broj $n \geq 10$.

Zadatak 4.9 Dokažite da za svaki prirodan broj n veći od 1 vrijedi

$$\frac{n}{2} < 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n - 1} < n.$$

Zadatak 4.10 Dokažite da za svaki prirodan broj n veći od 1 vrijedi

$$\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots + \frac{1}{n^2} < \frac{n-1}{n}.$$

Zadatak 4.11 Dokažite da za svaki prirodan broj n vrijedi

$$\frac{1}{2\sqrt{n}} \leq \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \cdots \cdot \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}.$$

Zadatak 4.12 Dokažite da za svaki prirodan broj n vrijedi

$$\underbrace{\sqrt{4 + \sqrt{4 + \sqrt{\cdots + \sqrt{4}}}}}_{n \text{ korijena}} < 3.$$

Zadatak 4.13 Dokažite da za svaki $n \in \mathbb{N}$ vrijedi

$$1 + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{n} \leq \frac{n^2 + 3n}{4}.$$

Zadatak 4.14 Dokažite da vrijedi

$$\sum_{i=1}^{2025} i \cdot 2^{i-1} = 1 + 2 \cdot 2 + 3 \cdot 2^2 + \cdots + 2025 \cdot 2^{2024} = 2024 \cdot 2^{2025} + 1.$$

Zadatak 4.15 Dokažite da za sve $a, b > 0$ i za svaki prirodan broj n vrijedi

$$2^{n-1}(a^n + b^n) \geq (a+b)^n.$$

Zadatak 4.16 Dokažite da za svaki prirodan broj n vrijedi

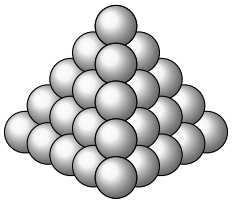
$$\underbrace{\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}_{n \text{ korijena}} = 2\cos\frac{\pi}{2^{n+1}}.$$

i uočite $a_{n+1} = \sqrt{2+a_n}$. U koraku indukcije možete iskoristiti $\cos 2x = 2\cos^2 x - 1$.

Zadatak 4.17 Neka je $x \in \mathbb{R} \setminus \{0\}$ takav da je $x + \frac{1}{x}$ cijeli broj. Dokažite da je za svaki $n \in \mathbb{N}$ broj $x^n + \frac{1}{x^n}$ cijeli.

Zadatak 4.18 Dokažite da za svaki prirodan broj n vrijedi da je umnožak bilo kojih n uzastopnih brojeva djeljiv s $n!$.

Zadatak 4.19 Kuglice su složene u pravilnu trostranu piramidu tako da je n kuglica duž svakog brida (vidi sliku 4.1). Dokažite da se piramida sastoji od $\frac{1}{6}n(n+1)(n+2)$ kuglica.



Slika 4.1: Piramida za $n = 5$

Zadatak 4.20 Dokažite da se za svaki prirodan broj n ploča dimenzija $2^n \times 2^n$ kojoj je otklonjen jedan kut može popločati trominama oblika  .

Zadatak 4.21 U nekoj državi postoji n gradova. Između svaka dva grada postoji jedna jednosmjerna cesta. Dokažite da postoji ruta kojom možemo obići svih n gradova tako da svaki posjetimo točno jednom.

Zadatak 4.22 Neka je $n \geq 2$ prirodan broj te neka su $A_1, A_2, \ldots, A_n$ skupovi. Dokažite da se element x nalazi u skupu

$$A_1 \triangle A_2 \triangle \ldots \triangle A_n$$

ako i samo ako za neparno mnogo indeksa $i \in \{1, 2, \ldots, n\}$ vrijedi $x \in A_i$.

Zadatak 4.23 Neka je $\leq$ bilo koji parcijalni uređaj na konačnom skupu S. Dokažite da se $\leq$ može proširiti do totalnog uređaja na S.

Cauchyjeva indukcija ili **indukcija unaprijed-unatrag**

Neka je $P(n)$ predikat koji ovisi o prirodnom broju n i neka vrijedi:

BAZA: $P(2)$ je istina.

KORAK 1: Ako je $P(2^n)$ istina za neki prirodan broj $n \in \mathbb{N}$, onda je i $P(2^{n+1})$ istina.

KORAK 2: Ako je $P(n)$ istina za neki prirodan broj $n \geq 2$, onda je i $P(n-1)$ istina.

Tada je $P(n)$ istina za sve prirodne brojeve n.

Zadatak 4.24 (Aritmetičko-geometrijska nejednakost) Neka su $x_1, \ldots, x_n \geq 0$. Tada vrijedi

$$\sqrt[n]{x_1 \cdots x_n} \leq \frac{x_1 + \cdots + x_n}{n}.$$

Upute za rješavanje zadataka

Uputa za Z4.4 U dokazu koraka, "namjestite" izraz uz 3^{2n+4} tako da dobijete izraz iz pretpostavke.

Uputa za Z4.9 Uočite da suma iz zadatka za $n+1$ ima 2^n pribrojnika više nego suma za n. U koraku indukcije iskoristite $\frac{1}{2^n} > \frac{1}{2^n+1} > \cdots > \frac{1}{2^{n+1}-1} > \frac{1}{2^{n+1}}$.

Uputa za Z4.12 Označite zadani izraz s n korijena sa a_n i uočite $a_{n+1} = \sqrt{4+a_n}$.

Uputa za Z4.14 Formulirajte tvrdnju za općeniti n tako da se zadana tvrdnja dobije uvrštavanjem $n = 2025$ i dokažite indukcijom tu općenitu tvrdnju. Tada očito vrijedi i zadana tvrdnja.

Uputa za Z4.16 Označite $a_n := \underbrace{\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}_{n \text{ korijena}}$

Uputa za Z4.17 Tvrdnju dokažite jakom indukcijom

Uputa za Z4.18 Tvrdnju dokažite indukcijom po n. Za dokaz tvrdnje u koraku indukcije iskoristite indukciju po k.

Uputa za Z4.19 Uočite da je svaki "sloj" piramide jednakostranični trokut sa k kuglica duž stranice, za $k = n, n-1, n-2, \ldots, 1$. Nadalje, piramida sa $n+1$ slojeva se sastoji od jednakostraničnog trokuta s $n+1$ kuglica duž stranice na dnu, na kojeg je dodana piramida s n slojeva. Koliko je kuglica potrebno za jednakostranični trokut?

Uputa za Z4.20 U koraku indukcije podijelite ploču dimenzija $2^{n+1} \times 2^{n+1}$ na četiri manje ploče dimenzija $2^n \times 2^n$. Jednoj od te četiri ploče je uklonjen jedan kut. Možete li krenuti s popločavanjem tako da svakoj od preostale tri ploče "zauzmete" jedan kut?

Uputa za Z4.21 Tvrdnju dokažite jakom indukcijom. U koraku indukcije, pokušajte podijeliti gradove $G_1, \ldots, G_n$ u dvije skupine tako da sigurno postoji ruta $R_1 \to G_{n+1} \to R_2$, pri čemu R_1 obilazi sve gradove iz prve skupine, a R_2 obilazi sve gradove iz druge skupine.

Uputa za Z4.22 U koraku indukcije, promatrajte $A_1 \triangle A_2 \triangle \ldots \triangle A_{n+1}$ kao simetričnu razliku dva skupa $(A_1 \triangle A_2 \triangle \ldots \triangle A_n) \triangle A_{n+1}$. Iskoristite definiciju simetrične razlike i pretpostavku indukcije.

Uputa za Z4.23 Uočite sljedeće: u svakom konačnom skupu s parcijalnim uređajem postoji element od kojeg nijedan drugi element nije strogo veći, tj. postoji *maksimalni* element. U koraku indukcije primijenite pretpostavku indukcije na skup svih elemenata osim maksimalnog, i zatim proširite taj uređaj i na maksimalni element.

Rješenja zadataka

Rješenje 4.1 Tvrdnju dokazujemo pomoću principa matematičke indukcije.
Za $n = 1$ vrijedi $1 = \frac{1(1+1)}{2}$.
Pretpostavimo da tvrdnja vrijedi za neki $n \in \mathbb{N}$, tj. da je

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

Tada je

$$1 + 2 + \ldots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2},$$

tj. tvrdnja vrijedi i za $n+1$.
Prema principu matematičke indukcije tvrdnja vrijedi za sve $n \in \mathbb{N}$.

Rješenje 4.2 Tvrdnju dokazujemo pomoću principa matematičke indukcije.
Za $n = 1$ vrijedi $2 \cdot 1 - 1 = 1 = 1^2$.
Pretpostavimo da tvrdnja vrijedi za neki $n \in \mathbb{N}$, tj. da je

$$1 + 3 + \ldots + (2n-1) = n^2.$$

Tada je

$$1 + 3 + \ldots + (2n-1) + (2(n+1)-1) = n^2 + (2n+1) = (n+1)^2,$$

tj. tvrdnja vrijedi i za $n+1$.
Prema principu matematičke indukcije tvrdnja vrijedi za sve $n \in \mathbb{N}$.

Rješenje 4.3 Tvrdnju dokazujemo pomoću principa matematičke indukcije.
Za $n = 1$ vrijedi $1^2 = 1 = \frac{1(1+1)(2 \cdot 1 + 1)}{6}$.
Pretpostavimo da tvrdnja vrijedi za neki $n \in \mathbb{N}$, tj. da je

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Tada je

$$\begin{aligned}1^2+2^2+\ldots+n^2+(n+1)^2 &= \frac{n(n+1)(2n+1)}{6}+(n+1)^2\\ &= \frac{n(n+1)(2n+1)+6(n+1)^2}{6}\\ &= \frac{(n+1)(2n^2+n+6n+6)}{6}\\ &= \frac{(n+1)(2n^2+7n+6)}{6}.\end{aligned}$$

S druge strane, vrijedi

$$\begin{aligned}\frac{(n+1)(n+2)(2(n+1)+1)}{6} &= \frac{(n+1)(n+2)(2n+3)}{6}\\ &= \frac{(n+1)(2n^2+7n+6)}{6},\end{aligned}$$

pa je $1^2+2^2+\ldots+n^2+(n+1)^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6}$ tj. tvrdnja vrijedi i za $n+1$.
Prema principu matematičke indukcije, tvrdnja vrijedi za sve $n \in \mathbb{N}$.

Rješenje 4.4 Tvrdnju dokazujemo pomoću principa matematičke indukcije.
Za $n=0$ vrijedi $3^{2\cdot 0+2}-8\cdot 0-9=9-9=0$, pa zbog $64 \mid 0$ tvrdnja vrijedi za $n=0$.
Pretpostavimo da za neki cijeli broj $n \geq 0$ vrijedi da $64 \mid 3^{2n+2}-8n-9$, tj. postoji cijeli broj k takav da je $3^{2n+2}-8n-9=64k$. Računamo:

$$\begin{aligned}3^{2(n+1)+2}-8(n+1)-9 &= 3^{2n+4}-8n-8-9\\ &= 3^2(3^{2n+2}-8n-9)+3^2\cdot 8n+3^2\cdot 9-8n-17\\ &= 9\cdot 64k+64n+64 = 64(9k+n+1).\end{aligned}$$

Dakle, $64 \mid 3^{2(n+1)+2}-8(n+1)-9$.
Prema principu matematičke indukcije tvrdnja vrijedi za sve cijele brojeve $n \geq 0$.

Rješenje 4.7 Za $n=8$ možemo naručiti po jedno pakiranje od 5 i od 3 medaljona. Za $n=9$ možemo naručiti tri pakiranja po 3 medaljona. Za $n=10$ možemo naručiti dva pakiranja po 5 medaljona.
Pretpostavimo da za neki $n \geq 8$ možemo naručiti točno n medaljona. Tada naručivanjem jednog dodatnog pakiranja od 3 medaljona dobivamo narudžbu od $n+3$ medaljona.
Prema principu matematičke indukcije tvrdnja vrijedi za svaki prirodan broj $n \geq 8$.

Rješenje 4.8 Za $n = 10$ vrijedi $1024 = 2^{10} > 10 \cdot 10^2 = 1000$.
Pretpostavimo da za neki prirodan broj $n > 10$ vrijedi $2^n > 10n^2$. Treba dokazati da je tada $2^{n+1} > 10(n+1)^2$. Zbog pretpostavke imamo $2^{n+1} = 2 \cdot 2^n > 2 \cdot 10n^2$, pa je dovoljno dokazati da je $2 \cdot 10n^2 > 10(n+1)^2$.
Vrijedi

$$\begin{aligned} 20n^2 > 10(n+1)^2 \quad &\Leftrightarrow \quad 2n^2 > n^2 + 2n + 1 \\ &\Leftrightarrow \quad n^2 - 2n - 1 > 0 \\ &\Leftrightarrow \quad (n-1)^2 > 2. \end{aligned}$$

Za $n \geq 10$ je $(n-1)^2 > 9^2 = 81 > 2$, pa vrijedi $2 \cdot 10n^2 > 10(n+1)^2$.
Po principu matematičke indukcije tvrdnja vrijedi za sve prirodne brojeve $n \geq 10$.

Rješenje 4.9 Za $n = 2$ zadana tvrdnja glasi

$$\frac{2}{2} < 1 + \frac{1}{2} + \frac{1}{3} < 2,$$

odnosno

$$1 < \frac{11}{6} < 2$$

što je očito istina.
Pretpostavimo da za neki prirodan broj $n \geq 2$ vrijedi

$$\frac{n}{2} < 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n - 1} < n.$$

Treba dokazati

$$\frac{n+1}{2} < \underbrace{1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n - 1}}_{=:S_1} + \underbrace{\frac{1}{2^n} + \cdots + \frac{1}{2^{n+1} - 1}}_{=:S_2} < n + 1.$$

Iz pretpostavke znamo da je $\frac{n}{2} < S_1 < n$. Još treba pokazati da je $\frac{1}{2} < S_2 < 1$. Uočimo:

$$\frac{1}{2^n} > \frac{1}{2^n + 1} > \cdots > \frac{1}{2^{n+1} - 1} > \frac{1}{2^{n+1}}.$$

Dakle, suma S_2 se sastoji od $(2^{n+1} - 1) - (2^n - 1) = 2^{n+1} - 2^n = 2^n$ pribrojnika koji su svi veći od $\frac{1}{2^{n+1}}$ i manji ili jednaki od $\frac{1}{2^n}$. Stoga vrijedi

$$2^n \cdot \frac{1}{2^{n+1}} < S_2 \leq 2^n \cdot \frac{1}{2^n},$$

odnosno

$$\frac{1}{2} < S_2 \leq 1$$

što je i trebalo pokazati.
Po principu matematičke indukcije tvrdnja vrijedi za sve prirodne brojeve $n \geq 2$.

Rješenje 4.10 Za $n = 2$ zadana tvrdnja glasi

$$\frac{1}{2^2} < \frac{1}{2},$$

što je očito istina.
Pretpostavimo da za neki prirodan broj $n \geq 2$ vrijedi

$$\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots + \frac{1}{n^2} < \frac{n-1}{n}.$$

Treba dokazati

$$\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots + \frac{1}{(n+1)^2} < \frac{n}{n+1}.$$

Po pretpostavci imamo:

$$\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots + \frac{1}{(n+1)^2} < \frac{n-1}{n} + \frac{1}{(n+1)^2}$$

pa je dovoljno dokazati

$$\frac{n-1}{n} + \frac{1}{(n+1)^2} \leq \frac{n}{n+1}.$$

Raspisom se dobije da je ta nejednakost ekvivalentna s $1 \geq 0$ koja je očito istinita.
Po principu matematičke indukcije tvrdnja vrijedi za sve prirodne brojeve $n \geq 2$.

Rješenje 4.11 Za $n = 1$ tvrdnja glasi:

$$\frac{1}{2} \leq \frac{1}{2} \leq \frac{1}{\sqrt{4}},$$

koja je očito istinita. Pretpostavimo da za neki prirodan broj n vrijedi:

$$\frac{1}{2\sqrt{n}} \leq \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \cdots \cdot \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}.$$

Trebamo dokazati:

$$\frac{1}{2\sqrt{n+1}} \leq \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \cdots \cdot \frac{2(n+1)-1}{2(n+1)} \leq \frac{1}{\sqrt{3(n+1)+1}}.$$

Po pretpostavci znamo:

$$\frac{1}{2\sqrt{n}}\cdot\frac{2n+1}{2n+2}\leq\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\cdot\ldots\cdot\frac{2n+1}{2n+2}\leq\frac{1}{\sqrt{3n+1}}\cdot\frac{2n+1}{2n+2}.$$

Vidimo da je dovoljno dokazati da vrijedi:

$$\frac{1}{2\sqrt{n+1}}\leq\frac{1}{2\sqrt{n}}\cdot\frac{2n+1}{2n+2}\quad\text{i}\quad\frac{1}{\sqrt{3n+1}}\cdot\frac{2n+1}{2n+2}\leq\frac{1}{\sqrt{3n+4}}.$$

Kvadriranjem i sređivanjem izraza se dobije da je prva nejednakost ekvivalentna s $n\geq -1$ što je očito istina te slično za drugu nejednakost (DZ).

Rješenje 4.12 Označimo $a_n := \underbrace{\sqrt{4+\sqrt{4+\sqrt{\cdots+\sqrt{4}}}}}_{n \text{ korijena}}$. Tada je $a_{n+1}=\sqrt{4+a_n}$ za svaki $n\in\mathbb{N}$.
Za $n=1$ imamo $a_1=\sqrt{4}=2$, što je očito manje od 3. Dakle, tvrdnja vrijedi za $n=1$.
Pretpostavimo da za neki $n\in\mathbb{N}$ vrijedi $a_n<3$. Tada je

$$a_{n+1}=\sqrt{4+a_n}<\sqrt{4+3}=\sqrt{7}<3.$$

Po principu matematičke indukcije za svaki $n\in\mathbb{N}$ vrijedi $a_n<3$, što je upravo tvrdnja zadatka.

Rješenje 4.13 Za $n=1$ vrijedi

$$1\leq\frac{1^2+3\cdot 1}{4}=1.$$

Pretpostavimo da za neki $n\in\mathbb{N}$ vrijedi

$$1+\sqrt{2}+\sqrt{3}+\cdots+\sqrt{n}\leq\frac{n^2+3n}{4}.$$

Tada je

$$1+\sqrt{2}+\sqrt{3}+\cdots+\sqrt{n}+\sqrt{n+1}\leq\frac{n^2+3n}{4}+\sqrt{n+1}.$$

Dovoljno je dokazati

$$\frac{n^2+3n}{4}+\sqrt{n+1}\leq\frac{(n+1)^2+3(n+1)}{4}.\qquad(\bigstar)$$

Kako je

$$\frac{(n+1)^2+3(n+1)}{4}=\frac{n^2+2n+1+3n+3}{4}=\frac{n^2+3n}{4}+\frac{n+2}{2},$$

treba dokazati

$$\sqrt{n+1} \leq \frac{n+2}{2}, \qquad (\spadesuit)$$

što je ekvivalentno s

$$(\sqrt{n+1})^2 - 2\sqrt{n+1} + 1 \geq 0,$$

odnosno

$$(\sqrt{n+1} - 1)^2 \geq 0.$$

Kako je kvadrat realnog broja nenegativan, ovo je očito istina, pa stoga vrijedi i ($\spadesuit$), što povlači ($\bigstar$). Dakle, tražena tvrdnja vrijedi za $n+1$.
Po principu matematičke indukcije tvrdnja vrijedi za sve $n \in \mathbb{N}$.

Rješenje 4.14 Dokazat ćemo da za svaki $n \in \mathbb{N}$ vrijedi

$$\sum_{i=1}^{n} i \cdot 2^{i-1} = 1 + 2 \cdot 2 + 3 \cdot 2^2 + \cdots + n \cdot 2^{n-1} = (n-1) \cdot 2^n + 1.$$

Za $n = 1$ tvrdnja glasi $1 = 0 \cdot 2^1 + 1$, što je očito istina.
Pretpostavimo da tvrdnja vrijedi za neki $n \in \mathbb{N}$. Tada je

$$\begin{aligned} 1 + 2 \cdot 2 + 3 \cdot 2^2 + \cdots + n \cdot 2^{n-1} + (n+1) \cdot 2^n &= (n-1) \cdot 2^n + 1 + (n+1) \cdot 2^n \\ &= 2^n \cdot 2n + 1 \\ &= 2^{n+1} \cdot n + 1. \end{aligned}$$

Dakle, tvrdnja vrijedi i za $n+1$.
Po principu matematičke indukcije tvrdnja vrijedi za sve $n \in \mathbb{N}$, pa onda posebno vrijedi i za $n = 2025$.

Rješenje 4.15 Neka su $a, b > 0$ proizvoljni. Matematičkom indukcijom dokazujemo

$$(\forall n \in \mathbb{N})(2^{n-1}(a^n + b^n)) \geq (a+b)^n).$$

Baza za $n = 1$ je očito ispunjena: $2^0(a^1 + b^1) \geq (a+b)^1$.
Pretpostavimo da za neki $n \in \mathbb{N}$ vrijedi $2^{n-1}(a^n + b^n)) \geq (a+b)^n$. Imamo:

$$(a+b)^{n+1} = (a+b)^b(a+b) \leq 2^{n-1}(a^n + b^n)(a+b) = 2^{n-1}(a^{n+1} + b^{n+1} + a^n b + ab^n)$$

Dovoljno je dokazati:

$$\begin{aligned} 2^{n-1}(a^{n+1} + b^{n+1} + a^n b + ab^n) &\leq 2^n(a^{n+1} + b^{n+1}) \\ \Leftrightarrow a^{n+1} + b^{n+1} + a^n b + ab^n &\leq 2(a^{n+1} + b^{n+1}) \\ \Leftrightarrow a^{n+1} + b^{n+1} - a^n b - ab^n &\geq 0 \\ \Leftrightarrow (a^n - b^n)(a-b) &\geq 0. \end{aligned}$$

Promotrimo dva slučaja:

(i) ako je $a \geq b$, tada je $a^n \geq b^n$ pa je $(a^n - b^n)(a-b) \geq 0$;

(ii) ako je $a < b$, tada je $a^n < b^n$ pa je $(a^n - b^n)(a-b) \geq 0$.

Dakle, u svakom slučaju vrijedi $(a^n - b^n)(a-b) \geq 0$ čime smo dokazali $2^{n-1}(a^{n+1} + b^{n+1} + a^n b + ab^n) \leq 2^n(a^{n+1} + b^{n+1})$. Dakle,

$$(a+b)^{n+1} \leq 2^{n-1}(a^{n+1} + b^{n+1} + a^n b + ab^n) \leq 2^n(a^{n+1} + b^{n+1}).$$

Po principu matematičke indukcije tvrdnja vrijedi $\forall n \in \mathbb{N}$.

Rješenje 4.16 Označimo sa a_n broj $\underbrace{\sqrt{2+\sqrt{2+\ldots+\sqrt{2}}}}_{n \text{ korijena}}$. Tada vidimo da vrijedi $a_1 = \sqrt{2}$ i

$$a_{n+1} = \sqrt{2+a_n}.$$

Matematičkom indukcijom dokazujemo da je $a_n = 2\cos\frac{\pi}{2^{n+1}}$ za svaki $nin\mathbb{N}$. Za $n = 1$ tvrdnja vrijedi jer je $\sqrt{2} = 2\cos\frac{\pi}{4}$.
Pretpostavimo da $a_n = 2\cos\frac{\pi}{2^{n+1}}$ vrijedi za neki prirodan broj $n \geq 1$.
Treba dokazati

$$a_{n+1} = 2\cos\frac{\pi}{2^{n+2}}.$$

Vrijedi

$$\begin{aligned} a_{n+1} &= \sqrt{2+a_n} \\ &= \sqrt{2+2\cos\frac{\pi}{2^{n+1}}} \\ &= \sqrt{2+2\left(2\cos^2\frac{\pi}{2^{n+2}} - 1\right)} \\ &= \sqrt{4\cos^2\frac{\pi}{2^{n+2}}} \\ &= 2\cos\frac{\pi}{2^{n+2}}, \end{aligned}$$

kao što je i trebalo dokazati. Ovdje smo u drugom redu koristili pretpostavku indukcije, u trećem redu identitet $\cos(2x) = 2\cos^2 x - 1$, i u zadnjem redu činjenicu da je $\cos x \geq 0$ za $x \in [0, \frac{\pi}{2}]$ (pa možemo uzeti korijen bez apsolutnih vrijednosti).

Rješenje 4.17 Tvdrnju ćemo dokazati jakom indukcijom po n.
Za $n = 1$ tvrdnja vrijedi po pretpostavci zadatka. Pretpostavimo da tvrdnja vrijedi za sve $k \leq n$. Tada je i broj

$$\left(x + \frac{1}{x}\right)\left(x^n + \frac{1}{x^n}\right) = x^{n+1} + \frac{1}{x^{n+1}} + x^{n-1} + \frac{1}{x^{n-1}}$$

cijeli kao umnožak dva cijela broja. Kako je $n-1 \leq n$ imamo da je i

$$x^{n-1} + \frac{1}{x^{n-1}}$$

cijeli broj (ovo vrijedi i za $n = 1$) pa je

$$x^{n+1} + \frac{1}{x^{n+1}} = \left(x + \frac{1}{x}\right)\left(x^n + \frac{1}{x^n}\right) - \left(x^{n-1} + \frac{1}{x^{n-1}}\right)$$

cijeli broj kao razlika dva cijela broja.

Rješenje 4.18 Trebamo dokazati sljedeću tvrdnju:

Za svaki prirodan broj n i za svaki prirodan broj k, broj $k \cdot (k+1) \cdot \ldots \cdot (k+n-1)$ je djeljiv s $n!$.

Dokazat ćemo tvrdnju indukcijom po n.
Za $n = 1$, treba dokazati da je svaki prirodan broj k djeljiv s $1!$, što je očito.
Pretpostavimo da za neki prirodan broj vrijedi sljedeća tvrdnja:

Za svaki prirodan broj k, broj $k \cdot (k+1) \cdot \ldots \cdot (k+n-1)$ je djeljiv s $n!$.

Da bismo proveli korak indukcije, potrebno je dokazati sljedeću tvrdnju:

Za svaki prirodan broj k, broj $k \cdot (k+1) \cdot \ldots \cdot (k+n-1) \cdot (k+n)$ je djeljiv s $(n+1)!$.

Tu tvrdnju ćemo dokazati indukcijom po k. Za $k = 1$, tvrdnja je očita jer je $1 \cdot 2 \cdot \ldots \cdot n \cdot (n+1) = (n+1)!$ svakako djeljivo s $(n+1)!$.
Pretpostavimo sada da za neki prirodan broj k vrijedi sljedeća tvrdnja:

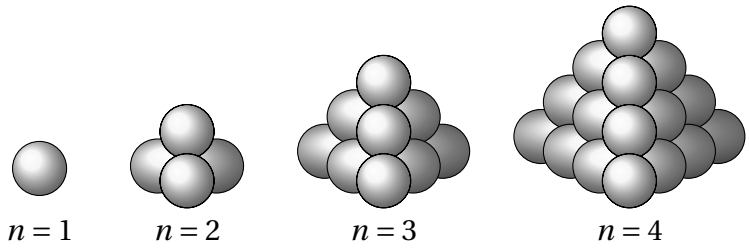
Broj $k \cdot (k+1) \cdot \ldots \cdot (k+n-1) \cdot (k+n)$ je djeljiv s $(n+1)!$.

Promotrimo broj $(k+1) \cdot (k+2) \cdot \ldots \cdot (k+n) \cdot (k+n+1)$. Rastavljanjem posljednje zagrade na dva dijela, možemo ga zapisati kao

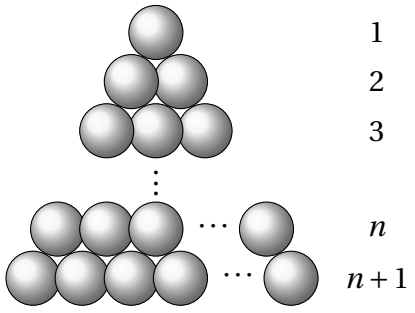
$$k \cdot (k+1) \cdot \ldots \cdot (k+n-1) \cdot (k+n) + (n+1) \cdot (k+1) \cdot (k+2) \cdot \ldots \cdot (k+n).$$

Prvi pribrojnik je prema pretpostavci indukcije (za varijablu k) djeljiv s $(n+1)!$. Drugi pribrojnik je oblika $(n+1) \cdot t$, gdje je t umnožak n uzastopnih brojeva. Po pretpostavci indukcije (za varijablu n), t je djeljiv s $n!$, pa je $(n+1) \cdot t$ djeljiv s $(n+1)!$. Dakle, naš promatrani broj je zbroj dva broja koji su djeljivi s $(n+1)!$, pa je i sam djeljiv s $(n+1)!$, čime je korak indukcije završen.

Rješenje 4.19 Promotrimo piramide za prvih nekoliko prirodnih brojeva n:



Uočimo da se piramida sa $n+1$ kuglica duž bridova sastoji od jednakostraničnog trokuta s $n+1$ kuglica duž stranice na kojeg je dodana piramida s n kuglica duž brida.
Matematičkom indukcijom dokazujemo da formula vrijedi za sve $n \in \mathbb{N}$. Za $n = 1$ formula daje $\frac{1}{6} \cdot 1 \cdot 2 \cdot 3 = 1$, što je točno jer se piramida u tom slučaju sastoji od samo jedne kuglice.
Pretpostavimo da je za piramidu s n kuglica duž brida potrebno $\frac{1}{6}n(n+1)(n+1)$ kuglica.
Za piramidu s $n+1$ kuglica duž brida potrebna je piramida s n kuglica duž brida i trokut s $n+1$ kuglica duž stranice.
Odredimo koliko je kuglica potrebno za trokut. Trokut također možemo promatrati "po slojevima":

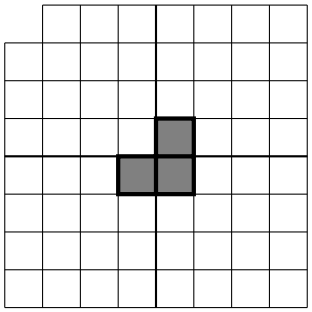


Za trokut je potrebno $1+2+3+\cdots+n+(n+1) = \frac{(n+1)(n+2)}{2}$ kuglica. (Koristili smo formulu iz zadatka 4.1)
Ukupno je za piramidu potrebno

$$\begin{aligned}\frac{(n+1)(n+2)}{2} + \frac{n(n+1)(n+2)}{6} &= \frac{1}{6}\big(3(n+1)(n+2) + n(n+1)(n+2)\big) \\ &= \frac{1}{6}(n+1)(n+2)(n+3)\end{aligned}$$

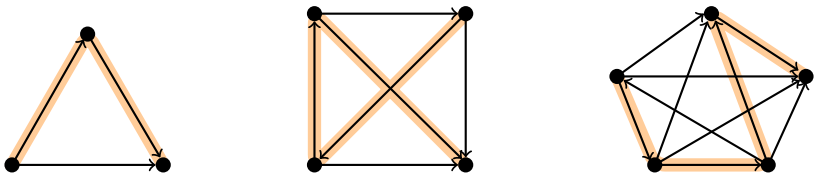
kuglica, kao što je i trebalo dokazati.

Rješenje 4.20 Tvrdnju ćemo dokazati indukcijom po $n \in \mathbb{N}$. Za $n = 1$ tvrdnja je očita: koji god kut bio otkinut, možemo popločati ostatak 2×2 ploče jednom trominom.
Pretpostavimo da za neki prirodan broj n možemo trominama popločati $2^n \times 2^n$ ploču kojoj nedostaje jedan kut.
Promotrimo $2^{n+1} \times 2^{n+1}$ ploču kojoj je otkinut neki kut. Bez smanjenja općenitosti, neka je to gornji lijevi kut.
Podijelimo ploču na četiri $2^n \times 2^n$ ploče. Gornju lijevu ploču od te četiri možemo po pretpostavci indukcije popločati trominama. Sada stavimo jednu trominu u centar ploče tako da pokriva točno po jedno polje od preostale tri manje ploče.



Tada je u svakoj od te tri također otklonjen jedan kut pa ju po pretpostavci također možemo popločati.

Rješenje 4.21 Promotrimo najprije nekoliko primjera:



Slika 4.2: Primjeri gradova i cesta za $n = 3, 4, 5$.

Tvrdnju ćemo dokazati jakom indukcijom po n.
Za $n = 1$ postoji samo jedan grad, pa tvrdnja trivijalno vrijedi.
Pretpostavimo da za svaki skup od k gradova, $k \leq n$ postoji ruta koja obilazi svaki grad točno jednom. Neka je $\{G_1, G_2, \ldots, G_{n+1}\}$ skup od $n+1$ gradova. Promotrimo grad G_{n+1}.
Prema uvjetu zadatka, za svaki od preostalih n gradova G_i postoji ili cesta $G_i \to G_{n+1}$, ili cesta $G_{n+1} \to G_i$. Označimo

$$S_1 = \{G_i \mid \text{ postoji cesta } G_i \to G_{n+1}\} \quad \text{i} \quad S_2 = \{G_i \mid \text{ postoji cesta } G_{n+1} \to G_i\}.$$

Kako su S_1 i S_2 skupovi od najviše n gradova takvi da između svaka dva grada postoji jedna jednosmjerna cesta, po pretpostavci indukcije postoji ruta R_1 koja obilazi sve gradove iz S_1 te ruta R_2 koja obilazi sve gradove iz S_2 točno jednom. Sada je $R_1 \to G_{n+1} \to R_2$ ruta koja obilazi svih $n+1$ gradova, svaki točno jednom. (Ako je $S_1 = \emptyset$ ili $S_2 = \emptyset$, tražena ruta je $G_{n+1} \to R_2$, odnosno $R_1 \to G_{n+1}$.)

Rješenje 4.22 Tvrdnju ćemo dokazati matematičkom indukcijom.
Za $n = 2$ tvrdnja slijedi iz definicije simetrične razlike: $x \in A_1 \triangle A_2$ ako i samo ako je x u točno jednom od A_1, A_2.
Pretpostavimo da tvrdnja zadatka vrijedi za neki prirodan broj $n \geq 2$. Promotrimo $n+1$ skupova $A_1, A_2, \ldots, A_{n+1}$.
Označimo s B_n skup

$$A_1 \triangle A_2 \triangle \ldots \triangle A_n.$$

Tada je

$$A_1 \triangle A_2 \triangle \ldots \triangle A_n \triangle A_{n+1} = B_n \triangle A_{n+1},$$

Pretpostavimo da je $x \in B_n \triangle A_{n+1}$. Tada imamo dva slučaja.

- $x \in B_n$, $x \notin A_{n+1}$. Tada po pretpostavci indukcije ima neparno mnogo indeksa $i \in \{1,2,\ldots,n\}$ za koje je $x \in A_i$. Kako $x \notin A_{n+1}$, slijedi da ima neparno mnogo indeksa $i \in \{1,2,\ldots,n,n+1\}$ za koje je $x \in A_i$.

- $x \notin B_n$, $x \in A_{n+1}$. Tada po pretpostavci indukcije ima parno mnogo indeksa $i \in \{1,2\ldots,n\}$ za koje je $x \in A_i$. Kako je $x \in A_{n+1}$, slijedi da ima neparno mnogo indeksa $i \in \{1,2,\ldots,n,n+1\}$ za koje je $x \in A_i$.

Pretpostavimo sada da $x \notin B_n \triangle A_{n+1}$. Ponovno imamo dva slučaja.

- $x \in B_n$, $x \in A_{n+1}$. Tada po pretpostavci indukcije ima neparno mnogo indeksa $i \in \{1,2,\ldots,n\}$ za koje je $x \in A_i$. Kako je $x \in A_{n+1}$, slijedi da ima parno mnogo indeksa $i \in \{1,2,\ldots,n,n+1\}$ za koje je $x \in A_i$.

- $x \notin B_n$, $x \notin A_{n+1}$. Tada po pretpostavci indukcije ima parno mnogo indeksa $i \in \{1,2\ldots,n\}$ za koje je $x \in A_i$. Kako $x \notin A_{n+1}$, slijedi da ima parno mnogo indeksa $i \in \{1,2,\ldots,n,n+1\}$ za koje je $x \in A_i$.

Dakle, $x \in B_n \triangle A_{n+1}$ ako i samo ako postoji neparno mnogo indeksa $i \in \{1,2,\ldots,n+1\}$ za koje je $x \in A_i$, čime je korak indukcije završen.

Rješenje 4.23 Prisjetimo se da je totalni uređaj onaj u kojem su svaka dva elementa usporediva, odnosno za sve a, b iz S vrijedi $a \leq b$ ili $b \leq a$.
Dokazat ćemo tvrdnju matematičkom indukcijom po broju elemenata skupa S.
Ako je S jednočlan, onda postoji samo jedan parcijalni uređaj na S i on je totalan, pa tvrdnja vrijedi.
Pretpostavimo da se svaki parcijalni uređaj na skupu s n elemenata može proširiti do totalnog uređaja.
Promotrimo skup S koji ima $n+1$ elemenata.
Prvo ćemo dokazati da postoji element $a \in S$ za koji ne postoji $b \in S$ različit od a takav da je $a \leq b$ (drugim riječima, a je maksimalan).
Pretpostavimo da takav element a ne postoji. Tada za svaki $x \in S$ postoji $y \in S$ takav da je $x \neq y$ i $x \leq y$.
Neka je sada x_0 bilo koji element skupa S. Tada možemo konstruirati niz $x_0, x_1, x_2, \ldots$ tako da za svaki $i \geq 0$ vrijedi $x_i \leq x_{i+1}$ i $x_i \neq x_{i+1}$. Tvrdimo da su svi elementi tako konstruiranog niza različiti. Naime, pretpostavimo da je $x_i = x_j$ za neke $i < j$. Tada vrijedi

$$x_i \leq x_{i+1} \leq \ldots \leq x_j = x_i.$$

Iz tranzitivnosti slijedi $x_{i+1} \leq x_i$. Međutim, otprije znamo da je $x_i \leq x_{i+1}$ i $x_i \neq x_{i+1}$, pa dobivamo kontradikciju s antisimetričnošću. Dakle, svi elementi $x_0, x_1, x_2, \ldots$ su međusobno različiti. To je nemoguće jer je S konačan skup. Dakle, naša pretpostavka je bila pogrešna, i postoji element $a \in S$ takav da niti jedan član S različit od a nije veći od a.
Sada promotrimo skup $S' = S \setminus \{a\}$. Restrikcija parcijalnog uređaja $\leq$ je parcijalni uređaj na S', te S' ima n elemenata. Stoga možemo primijeniti pretpostavku indukcije na S' i $\leq$ te možemo $\leq$ proširiti do totalnog uređaja $\preceq$ na S'. Sada $\preceq$ možemo još proširiti na S tako da definiramo $b \preceq a$ za svaki $b \in S$.
Dobivena relacija je totalni uređaj na S, čime je završen korak indukcije.

Rješenje 4.24 Tvrdnju ćemo dokazati pomoću Cauchyjeve indukcije. Za $n = 2^1$ tvrdnja slijedi zbog:

$$\sqrt{x_1 x_2} \leq \frac{x_1 + x_2}{2} \iff (\sqrt{x_1} - \sqrt{x_2})^2 \geq 0.$$

Pretpostavimo da tvrdnja vrijedi za neki $n = 2^k$ i dokažimo da tada vrijedi i za $n = 2^{k+1}$. Primjenom pretpostavke indukcije i AG nejednakosti na 2 člana, vrijedi

$$\begin{aligned}(x_1 \cdots x_n) &= (x_1 \cdots x_{2^k} x_{2^k+1} \cdots x_{2^{k+1}})^{\frac{1}{2^{k+1}}} \\ &\leq \left(\frac{x_1 + \cdots + x_{2^k}}{2^k}\right)^{\frac{1}{2}} \left(\frac{x_{2^k+1} + \cdots + x_{2^{k+1}}}{2^k}\right)^{\frac{1}{2}} \\ &= \frac{x_1 + \cdots + x_n}{n}.\end{aligned}$$

Nadalje, primijetimo da ako tvrdnja vrijedi za neki $n \in \mathbb{N}$, tada vrijedi i za $n-1$. Naime, kako tvrdnja

$$(x_1 \cdots x_n)^{\frac{1}{n}} \leq \frac{x_1 + \cdots + x_n}{n}$$

vrijedi za sve nenegativne realne brojeve, posebno vrijedi i u slučaju kad odaberemo x_n koji ovisi o prvih $n-1$ brojeva na način $x_n := \frac{x_1+\cdots+x_{n-1}}{n-1}$ pa uvrštavanjem dobivamo:

$$\left(x_1 \cdots x_{n-1} \left(\frac{x_1 + \cdots + x_{n-1}}{n-1}\right)\right)^{\frac{1}{n}} \leq \frac{x_1 + \cdots + x_{n-1} + \frac{x_1+\cdots+x_{n-1}}{n-1}}{n} = \frac{x_1 + \cdots + x_{n-1}}{n-1}.$$

Konačno, tvrdnja slijedi dijeljenjem obje strane s $\left(\frac{x_1+\cdots+x_{n-1}}{n-1}\right)^{\frac{1}{n}}$ i sređivanjem izraza.

Poglavlje 5

Elementarna teorija brojeva

5.1 Djeljivost i najveća zajednička mjera

Definicija 5.1. Kažemo da broj $a \in \mathbb{Z} \setminus \{0\}$ **dijeli** broj $b \in \mathbb{Z}$ i pišemo $a \mid b$ ako postoji broj $k \in \mathbb{Z}$ takav da je $b = k \cdot a$. Tada kažemo da je a **djelitelj** od b, a da je b **višekratnik** od a.

Napomena 5.2. Primijetimo da po definiciji slijedi da je 0 djeljiv svakim brojem $a \neq 0$, jer za svaki $a \neq 0$ postoji $k \in \mathbb{Z}$ takav da je $k \cdot a = 0$. Naime, možemo uzeti $k = 0$.

Propozicija 5.3 (Svojstva dijeljenja)**.**

1. $(\forall a \in \mathbb{Z})(a \mid a)$,
2. $(\forall a, b, c \in \mathbb{Z})((a \mid b \wedge b \mid c) \Rightarrow a \mid c)$,
3. $(\forall a, b \in \mathbb{Z})((a \mid b \wedge b \mid a) \Rightarrow (a = b \vee a = -b))$,
4. $(\forall a, b, c \in \mathbb{Z})((a \mid b \wedge a \mid c) \Rightarrow a \mid b + c)$,
5. $(\forall a, a', b, b' \in \mathbb{Z})((a \mid b \wedge a' \mid b') \Rightarrow aa' \mid bb')$,
6. $(\forall a, b \in \mathbb{Z})(a \mid b \Rightarrow (\forall c \in \mathbb{Z})\,(a \mid b \cdot c))$.

Teorem 5.4 (Teorem o dijeljenju s ostatkom)**.** Neka su $a, b \in \mathbb{Z}$ cijeli brojevi takvi da je $b > 0$. Tada postoje jedinstveni brojevi $q, r \in \mathbb{Z}$ takvi da je

$$a = q \cdot b + r, \qquad \text{pri čemu je } 0 \leq r < b.$$

Broj q zovemo **kvocijent**, a broj r **ostatak** pri dijeljenju broja a brojem b.

Definicija 5.5. Neka su $a, b \in \mathbb{N}$. **Najveća zajednička mjera** brojeva a i b je najveći prirodan broj koji dijeli i broj a i broj b. Taj broj označavamo s $M(a,b)$. **Najmanji zajednički višekratnik** brojeva a i b je najmanji prirodan broj koji je djeljiv i brojem a i brojem b. Taj broj označavamo s $V(a,b)$.

Pojam najveće zajedničke mjere možemo definirati i za cijele brojeve: ako su $a, b, \in \mathbb{Z}$, definiramo

$$M(a,b) := \begin{cases} 0, & \text{ako je } a = b = 0; \\ |a|, & \text{ako je } a \neq 0 \text{ i } b = 0; \\ |b|, & \text{ako je } a = 0 \text{ i } b \neq 0; \\ M(|a|,|b|), & \text{ako je } a \neq 0 \text{ i } b \neq 0. \end{cases}$$

Uočimo da je najveća zajednička mjera dvaju brojeva uvijek prirodan broj (ili 0).

Definicija 5.6. Kažemo da su brojevi $a, b \in \mathbb{Z}$ **relativno prosti** ako je $M(a,b) = 1$.

Teorem 5.7. (**Bézoutov identitet**) Neka su $a, b \in \mathbb{Z}$. Tada postoje cijeli brojevi $x, y \in \mathbb{Z}$ takvi da je

$$M(a,b) = x \cdot a + y \cdot b.$$

Dodatno, $M(a,b)$ je najmanji prirodni broj koji se može zapisati u gornjem obliku.

Zadatak 5.1 Neka su $a, b \in \mathbb{Z}$, te neka je $d = M(a,b)$. Pokažite da je tada

$$\{xa + yb \mid x, y \in \mathbb{Z}\} = \{nd \mid n \in \mathbb{Z}\}.$$

Zadatak 5.2 Izračunajte najveću zajedničku mjeru brojeva $2^{2024} - 1$ i $2^{2022} - 1$.

Najveća zajednička mjera se može ekvivalentno definirati na sljedeći način:

Definicija 5.8. Neka su $a, b \in \mathbb{Z}$. Za broj $d \in \mathbb{N}_0$ kažemo da je **najveća zajednička mjera** brojeva a i b, te pišemo $d = M(a,b)$, ako vrijedi:

(i) $d \mid a$ i $d \mid b$,

(ii) ako je $d' \in \mathbb{N}_0$ neki drugi broj takav da vrijedi $d' \mid a$ i $d' \mid b$, onda vrijedi i $d' \mid d$.

Zadatak 5.3 Dokažite da za sve $a, b \in \mathbb{N}$ vrijedi sljedeće:

(a) $M(a,b) = M(-a,b) = M(a,-b) = M(-a,-b)$;

(b) $M(a,b) = M(a,a+b)$;

(c) $(\forall n \in \mathbb{N})(M(na,nb) = nM(a,b))$.

Propozicija 5.9. Neka su $a, b \in \mathbb{N}$ te $q, r \in \mathbb{N}_0$ takvi da je $a = qb + r$. Tada je

$$M(a,b) = M(b,r).$$

Euklidov algoritam

Neka su a i b prirodni brojevi. Sve dok je $b \neq 0$, ponavljamo sljedeće korake:

(1) Koristeći teorem o dijeljenju s ostatkom odredimo q, r takve da je $a = qb + r$ i $0 \leq r < b$.

(2) Zamijenimo a s b i b s r (tj. nastavljamo postupak kao da želimo odrediti $M(b,r)$.

Ako smo u nekom koraku dobili $b = 0$, tada je broj a iz tog koraka tražena najveća zajednička mjera.

Zadatak 5.4 Izračunajte $M(420, 195)$ Euklidovim algoritmom.

Zadatak 5.5 Dokažite da su za svaki prirodni broj n brojevi $28n + 10$ i $8n + 3$ relativno prosti.

Zadatak 5.6 Neka su a i b prirodni brojevi. Dokažite da je $M(5a+3b, 13a+8b) = M(a,b)$.

Zadatak 5.7 Neka su a i b prirodni brojevi takvi da $ab \mid a^2 + b^2$. Dokažite da je $a = b$.

5.2 Kongruencije

Definicija 5.10. Neka su $a, b \in \mathbb{Z}$ te $n \in \mathbb{N}$. Kažemo da je a **kongruentan** b **modulo** n i pišemo $a \equiv b \pmod{n}$ ako vrijedi $n \mid a-b$.

Napomena 5.11. Neka su $a, b \in \mathbb{Z}$ cijeli brojevi i $n \in \mathbb{N}$ prirodan broj takvi da je $0 \leq b < n$. Lako se vidi da je $a \equiv b \pmod{n}$ ako i samo ako je b ostatak pri dijeljenju a sa n. Pokušajte to sami dokazati!

Propozicija 5.12. Relacija "biti kongruentan modulo n" je relacija ekvivalencije na $\mathbb{Z}$, za svaki $n \in \mathbb{N}$.

Dokaz propozicije 5.12. Neka je $n \in \mathbb{N}$ proizvoljan.
Za svaki $a \in \mathbb{Z}$ vrijedi $n \mid 0 = a-a$, pa je $a \equiv a \pmod{n}$. Dakle, relacija "biti kongruentan modulo n" je refleksivna.
Pretpostavimo da za neke $a, b \in \mathbb{Z}$ vrijedi $a \equiv b \pmod{n}$. Tada vrijedi $n \mid a-b$, pa vrijedi i $n \mid -(a-b) = b-a$, tj. $b \equiv a \pmod{n}$. Dakle, relacija je simetrična.
Pretpostavimo da za neke $a, b, c \in \mathbb{Z}$ vrijedi $a \equiv b \pmod{n}$ i $b \equiv c \pmod{n}$. Tada $n \mid a-b$ i $n \mid b-c$, pa $n \mid (a-b)+(b-c) = a-c$, tj. $a \equiv c \pmod{n}$. Dakle, relacija je tranzitivna. □

Napomena 5.13. Neka je $n \in \mathbb{N}$. Odredimo klase ekvivalencije za relaciju "biti kongruentan modulo n". Za neki cijeli broj $a \in \mathbb{Z}$ imamo

$$\begin{aligned} b \in [a] &\iff a \equiv b \pmod{n} \\ &\iff n \mid a-b \\ &\iff (\exists k \in \mathbb{Z})(a-b = kn) \\ &\iff (\exists k \in \mathbb{Z})(b = a+(-k)n) \\ &\iff (\exists k \in \mathbb{Z})(b = a+kn) \end{aligned}$$

Dakle, $[a] = \{b \in \mathbb{Z} \mid (\exists k \in \mathbb{Z})(b = a+kn)\} = \{a+kn \mid k \in \mathbb{Z}\}$. Drugim riječima, $[a]$ je skup svih brojeva koji se od a razlikuju za višekratnik od n, ili ekvivalentno, skup svih brojeva koji pri dijeljenju s n daju isti ostatak kao a.
Može se pokazati (pogledajte propoziciju 5.19. u skripti za predavanja) da je pripadni kvocijentni skup

$$\mathbb{Z}/_{\cong (\mathrm{mod}\ n)} = \{[0], [1], [2], \ldots, [n-1]\}.$$

Zadatak 5.8 Dokažite sljedeća svojstva kongruencije: ako je

$$a_1 \equiv b_1 \pmod{n} \quad \text{i} \quad a_2 \equiv b_2 \pmod{n},$$

tada je i

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{n} \quad \text{te} \quad a_1 a_2 \equiv b_1 b_2 \pmod{n}.$$

Zadatak 5.9 Dokažite da za sve $a, b \in \mathbb{Z}$ i $n, k \in \mathbb{N}$ vrijedi: ako je

$$a \equiv b \pmod{n}$$

tada je i

$$a^k \equiv b^k \pmod{n}.$$

Napomena 5.14. Iz zadataka 5.8 i 5.9 slijedi da kongruencije smijemo međusobno zbrajati, oduzimati i množiti. Posebno, kako je relacija kongruencije refleksivna, smijemo s obje strane kongruencije dodati ili oduzeti neki cijeli broj, te obje strane pomnožiti nekim cijelim brojem. No, kongruencije ne možemo "kratiti", tj. ne možemo obje strane podijeliti nekim brojem. Primjerice, vrijedi $6 \equiv 2 \pmod{4}$, ali ne i $3 \equiv 1 \pmod{4}$.

Zadatak 5.10 Dokažite da je zbroj kubova triju uzastopnih cijelih brojeva uvijek djeljiv s 9.

Zadatak 5.11 Dokažite da niti jedan član niza $a_n = 4^n + \dfrac{5 + (-1)^n}{2}$ nije kvadrat prirodnog broja.

Zadatak 5.12 Nađite sve parove prirodnih brojeva (x, y) takve da su brojevi $4x^2 + 3y^2$ i $3x^2 + 4y^2$ kvadrati prirodnih brojeva.

Zadatak 5.13 Dokažite da je $mn(m^6 - n^6)$ djeljivo s 21 za sve $m, n \in \mathbb{N}$.

5.3 Prosti brojevi

Definicija 5.15. Prirodan broj $p > 1$ koji je djeljiv samo brojem 1 i samim sobom zovemo **prosti** ili **prim** broj. Za ostale brojeve veće od 1 kažemo da su **složeni**. Broj 1 nije ni prost ni složen.

Teorem 5.16. Prostih brojeva ima beskonačno mnogo.

Teorem 5.17 (Osnovni teorem aritmetike)**.** Za prirodan broj $n > 1$ postoje jedinstveni brojevi $k, \alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N}$ te prosti brojevi $p_1 < p_2 < \cdots < p_k$ takvi da je

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Zadatak 5.14 Dokažite: ako je broj n složen, onda postoji njegov djelitelj različit od 1 koji je manji ili jednak $\sqrt{n}$.

Napomena 5.18. Često se koristimo obratom po kontrapoziciji tvrdnje iz zadatka 5.14 za provjeru je li neki broj prost: ako nijedan broj $1 < p \leq \sqrt{n}$ ne dijeli broj n, tada je n prost. Drugim riječima, djelitelje broja n je dovoljno tražiti među prostim brojevima manjim ili jednakim $\sqrt{n}$.

Propozicija 5.19. Neka su $a, b \in \mathbb{Z}$, te $p \in \mathbb{N}$ prost broj. Tada vrijedi:

$$p \mid a \cdot b \implies p \mid a \text{ ili } p \mid b.$$

Zadatak 5.15 Dokažite:

(a) Ako su p i $8p-1$ prosti brojevi, onda je $8p+1$ složen broj.

(b) Ako su p i $8p^2+1$ prosti brojevi, onda je $8p^2-1$ prost broj.

Zadatak 5.16 Odredite sve proste brojeve p, q, r za koje vrijedi jednakost $p^q = r - 1$.

Zadatak 5.17 Dokažite da ostatak pri dijeljenju prostog broja s 30 ne može biti složen broj.

Zadatak 5.18 Dokažite da postoji beskonačno mnogo prostih brojeva oblika $4m+3$, $m \in \mathbb{N}_0$.

5.4 Eulerov teorem i mali Fermatov teorem

Definicija 5.20. Neka je funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ definirana ovako: $\varphi(n)$ je jednak broju elemenata skupa $\{1, 2, \ldots, n\}$ koji su relativno prosti sa n. Funkciju φ zovemo **Eulerova funkcija**.

Propozicija 5.21. Vrijede sljedeća svojstva Eulerove funkcije:

(1) Ako su $a, b > 1$ prirodni brojevi takvi da je $M(a,b) = 1$, onda je $\varphi(ab) = \varphi(a)\varphi(b)$.

(2) Ako je p prost broj i $k \geq 1$, onda je $\varphi(p^k) = p^k - p^{k-1}$.

Teorem 5.22. Neka je $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ rastav broja n na proste faktore. Tada vrijedi

$$\begin{aligned}\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-2})\cdots(p_k^{\alpha_k} - p_k^{\alpha_k-1})\\ &= p_1^{\alpha_1-1} p_2^{\alpha_2-1} \cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).\end{aligned}$$

Zadatak 5.19 Riješite jednadžbu $\varphi(7^x) = 294$.

Zadatak 5.20 Dokažite da jednadžba $\varphi(n) = 14$ nema rješenja.

Zadatak 5.21 Odredite sve prirodne brojeve n takve da $\varphi(n) \mid n^2 + 1$.

Teorem 5.23 (Eulerov teorem)**.** Neka je $n \in \mathbb{N}$, te $a \in \mathbb{Z}$ takav da je $M(a,n) = 1$. Tada vrijedi

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Teorem 5.24 (Mali Fermatov teorem)**.** Neka je $p \in \mathbb{N}$ prost broj, te $a \in \mathbb{Z}$ takav da $p \nmid a$. Tada vrijedi

$$a^{p-1} \equiv 1 \pmod{p}.$$

Zadatak 5.22 Odredite ostatak pri dijeljenju broja $1^{30} + 2^{30} + \cdots + 10^{30}$ brojem 11.

Zadatak 5.23 Dokažite da je za svaki prost broj p i svaki prirodan broj k suma

$$1 + 1^{k(p-1)} + 2^{k(p-1)} + \cdots + p^{k(p-1)}$$

djeljiva s p.

Zadatak 5.24 Dokažite da je za svaki prirodan broj n koji nije djeljiv s 4 zbroj

$$1^n + 2^n + 3^n + 4^n$$

djeljiv s 5.

Zadatak 5.25 Odredite posljednju znamenku broja

$$7^{1998^{1997}} + 3^{1998^{1997}}.$$

Zadatak 5.26 Dokažite da je broj $2222^{5555} + 5555^{2222}$ djeljiv sa 7.

Zadatak 5.27 Odredite ostatak pri dijeljenju broja $140^{67} + 153^{51}$ brojem 17.

Zadatak 5.28 Dokažite da $7 \mid 3^{2n+1} + 2^{2n+2}$ za svaki $n \in \mathbb{N}$.

Zadatak 5.29 Neka su $n \in \mathbb{N}$ i $a \in \mathbb{Z}$ takvi da je $M(a,n) = 1$. Pretpostavimo da je $d \in \mathbb{N}$ najmanji prirodni broj za koji vrijedi

$$a^d \equiv 1 \pmod{n}.$$

Dokažite: ako je $m \in \mathbb{N}$ takav da je $a^m \equiv 1 \pmod{n}$, tada d dijeli m. Posebno, d dijeli $\varphi(n)$.

Napomena 5.25. Potencija dobivena Malim Fermatovim ili Eulerovim teoremom ne mora biti najmanja moguća. Prethodni zadatak nam kaže da se najmanji takav broj nalazi među djeliteljima onih potencija dobivenih tim dvama teoremima. To nam može pomoći da lakše pronađemo potencije koje će davati "male" ostatke; idealno 1 ili -1.

Zadatak 5.30 Odredite ostatak pri dijeljenju broja $3^{105} + 4^{105}$ brojem 13.

Zadatak 5.31 Neka je p prost broj koji daje ostatak 3 pri dijeljenju s 4. Dokažite da ne postoji cijeli broj x takav da $p \mid x^2 + 1$.

Zadatak 5.32 Dokažite da postoji beskonačno mnogo prostih brojeva oblika $4m+1$, $m \in \mathbb{N}$.

Zadatak 5.33 Dokažite da za svaki prost broj p vrijedi

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Zadatak 5.34 Neka je 3^k potencija broja 3 koja ima m znamenaka. Dokažite da postoji veća potencija broja 3 kojoj se zadnjih m znamenaka poklapa sa znamenkama od 3^k.

Zadatak 5.35

a) Odredite sve ostatke koje potencije broja 2 mogu davati pri dijeljenju sa 7.

b) Dokažite da jednadžba $2^n + 1 = 11m^6$ nema prirodnih rješenja.

Zadatak 5.36 Odredite zadnje tri znamenke broja 5^{2024}.

Zadatak 5.37 Odredite sve proste brojeve p takve da $p \mid 29^p + 1$.

Zadatak 5.38 Odredite sve prirodne brojeve n za koje je $7^n - 2^n - 9$ kvadrat prirodnog broja.

Zadatak 5.39 Odredite sve prirodne brojeve n takve da je $\varphi(n) = 56$.

Upute za rješavanje zadataka

Uputa za Z5.5 Odredite najveću zajedničku mjeru Euklidovim algoritmom.

Uputa za Z5.9 Tvrdnju dokažite indukcijom po k.

Uputa za Z5.10 Označite tri uzastopna prirodna broja sa $k-1$, k i $k+1$ te izračunajte zbroj njihovih kubova. Dokažite da je izraz $k(k^2+2)$ uvijek djeljiv s 3.

Uputa za Z5.11 Odredite a_n ovisno o parnosti od n. Uočite koji ostatak a_n daje pri dijeljenju sa 4. Zatim provjerite koje ostatke kvadrat prirodnog broja može dati pri dijeljenju sa 4.

Uputa za Z5.12 Pokušajte dokazati sljedeće: ako je (x, y) rješenje zadatka, onda je i $\left(\frac{x}{2}, \frac{y}{2}\right)$ rješenje zadatka. Možete li pomoću toga dobiti kontradikciju?

Uputa za Z5.13 Promatrajte posebno djeljivost sa 3 i sa 7. Analizirajte ostatke koje šesta potencija prirodnog broja može dati pri dijeljenju sa 3 ili sa 7.

Uputa za Z5.16 Promatrajte parnost.

Rješenja zadataka

Rješenje 5.1 Kako $d \mid a$ i $d \mid b$, to posebno $d \mid xa + yb$ za sve $x, y \in \mathbb{Z}$. Drugim riječima, za sve $x, y \in \mathbb{Z}$ postoji $n \in \mathbb{Z}$ takav da je

$$ax + by = nd.$$

Iz toga zaključujemo da inkluzija $\subseteq$ vrijedi.
S druge strane, iz Bezoutove leme slijedi da postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je

$$d = x_0 a + y_0 b.$$

Tada je za svaki $n \in \mathbb{Z}$

$$nd = n(x_0 a + y_0 b) = (nx_0)a + (ny_0)b \in \{xa + yb \mid x, y \in \mathbb{Z}\}.$$

pa vidimo da vrijedi i obratna inkluzija $\supseteq$, te je jednakost skupova time dokazana.

Rješenje 5.2 Označimo brojeve s

$$a = 2^{2024} - 1, \quad \text{i} \quad b = 2^{2022} - 1.$$

Primijetimo za početak kako je

$$a = 4 \cdot 2^{2022} - 1 = 4 \cdot (2^{2022} - 1) + 4 - 1 = 4b + 3.$$

Zaključujemo kako se broj 3 može prikazati kao linearna kombinacija brojeva a i b na sljedeći način:

$$3 = a - 4b.$$

Kako je $M(a, b)$ prema Bézoutovom identitetu najmanji prirodni broj koji se može prikazati na takav način, slijedi $M(a, b) \leq 3$.
Pokažimo sada da vrijedi $3 \mid a$ i $3 \mid b$. Prvo imamo

$$2^{2022} = (2^2)^{1011} = (3+1)^{1011} = 3^{1011} + 1011 \cdot 3^{1010} + \binom{1011}{2} 3^{1009} + \ldots + 1011 \cdot 3 + 1,$$

pa je

$$b = 2^{2022} - 1 = 3 \cdot \left(3^{1010} + 1011 \cdot 3^{1009} + \cdots + 1011\right)$$

tj. $3 \mid b$. S druge strane, kako je $a = 4b + 3$ i $3 \mid b$, vidimo da $3 \mid a$. S obzirom da je $M(a, b)$ najveći prirodan broj koji dijeli i a i b, zaključujemo da je $3 \leq M(a, b)$, što u kombinaciji s maloprije dokazanim daje $M(a, b) = 3$.

Rješenje 5.3

(a) Pokažimo prvo $M(a,b) = M(-a,b)$. Kako $M(a,b)$ dijeli a, taj broj mora dijeliti i $-a$, a kako on dijeli i b, slijedi $M(a,b) \mid M(-a,b)$. Slično, $M(-a,b)$ dijeli i $-(-a) = a$ i b, pa je $M(-a,b) \mid M(a,b)$. Kako je djeljivost antisimetrična na $\mathbb{N}_0$, slijedi $M(a,b) = M(-a,b)$.

Primjenom upravo dokazanog, te korištenjem činjenice da je poredak za najveću zajedničku mjeru nebitan, dobivamo redom

$$M(a,b) = M(b,a) = M(-b,a) = M(a,-b) = M(-a,-b).$$

(b) Kako $M(a,b)$ dijeli i a i b, on dijeli i $a+b$, slijedi

$$M(a,b) \mid M(a,a+b).$$

Slično, kako $M(a,a+b)$ dijeli i a i $a+b$, on dijeli i $(a+b)-a = b$, pa vrijedi

$$M(a,a+b) \mid M(a,b),$$

odakle kao u prethodnom podzadatku zaključujemo

$$M(a,b) = M(a,a+b).$$

(c) Neka je $n \in \mathbb{N}$. Označimo s $d_1 = M(a,b)$ i $d_2 = M(na,nb)$. Treba dokazati da je $d_2 = nd_1$.

Prema Bézoutovom identitetu, postoje cijeli brojevi x_1, y_1, x_2, y_2 takvi da vrijedi

$$d_1 = x_1 a + y_1 b \quad \text{i} \quad d_2 = x_2(na) + y_2(nb).$$

Imamo

$$d_2 = n(x_2 a + y_2 b).$$

Kako su d_2 i n prirodni brojevi, i $x_2 a + y_2 b$ mora biti prirodan broj. Kako je d_1 najmanji prirodan broj koji se može prikazati kao $xa + yb$, slijedi da je

$$x_2 a + y_2 b \geq d_1,$$

pa imamo

$$d_2 = n(ax_2 + by_2) \geq nd_1.$$

S druge strane, imamo

$$nd_1 = n(x_1 a + y_1 b) = x_1(na) + y_1(nb).$$

Kako je $x_1(na) + y_1(nb)$ prirodan broj, a d_2 je najmanji prirodan broj koji se može zapisati u ovakvom obliku, slijedi

$$nd_1 \geq d_2,$$

što u kombinaciji s prethodno dobivenim daje

$$nd_1 = d_2.$$

Rješenje 5.4 Dijelimo s ostatkom brojeve 420 i 195:

$$420 = 2 \cdot 195 + 30.$$

Sada radimo isto za brojeve 195 i 30:

$$195 = 6 \cdot 30 + 15,$$

te konačno

$$30 = 2 \cdot 15 + 0.$$

Dakle, $M(420, 195) = 15$.

Rješenje 5.5 Imamo

$$28n + 10 = 24n + 9 + 4n + 1 = 2(8n + 3) + (4n + 1),$$

pa iz Propozicije 5.9 slijedi

$$M(28n + 10, 8n + 3) = M(8n + 3, 4n + 1).$$

Sada ponavljamo postupak:

$$8n + 3 = 8n + 2 + 1 = 2(4n + 1) + 1,$$

pa je

$$M(8n + 3, 4n + 1) = M(4n + 1, 1) = 1.$$

Dakle, ovi brojevi su relativno prosti.

Rješenje 5.6 Koristit ćemo više puta svojstvo $M(x,y) = M(x,y-x)$. Imamo

$$\begin{aligned} M(5a+3b,13a+8b) &= M(5a+3b,13a+8b-2(5a+3b)) \\ &= M(5a+3b,3a+2b) \\ &= M(5a+3b-(3a+2b),3a+2b) \\ &= M(2a+b,3a+2b) \\ &= M(2a+b,3a+2b-2(2a+b)) \\ &= M(2a+b,-a) \\ &= M(2a+b,a) \\ &= M(b,a) = M(a,b). \end{aligned}$$

Rješenje 5.7 Neka je $d = M(a,b)$. Tada možemo zapisati $a = da_0$ i $b = db_0$, gdje su a_0 i b_0 relativno prosti prirodni brojevi. S novim oznakama, uvjet djeljivosti postaje

$$d^2 a_0 b_0 \mid d^2(a_0^2 + b_0^2).$$

To je ekvivalentno s $a_0 b_0 \mid a_0^2 + b_0^2$. Iz toga slijedi da $a_0 \mid a_0^2 + b_0^2$, pa $a_0 \mid b_0^2$. Međutim, kako su a_0 i b_0 relativno prosti, isto vrijedi i za a_0 i b_0^2, pa mora biti $a_0 = 1$. Analogno zaključujemo $b_0 = 1$, pa je $a = b = d$.

Rješenje 5.8 Pretpostavimo da vrijedi

$$a_1 \equiv b_1 \pmod{n} \quad \text{i} \quad a_2 \equiv b_2 \pmod{n},$$

odnosno

$$n \mid b_1 - a_1 \quad \text{i} \quad n \mid b_2 - a_2.$$

Tada imamo i

$$n \mid (b_1 - a_1) \pm (b_2 - a_2) = (b_1 \pm b_2) - (a_1 \pm a_2),$$

što daje prvu tvrdnju.
Za dokaz druge tvrdnje primijetimo da je

$$b_1 b_2 - a_1 a_2 = b_1 b_2 - a_1 a_2 + b_1 a_2 - b_1 a_2 = b_1(b_2 - a_2) + a_2(b_1 - a_1),$$

pa kako n dijeli svaki od pribrojnika, zaključujemo da vrijedi

$$n \mid b_1 b_2 - a_1 a_2.$$

Rješenje 5.9 Neka su $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$ takvi da je $a \equiv b \pmod{n}$. Dokazujemo $a^k \equiv b^k \pmod{n}$ indukcijom po k. Za $k = 1$ tvrdnja vrijedi po pretpostavci zadatka.
Pretpostavimo da tvrdnja vrijedi za neki $k \in \mathbb{N}$, tj. da je $a^k \equiv b^k \pmod{n}$. Kako je $a^{k+1} = a \cdot a^k$ i $b^{k+1} = b \cdot b^k$, primjenom zadatka 5.8 na brojeve $a_1 = a$, $a_2 = a^k$, $b_1 = b$ i $b_2 = b^k$ slijedi

$$a^{k+1} \equiv b^{k+1} \pmod{n},$$

čime je dokaz završen.

Rješenje 5.10 Označimo tri uzastopna cijela broja s $k-1, k, k+1$. Računamo zbroj kubova:

$$\begin{aligned}(k-1)^3 + k^3 + (k+1)^3 &= (k^3 - 3k^2 + 3k - 1) + k^3 + (k^3 + 3k^2 + 3k + 1) \\ &= 3k^3 + 6k \\ &= 3k(k^2 + 2).\end{aligned}$$

Kako broj 3 već dijeli ovaj izraz, za djeljivost s 9 nam je dovoljno pokazati da za sve $k \in \mathbb{Z}$ broj 3 dijeli $k(k^2+2)$. Promotrimo stoga ostatke koji ovaj izraz može dati pri dijeljenju s 3, ovisno o tome koji ostatak broj k daje pri dijeljenju s 3. Razlikujemo tri slučaja:

1°) $k \equiv 0 \pmod{3}$. Tada $3 \mid k$, pa posebno i $3 \mid k(k^2+2)$, te u ovom slučaju tvrdnja vrijedi.

2°) $k \equiv 1 \pmod{3}$. Koristeći prethodni zadatak, tada je $k^2 \equiv 1 \pmod{3}$, pa je onda i

$$k^2 + 2 \equiv 1 + 2 \equiv 3 \equiv 0 \pmod{3}.$$

Dakle, u ovom slučaju 3 dijeli k^2+2, pa ponovno zaključujemo da tvrdnja vrijedi.

3°) $k \equiv 2 \pmod{3}$. Slično kao u prethodnom slučaju je tada

$$k^2 + 2 \equiv 2^2 + 2 \equiv 6 \equiv 0 \pmod{3},$$

pa tvrdnja vrijedi i u ovom, posljednjem slučaju.

Rješenje 5.11 Zapišimo opći član niza a_n na sljedeći način:

$$a_n = \begin{cases} 4^n + 3, & n \text{ paran}, \\ 4^n + 2, & n \text{ neparan}. \end{cases}$$

Vidimo da svaki član ovog niza pri dijeljenju s 4 daje ostatak ili 2 ili 3. Provjerimo kakve ostatke mogu davati kvadrati prirodnih brojeva. Neka je $n \in \mathbb{N}$ proizvoljan prirodni broj.

- Ako je $n \equiv 0 \pmod 4$, onda je i $n^2 \equiv 0 \pmod 4$;
- ako je $n \equiv 1 \pmod 4$, onda je i $n^2 \equiv 1 \pmod 4$;
- ako je $n \equiv 2 \pmod 4$, onda je $n^2 \equiv 4 \equiv 0 \pmod 4$;
- ako je $n \equiv 3 \pmod 4$, onda je i $n^2 \equiv 9 \equiv 1 \pmod 4$.

Vidimo da kvadrati prirodnih brojeva pri dijeljenju s 4 mogu davati samo ostatke 0 ili 1, pa zaključujemo da nijedan od članova niza a_n nije kvadrat prirodnog broja.

Rješenje 5.12 Iz prethodnog zadatka znamo da kvadrati daju samo ostatke 1 i 0 pri dijeljenju s 4. Ako je x neparan, onda $x^2 \equiv 1 \pmod 4$, pa je $3x^2 + 4y^2 \equiv 3 \pmod 4$, što je nemoguće jer je to potpun kvadrat. Zaključujemo da x mora biti paran. Analogno zaključujemo da je y nužno paran. Zapišimo $x = 2x_1$, $y = 2y_1$. Tada je

$$3x^2 + 4y^2 = 4(3x_1^2 + 4y_1^2),$$
$$3y^2 + 4x^2 = 4(3y_1^2 + 4x_1^2).$$

Zaključujemo da su i $3x_1^2 + 4y_1^2$ i $3y_1^2 + 4x_1^2$ kvadrati prirodnih brojeva. Drugim riječima, ako je (x, y) rješenje zadatka, tada je $\left(\frac{x}{2}, \frac{y}{2}\right)$ rješenje zadatka. Dakle, počevši od nekog rješenja, dobili smo "manje rješenje". To zvuči nemoguće jer se ne možemo beskonačno spuštati, samo trebamo smisliti kako to precizno argumentirati.
Pretpostavimo da postoji barem jedno rješenje zadatka (x, y).
Neka je (x_0, y_0) rješenje zadatka čija je x-koordinata minimalna (to ima smisla jer je skup $\mathbb{N}$ dobro uređen). Međutim, tada je $\left(\frac{x_0}{2}, \frac{y_0}{2}\right)$ rješenje zadatka čija je x-koordinata strogo manja od najmanje moguće. To je kontradikcija. Zaključujemo da nema ni jednog rješenja.

Napomena 5.26. Metoda iz ovog zadatka zove se *beskonačni spust*: krenuvši od nekog rješenja, konstruiramo novo rješenje koje je na neki način "manje" od početnog. Ponavljanjem tog postupka dolazimo do kontradikcije i zaključujemo da ne postoje rješenja.

Rješenje 5.13 Neka su $m, n \in \mathbb{N}$.
Kako je $21 = 3 \cdot 7$ (a 3 i 7 su relativno prosti), dovoljno je pokazati da je broj $mn(m^6 - n^6)$ djeljiv s 3 i 7.
Pokažimo prvo djeljivost s 3. Ako je jedan od brojeva m, n djeljiv s 3, tada je očito i cijeli izraz djeljiv s 3. Ako niti jedan od brojeva m i n nije djeljiv s 3, tada oni pri dijeljenju s 3 daju ostatak 1 ili 2. Uočimo

$$k \equiv 1 \pmod 3 \implies k^6 \equiv 1 \pmod 3$$

i

$$k \equiv 2 \pmod 3 \implies k^6 \equiv 64 \equiv 1 \pmod 3,$$

odnosno, šesta potencija broja koji nije djeljiv s 3 uvijek daje ostatak 1 pri dijeljenju s 3. Prema tome, ako niti jedan od brojeva m i n nije djeljiv s 3, onda i m^6 i n^6 pri dijeljenju s 3 daju ostatak 1, pa $m^6 - n^6$ daje ostatak 0, tj. djeljiv je s 3.
Na identičan način pristupamo i djeljivosti sa 7. Odredimo prvo sve moguće ostatke pri dijeljenju šestih potencija prirodnih brojeva sa 7.

- $k \equiv 0 \pmod 7 \implies k^6 \equiv 0 \pmod 7$
- $k \equiv 1 \pmod 7 \implies k^6 \equiv 1 \pmod 7$
- $k \equiv 2 \pmod 7 \implies k^6 \equiv 64 \equiv 1 \pmod 7$
- $k \equiv 3 \pmod 7 \implies k^6 \equiv 3^6 = 9^3 \equiv 2^3 = 8 \equiv 1 \pmod 7$

Za analizu preostala tri ostatka iskoristit ćemo sljedeće: ako je $a \equiv b \pmod n$, onda je i $a \equiv b - n \pmod n$. Ovo je vrlo korisno kada je b "blizu" n (tj. ako je bliže n nego nuli), jer je tada $b - n$ negativan broj "male" apsolutne vrijednosti, pa je računanje potencija puno lakše.

- $k \equiv 4 \equiv -3 \pmod 7 \implies k^6 \equiv (-3)^6 = 3^6 \equiv 1 \pmod 7$
- $k \equiv 5 \equiv -2 \pmod 7 \implies k^6 \equiv (-2)^6 = 2^6 \equiv 1 \pmod 7$
- $k \equiv 6 \equiv -1 \pmod 7 \implies k^6 \equiv (-1)^6 = 1 \pmod 7$

Sada su argumenti isti kao u prethodnom dijelu: ukoliko je jedan od brojeva m i n djeljiv sa 7, cijeli izraz je također djeljiv sa 7, a ako nijedan nije djeljiv sa 7, onda njihove šeste potencije obje daju ostatak 1, pa je razlika šestih potencija djeljiva sa 7.

Rješenje 5.14 Pretpostavimo suprotno, tj. je broj n složen te da su svi njegovi djelitelji koji su različiti od 1 ujedno veći od $\sqrt{n}$. Kako je broj n složen, postoje $p, q > 1$ takvi da je $n = p \cdot q$. Prema pretpostavci su oba broja p, q veća od $\sqrt{n}$, pa slijedi

$$n = p \cdot q > \sqrt{n} \cdot \sqrt{n} = n,$$

što je nemoguće.

Rješenje 5.15

(a) Pretpostavimo da su p i $8p-1$ prosti brojevi. Promotrimo tri uzastopna broja $8p - 1, 8p, 8p + 1$. Jedan od njih mora biti djeljiv s 3, pa promotrimo te slučajeve:

1°) $8p-1$ je djeljiv s 3: kako je prema pretpostavci $8p-1$ prost broj, moralo bi biti $8p-1=3$, pa je ovaj slučaj neostvariv.

2°) p je djeljiv s 3, odnosno zbog toga što je p prost, $p=3$. Tada je $8p-1=23$, što je prost broj, a $8p+1=25$ je složen, pa je implikacija valjana u tom slučaju.

3°) $8p+1$ je djeljiv s 3 i očito različit od 3, pa je i složen.

(b) Pretpostavimo da su p i $8p^2+1$ prosti brojevi. Promotrimo ponovno tri uzastopna broja $8p^2-1, 8p^2, 8p^2+1$. S obzirom da je $8p^2+1$ prost i očito veći od 3, imamo dvije mogućnosti: $p=3$ ili $3 \mid 8p^2-1$. Za $p=3$ je $8p^2+1=73$ prost broj, te je $8p^2-1=71$ prost, pa je implikacija valjana u tom slučaju. Pokažimo još da je slučaj $3 \mid 8p^2-1$ nemoguć. Ako je $p \equiv 1 \pmod 3$ imamo

$$8p^2-1 \equiv 7 \equiv 1 \pmod 3,$$

dok je u slučaju $p \equiv 2 \pmod 3$ isto

$$8p^2-1 \equiv 1 \pmod 3,$$

pa zaključujemo da 3 nikad ne dijeli broj oblika $8p^2-1$.

Rješenje 5.16 Ako je $r=2$, tada bi imali $p^q=1$, što je nemoguće za proste brojeve p,q. Stoga mora biti $r>2$, te je broj $r-1$ u tom slučaju uvijek paran. Dakle, da bi jednakost vrijedila, lijeva strana mora biti paran broj, što je moguće jedino u slučaju $p=2$, pa tražimo sve moguće proste brojeve q,r takve da je

$$2^q+1=r.$$

Ako je $q=2$, onda vidimo da jednakost vrijedi za $r=5$, pa je jedno rješenje $(p,q,r)=(2,2,5)$. Ako bi bilo $q>2$, q bi posebno bio neparan broj, pa bi imali

$$2^q+1 \equiv (-1)^q+1 \equiv 0 \pmod 3.$$

Tada bi broj r morao biti djeljiv s 3, a to je moguće jedino ako je $r=3$. Međutim, to se ne može dogoditi jer je $2^q>4$ za sve proste brojeve q. Dakle, jedino rješenje je $(p,q,r)=(2,2,5)$.

Rješenje 5.17 Neka je p proizvoljan prost broj. Primjenom teorema o dijeljenju s ostatkom dobivamo brojeve $q,r \in \mathbb{N}$, $0 \le r < 30$ takve da je

$$p=30 \cdot q+r.$$

Pritom je $M(p,30) = M(30,r)$. Ako je $p < 30$, tada tvrdnja očito vrijedi jer je $p = r$. Ako je $p > 30$, pokažimo da je tada r prost. Kako je u tom slučaju

$$1 = M(30,p) = M(30,r),$$

slijedi da brojevi 2,3 i 5 ne dijele r. Kako je $\sqrt{r} < \sqrt{30} < 6$, prema tvrdnji zadatka 5.14 slijedi tvrdnja.

Rješenje 5.18 Pretpostavimo suprotno, tj. da prostih brojeva oblika $4m+3$, $m \in \mathbb{N}_0$ postoji konačno. Označimo ih s

$$3 = p_1, 7 = p_2, \ldots, p_{k-1}, p_k, \qquad k \in \mathbb{N}.$$

Promotrimo broj

$$n = 4p_2p_3\cdots p_k + 3.$$

Pokažimo da je ovaj broj prost. Očito, n nije paran. Također, $3 \nmid n$ jer bi u suprotnom jedan od brojeva $p_2, p_3, \ldots, p_k$ bio djeljiv s 3, što je nemoguće jer su to po pretpostavci prosti brojevi veći od 3.
Također, nijedan od brojeva $p_2, p_3, \ldots, p_k$ ne dijeli n: u suprotnom bi taj broj morao dijeliti i $n - p_1p_2\cdots p_k = 3$, što je nemoguće. Kako su to po pretpostavci svi prosti brojevi oblika $4m+3$, zaključujemo da n nema prostih faktora tog oblika.
Dakle, prosti faktori od n mogu biti jedino oblika $4m+1$, pa imamo

$$n = q_1q_2\cdots q_t$$

pri čemu su $q_1, q_2, \ldots, q_t$ prosti brojevi kongruentni s 1 modulo 4. Sada imamo

$$n = q_1q_2\cdots q_t \equiv 1\cdot 1\cdot \ldots \cdot 1 = 1 \pmod 4,$$

a s druge strane je

$$n = 4p_2p_3\cdots p_k + 3 \equiv 3 \pmod 4$$

čime smo došli do kontradikcije. Dakle, prostih brojeva oblika $4m+3$ ima beskonačno mnogo.

Rješenje 5.19 Koristimo propoziciju 5.21. Imamo

$$294 = \varphi(7^x) = 7^x - 7^{x-1} = 6\cdot 7^{x-1},$$

odakle slijedi

$$49 = 7^{x-1},$$

pa je jedino rješenje $x = 3$.

Rješenje 5.20 Zapišimo proizvoljan prirodan broj u obliku $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, gdje je $p_1 < p_2 < \cdots < p_k$. Kako je tada

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

da bi n bio rješenje jednadžbe moralo bi biti

$$p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1}(p_1 - 1) \cdots (p_k - 1) = 14.$$

Kako 7 dijeli desnu stranu, mora dijeliti i lijevu stranu. Imamo dva slučaja:

1°) $7 \mid p_i - 1$ za neki $i \in \{1, \ldots, k\}$. Tada je $p_i - 1 = 7$ ili $p_i - 1 = 14$, tj. $p_1 = 8$ ili $p_i = 15$, što je nemoguće jer je p_i prost broj.

2°) $7 \mid p_i^{\alpha_i - 1}$ za neki $i \in \{1, \ldots, k\}$. Tada je $p_i = 7$, pa se s lijeve strane javlja faktor $p_i - 1 = 7 - 1 = 6$, što nije moguće jer $6 \nmid 14$.

Dakle, ne postoji broj n takav da je $\varphi(n) = 14$.

Rješenje 5.21 Za $n = 1$ ili $n = 2$ imamo $\varphi(n) = 1$, pa su $n = 1$ i $n = 2$ rješenja zadatka.
Primijetimo da iz formule za $\varphi(n)$ slijedi da je $\varphi(n)$ paran kad god je $n > 2$. Naime, ako je n djeljiv neparnim prostim brojem p, onda je $\varphi(n)$ djeljiv parnim brojem $p - 1$, pa je $\varphi(n)$ djeljiv i s 2. Ako n nije djeljiv neparnim prostim brojevima, onda je n potencija broja 2, ali $\varphi(2^k) = 2^{k-1}$, što je djeljivo s 2 ako je $k > 1$.
Neka je sada $n > 2$ takav da $\varphi(n) \mid n^2 + 1$. Tada $2 \mid \varphi(n) \mid n^2 + 1$, pa je n nužno neparan.
Pretpostavimo da dva različita neparna prosta broja p i q dijele n. Tada $(p-1)(q-1)$ dijeli $\varphi(n)$, pa i 4 dijeli $\varphi(n)$, pa je $n^2 + 1$ djeljiv s 4. Međutim, otprije znamo da kvadrati daju ostatak 0 ili 1 pri dijeljenju s 4, pa $n^2 + 1$ daje ostatak 1 ili 2 pri dijeljenju s 4 i ne može biti djeljiv s 4. Došli smo do kontradikcije, pa n može biti djeljiv najviše jednim neparnim prostim brojem. Dakle, $n = p^k$ za neki neparan prost broj p i neki prirodan broj k.
Tada djeljivost $\varphi(n) \mid n^2 + 1$ možemo zapisati kao

$$p^k - p^{k-1} \mid p^{2k} + 1.$$

Ako je $k > 1$, onda je lijeva strana djeljivosti djeljiva s p, ali desna nije, što je nemoguće. Dakle, $k = 1$ i

$$p - 1 \mid p^2 + 1.$$

Međutim, imamo $p \equiv 1 \pmod{p-1}$, pa je $p^2 + 1 \equiv 2 \pmod{p-1}$. Dakle, $2 \equiv 0 \pmod{p-1}$ odnosno $p - 1 \mid 2$. To je moguće jedino za $p = 3$.
Zaključujemo da su $1, 2, 3$ jedina rješenja zadatka.

Rješenje 5.22 Su svi brojevi $1,\ldots,10$ relativno prosti s 11, prema Malom Fermatovom teoremu vrijedi

$$1^{10} \equiv 1 \pmod{11}, \quad 1^{10} \equiv 1 \pmod{11}, \quad \ldots \quad 10^{10} \equiv 1 \pmod{11}.$$

Odavde slijedi

$$1^{30} + 2^{30} + \cdots + 10^{30} \equiv 1^3 + 1^3 + \cdots + 1^3 = 10 \pmod{11},$$

tj. traženi ostatak je 10.

Rješenje 5.23 Prema Malom Fermatovom teoremu, za brojeve $a \in \{1,\ldots,p-1\}$ vrijedi

$$a^{k(p-1)} = (a^{p-1})^k \equiv 1^k = 1 \pmod{p},$$

pa je

$$1 + 1^{k(p-1)} + 2^{k(p-1)} + \cdots + (p-1)^{k(p-1)} + p^{k(p-1)} \equiv p + p^{k(p-1)} \equiv 0 \pmod{p}.$$

Rješenje 5.24 Prema Malom Fermatovom teoremu, za svaki prirodan broj $n = 4k + l$ i brojeve $a \in \{1,\ldots,4\}$ vrijedi

$$a^{4k+l} = (a^4)^k \cdot a^l \equiv 1^k \cdot a^l = a^l \pmod{5},$$

pa je

$$1^{4k+l} + 2^{4k+l} + 3^{4k+l} + 4^{4k+l} \equiv 1^l + 2^l + (-2)^l + (-1)^l \pmod{5}.$$

Za $l = 1$ i $l = 3$ je dobiveni izraz jednak 0, a za $l = 2$ je jednak 10. U svakom slučaju, dobiveni izraz je kongruentan nuli modulo 5.

Rješenje 5.25 Kako je $M(7,10) = M(3,10) = 1$ i $\varphi(10) = 4$, prema Eulerovom teoremu vrijedi

$$7^4 \equiv 1 \pmod{10}, \quad \text{i} \quad 3^4 \equiv 1 \pmod{10}.$$

Kako je $1998 \equiv 2 \pmod{4}$, to je

$$1998^{1997} \equiv 2^{1997} \equiv 0 \pmod{4}.$$

Konačno, imamo

$$7^{1998^{1997}} + 3^{1998^{1997}} \equiv 7^0 + 3^0 \equiv 2 \pmod{10}.$$

Rješenje 5.26 Napravit ćemo nekoliko pomoćnih računa. Prvo, običnim dijeljenjem vidimo da vrijedi

$$1111 \equiv 5 \pmod 7.$$

Stoga je

$$2222 \equiv 10 \equiv 3 \pmod 7 \quad \text{i} \quad 5555 \equiv 25 \equiv 4 \pmod 7,$$

pa nam je dovoljno provjeriti da je broj

$$3^{5555} + 4^{2222}$$

djeljiv sa 7. Također, primjenom Malog Fermatovog teorema, dobivamo

$$3^6 \equiv 1 \pmod 7 \quad \text{i} \quad 4^6 \equiv 1 \pmod 7.$$

Kako je $1111 \equiv 1 \pmod 6$, tada je

$$3^{5555} + 4^{2222} \equiv 3^5 + 4^2 \equiv 5 + 2 \equiv 0 \pmod 7.$$

Rješenje 5.27 Prvo vidimo kako je

$$140 \equiv 4 \pmod{17} \quad \text{i} \quad 153 \equiv 0 \pmod{17}.$$

Također, prema Malom Fermatovom teoremu je

$$4^{16} \equiv 1 \pmod{17},$$

pa jer je $67 \equiv 3 \pmod{16}$ imamo

$$140^{67} + 153^{51} \equiv 4^3 + 0 \equiv 4 \cdot 16 \equiv -4 \equiv 13 \pmod{17}.$$

Rješenje 5.28 Za svaki $n \in \mathbb{N}$ imamo

$$3^{2n+1} + 2^{n+2} \equiv 3 \cdot 9^n + 2^{n+2} \equiv 3 \cdot 2^n + 4 \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \pmod 7.$$

Rješenje 5.29 Neka je $0 \leq r < d$ takav da je $m \equiv r \pmod d$. Tada je

$$a^r \equiv a^m \equiv 1 \pmod n,$$

pa kako je po pretpostavci d bio najmanji prirodni broj za koji to vrijedi, mora biti $r = 0$, što znači upravo da d dijeli m.

Rješenje 5.30 Mali Fermatov teorem nam daje

$$3^{12} \equiv 4^{12} \equiv 1 \pmod{13}.$$

Ako promotrimo neke od djelitelja broja 12, možemo vidjeti da vrijedi

$$3^3 \equiv 1 \pmod{13}, \qquad 4^3 \equiv -1 \pmod{13}$$

pa je

$$3^{105} + 4^{105} \equiv (3^3)^{35} + (4^3)^{35} \equiv 1^{35} + (-1)^{35} \equiv 0 \pmod{13}.$$

Rješenje 5.31 Ovaj zadatak možemo svesti na zadatak 5.29. Pretpostavimo da postoji takav x. Tada $x^2 \equiv -1 \pmod{p}$ implicira da je $x^4 \equiv 1 \pmod{p}$. Nadalje, tvrdimo da je x^4 je najmanja potencija od x kongruentna s 1 modulo p. Naime, ako je $x \equiv 1 \pmod{p}$, onda je $x^2 \equiv 1 \pmod{p}$, kontradikcija. Iz pretpostavke slijedi $x^2 \not\equiv 1 \pmod{p}$. Ako bi bilo $x^3 \equiv 1 \pmod{p}$, onda bi zadatak 5.29 implicirao da $3 \mid 4$, kontradikcija. Dakle, x^4 je stvarno najmanja takva potencija.
Prema spomenutom zadatku, slijedi da $4 \mid \varphi(p)$ odnosno $4 \mid p-1$, kontradikcija s pretpostavkom zadatka.

Rješenje 5.32 Pretpostavimo suprotno, tj. da prostih brojeva oblika $4m+1$ postoji konačno. Označimo ih s $p_1, p_2, \ldots, p_k$. Promotrimo broj

$$(2p_1p_2\cdots p_k)^2 + 1.$$

Taj broj je veći od 1, pa je djeljiv nekim prostim brojem. Očito nije djeljiv s 2 niti s $p_1, \ldots, p_k$ jer daje ostatak 1 s njima. Prema prethodnom zadatku, nije djeljiv prostim brojevima oblika $4m+3$. Međutim, onda nije djeljiv ni jednim prostim brojem, čime smo došli do kontradikcije.

Rješenje 5.33 Dat ćemo dva rješenja:

(I) Za proizvoljni prirodni broj $n \in \mathbb{N}$ uvijek vrijedi $n^p \equiv n \pmod{p}$. Zaista, imamo dva slučaja:

(a) $\boxed{p \nmid n}$ Tada je prema malom Fermatovom teoremu

$$n^p \equiv n \pmod{p}.$$

(b) $\boxed{p \mid n}$ Tada je

$$n^p \equiv n \equiv 0 \pmod{p}.$$

Primjenom upravo dokazanog dobivamo

$$(a+b)^p \equiv a+b \equiv a^p + b^p \pmod{p}.$$

(II) Raspišimo izraz

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}.$$

Promotrimo koeficijente $\binom{p}{k}$ za $1 \leq k \leq p-1$. S obzirom da je

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdots k}$$

cijeli broj (razmislite zašto) i uz činjenicu da su svi $1, 2, \ldots k$ strogo manji od p te ga samim time ne dijele, zaključujemo da vrijedi

$$p \mid \binom{p}{k}, \qquad k = 1, 2 \ldots, p-1.$$

Tada je

$$(a+b)^p \equiv a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} \equiv a^p + b^p \pmod{p}.$$

Rješenje 5.34 Označimo s 3^t tu veću potenciju broja 3 koju tražimo (cilj je konstruirati prikladni t).
Zapišimo preko kongruencija što to znači da se zadnjih m znamenaka poklapa sa zadnjih m znamenaka od 3^k.
To možemo zapisati kao

$$3^t \equiv 3^k \pmod{10^m}.$$

Sada treba pronaći prikladni t. To možemo pomoću Eulerovog teorema. Naime, 3 i 10^m su relativno prosti, pa je $3^{\varphi(10^m)} \equiv 1 \pmod{10^m}$. Ako pomnožimo obje strane kongruencije s 3^k, dobivamo

$$3^{k+\varphi(10^m)} \equiv 3^k \pmod{10^m},$$

pa možemo uzeti $t = k + \varphi(10^m)$.

Rješenje 5.35

a) Imamo $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$ i nakon toga se ostaci ponavljaju. Dakle, mogući ostaci su $1, 2, 4$.

b) Prema a) dijelu zadatka, lijeva strana jednadžbe daje ostatke $2, 3, 5$ pri dijeljenju sa 7. Prema malom Fermatovom teoremu, m^6 daje ostatak 0 ili 1 pri dijeljenju sa 7. Onda $11m^6$ daje ostatak 0 ili 4 pri dijeljenju sa 7. Kako su $\{2, 3, 5\}$ i $\{0, 4\}$ disjunktni skupovi ostataka pri dijeljenju sa 7, zaključujemo da jednadžba nema rješenja (štoviše, čak ni kongruencija $2^n + 1 \equiv 11m^6 \pmod 7$ nema rješenja).

Rješenje 5.36 Važno je napomenuti da ovdje ne možemo iskoristiti Eulerov teorem jer 5 i 1000 nisu relativno prosti.
Svejedno, možemo isprobati koje ostatke daje prvih nekoliko potencija broja 5, pa možda primijetimo neki uzorak.
Vrijedi $5^1 \equiv 5 \pmod{1000}$, $5^2 \equiv 25 \pmod{1000}$, $5^3 \equiv 125 \pmod{1000}$, $5^4 \equiv 625 \pmod{1000}$, $5^5 \equiv 125 \pmod{1000}$, $5^6 \equiv 625 \pmod{1000}$. Vidimo da se ostatci 125 i 625 izmjenjuju nakon 5^3. Onda je

$$5^{2024} \equiv 5^{2022} \equiv \ldots \equiv 5^6 \equiv 5^4 \equiv 625 \pmod{1000},$$

pa su zadnje tri znamenke 625.

Rješenje 5.37 Očito $p = 29$ nije rješenje zadatka. Zato su p i 29 relativno prosti pa po malom Fermatovom teoremu slijedi da je $29^{p-1} \equiv 1 \pmod p$, odnosno $29^p \equiv 29 \pmod p$. Po uvjetu zadatka imamo da je $29^p \equiv -1 \pmod p$ pa je $29 \equiv -1 \pmod p$, odnosno $p \mid 30$. Iz ovoga slijedi da su jedina moguća rješenja $p = 2, 3, 5$. To i jesu rješenja jer imamo $29^p + 1 \equiv 29 + 1 \equiv 0 \pmod p$ za svaki od tih slučajeva.

Rješenje 5.38 Neka je $k \in \mathbb{N}$ takav da je $7^n - 2^n - 9 = k^2$. Lijeva strana je paran broj pa k mora biti paran. Slučaj $n = 1$ očito nije rješenje pa pretpostavimo da je $n \geq 2$. Tada imamo $7^n \equiv k^2 + 2^n + 9 \equiv 1 \pmod 4$. Po Eulerovom teoremu imamo da je $7^2 \equiv 1 \pmod 4$ te je stoga $7^{2l} \equiv 1 \pmod 4$ i $7^{2l+1} \equiv 3 \pmod 4$. Dakle, n mora biti paran, označimo $n = 2m$.
Primijetimo da je $k^2 = 7^{2m} - 2^{2m} - 9 < 7^{2m}$ pa je $k < 7^m$, odnosno $k \leq 7^m - 1$. Dakle, $7^{2m} - 2^{2m} - 9 = k^2 \leq (7^m - 1)^2$ iz čega dobivamo $2 \cdot 7^m \leq 4^m + 10$. Uočimo da $m = 1$ zadovoljava nejednadžbu te je $n = 2$ rješenje jer je $7^2 - 2^2 - 9 = 36 = 6^2$. Pokažimo da za $m > 1$ vrijedi $2 \cdot 7^m > 4^m + 10$ matematičkom indukcijom. Za $m = 2$ očito vrijedi $2 \cdot 49 > 16 + 10$. Pretpostavimo da tvrdnja vrijedi za m. Tada:

$$2 \cdot 7^{m+1} > 7(4^m + 10) = 7 \cdot 4^m + 70 > 4 \cdot 4^m + 10 = 4^{m+1} + 10.$$

Rješenje 5.39 Pretpostavimo da je $n \in \mathbb{N}$ takav da je $\varphi(n) = 56$. Označimo sa p najveći prosti faktor od n. Tada je

$$n = p^{\alpha} \cdot n'$$

za neki $n' \in \mathbb{N}$, pri čemu je $M(p, n') = 1$. Vrijedi

$$56 = \varphi(n) = \varphi(p^{\alpha})\varphi(n') = p^{\alpha-1}(p-1)\varphi(n').$$

Vidimo da broj $p-1$ mora dijeliti 56, pa je

$$p - 1 \in \{1, 2, 4, 7, 8, 14, 28, 56\},$$

odnosno

$$p \in \{2, 3, 5, \not{8}, \not{9}, \not{15}, 29, \not{57}\}$$

(eliminiramo brojeve koji nisu prosti).
Promotrimo redom slučajeve:

1°) $\boxed{p = 29}$ Imamo

$$56 = 29^{\alpha-1} \cdot 28 \cdot \varphi(n') \quad \Longrightarrow \quad 2 = 29^{\alpha-1} \cdot \varphi(n').$$

Kako $29 \not| 2$, jedina mogućnost je $\alpha = 1$. Dakle, preostaje naći sve $n' \in \mathbb{N}$ takve da je $\varphi(n') = 2$.

Označimo sa p' najveći prosti faktor od n', tj. $n' = p'^{\beta} \cdot n''$, pri čemu je $M(p', n'') = 1$. Na isti način kao gore zaključujemo da $p' - 1$ dijeli 2, odakle slijedi $p' \in \{2, 3\}$.

Ako je $p' = 3$, imamo $2 = 3^{\beta-1} \cdot 2 \cdot \varphi(n'')$, odakle slijedi $3^{\beta-1}\varphi(n'') = 1$. Jedina mogućnost je $\beta = 1$, što nas vodi na jednadžbu $\varphi(n'') = 1$ čija rješenja su $n'' = 1$ i $n'' = 2$.

Ako je $p' = 2$, mora biti $n' = 2^{\beta}$ (jer je p' *najveći* prosti faktor od n'), pa imamo

$$2 = \varphi(2^{\beta}) = 2^{\beta-1}$$

odakle slijedi $\beta = 2$, tj. $n' = 4$.

Dakle, našli smo tri rješenja polazne jednadžbe: $n = 29 \cdot 3 \cdot 1 = 87$, $n = 29 \cdot 3 \cdot 2 = 174$ i $n = 29 \cdot 2^2 = 116$.

2°) $\boxed{p = 5}$ Imamo

$$56 = 5^{\alpha-1} \cdot 4 \cdot \varphi(n') \quad \Longrightarrow \quad 14 = 5^{\alpha-1} \cdot \varphi(n').$$

Kako $5 \not| 14$, ponovno je jedina mogućnost $\alpha = 1$, pa preostaje naći sve $n' \in \mathbb{N}$ takve da je $\varphi(n') = 14$.

Budući da je $p = 5$ po pretpostavci najveći prosti faktor od n, prosti faktori od n' mogu biti samo 2 i 3. Dakle, imamo tri mogućnosti: $n' = 3^\beta 2^\gamma$, $n' = 3^\beta$ i $n' = 2^\beta$. Ta tri slučaja vode do jednadžbi

$$14 = 3^{\beta-1} \cdot 2 \cdot 2^{\gamma-1} \cdot 1, \qquad 14 = 3^{\beta-1} \cdot 2 \quad \text{i} \quad 14 = 2^{\beta-1} \cdot 1$$

od kojih nijedna nema rješenje.

3°) $\boxed{p = 3}$ Ako je $p = 3$ najveći prosti faktor od n, jedine mogućnosti su $n = 3^\alpha 2^\beta$ ili $n = 3^\alpha$. Slijedi

$$56 = 3^{\alpha-1} \cdot 2 \cdot 2^{\beta-1} \cdot 1 \quad \text{ili} \quad 56 = 3^{\alpha-1} \cdot 2,$$

pa ni u ovom slučaju nema rješenja.

4°) $\boxed{p = 2}$ Jedina mogućnost je $n = 2^\alpha$, odnosno

$$56 = 2^{\alpha-1}$$

pa ponovno nema rješenja.

Dakle, rješenja jednadžbe $\varphi(n) = 56$ su $n \in \{87, 116, 174\}$.

Poglavlje 6

Polinomi

6.1 Osnovni pojmovi

Definicija 6.1. Polinom n-tog stupnja (nad $\mathbb{R}$) je funkcija $f : \mathbb{R} \to \mathbb{R}$ dana sa

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i,$$

gdje su $n \in \mathbb{N}_0$, $a_0, a_1, \ldots, a_n \in \mathbb{R}$. Brojeve $a_0, \ldots, a_n$ zovemo **koeficijenti polinoma**.
Ako je $f(x) = 0$ za sve $x \in \mathbb{R}$, onda polinom f zovemo **nulpolinom** i pišemo $f = 0$.
Ako je $a_n \neq 0$, broj n zovemo **stupanj polinoma** te pišemo $\deg f = n$, a broj a_n zovemo **vodeći koeficijent**. Broj a_0 zovemo **slobodni koeficijent**.
Skup svih polinoma $f : \mathbb{R} \to \mathbb{R}$ označavamo sa $\mathbb{R}[x]$.

Napomena 6.2. Stupanj nulpolinoma se uglavnom ne definira. No, nekad je iz formalnih razloga pogodno staviti $\deg 0 = -1$ ili $\deg 0 = -\infty$.

Teorem 6.3 (O nulpolinomu)**.** Polinom $p(x) = \sum_{i=0}^{n} a_i x^i$ jednak je nulpolinomu ako i samo ako je $a_i = 0$ za sve $i = 0, 1, \ldots, n$.

Teorem 6.4 (O jednakosti polinoma)**.** Polinomi $p(x) = \sum_{i=0}^{n} a_i x^i$ i $q(x) = \sum_{i=0}^{m} b_i x^i$ su jednaki ako i samo ako je $m = n$ i $a_i = b_i$ za sve $i = 0, 1, \ldots, n$.

Zadatak 6.1 Odredite polinom $f \in \mathbb{R}[x]$ koji zadovoljava sljedeće uvjete

- $\deg f = 3$,
- $f(0) = 0$,
- $f(x) - f(x-1) = x^2, \quad \forall x \in \mathbb{R}$.

Operacije na polinomima

Neka su $f, g \in \mathbb{R}[x]$,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{6.1}$$

i

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0. \tag{6.2}$$

Operacije zbrajanja i množenja polinoma definiramo kao i pripadne operacije na funkcijama, tj. po točkama: za $x \in \mathbb{R}$ definiramo vrijednost funkcija $f+g$ i fg u točki x ovako:

$$\begin{aligned}(f+g)(x) &:= f(x) + g(x),\\ (fg)(x) &:= f(x)g(x).\end{aligned}$$

Pokažimo da su funkcije $f+g$ i fg su ponovno polinomi. Imamo

$$\begin{aligned}(f+g)(x) &= a_n x^n + \cdots + a_1 x + a_0 + b_m x^m + \cdots + b_1 x + b_0 \\ &= \begin{cases} a_n x^n + \cdots + (a_m + b_m) x^m + \cdots + (a_1 + b_1)x + (a_0 + b_0), & n > m \\ (a_n + b_n) x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0), & n = m \\ b_m x^m + \cdots + (a_n + b_n) x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0), & m > n \end{cases}\end{aligned} \tag{6.3}$$

te

$$\begin{aligned}(fg)(x) &= (a_n x^n + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0) \\ &= a_n b_m x^{n+m} + (a_{n-1} b_m + a_n b_{m-1}) x^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1)x + a_0 b_0,\end{aligned} \tag{6.4}$$

odakle vidimo da se $f+g$ i fg mogu zapisati u obliku iz definicije 6.1.
Kompozicija polinoma definira se također kao kompozicija funkcija: za $x \in \mathbb{R}$ je

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

Kompozicija polinoma je ponovno polinom:

$$\begin{aligned}(f \circ g)(x) &= a_n (b_m x^m + \cdots + b_1 x + b_0)^n + a_{n-1}(b_m x^m + \cdots + b_1 x + b_0)^{n-1} + \ldots \\ &\qquad + a_1 (b_m x^m + \cdots + b_1 x + b_0) + a_0 \\ &= a_n b_m^n x^{mn} + (\text{niže potencije})\end{aligned} \tag{6.5}$$

Ovdje bi bilo kompliciranо zapisati točan raspis po potencijama od x, ali možemo iskoristiti poznate činjenice: svaki izraz oblika $a_i(b_m x^m + \cdots + b_1 x + b_0)^i$ je polinom kao produkt polinoma, pa je i $f \circ g$ polinom kao zbroj takvih izraza.
Dijeljenje polinoma nije standardna operacija jer rezultat ne mora ponovno biti polinom. Općenito, funkciju dobivenu dijeljenjem polinoma zovemo **racionalna funkcija**. Za polinome $f, g \in \mathbb{R}[x]$ je

$$\left(\frac{f}{g}\right)(x) := \frac{f(x)}{g(x)},$$

s domenom $\{x \in \mathbb{R} : g(x) \neq 0\}$.

Iz formula (6.3), (6.4) i (6.5) lako se vidi da za stupanj ne-nul polinoma f i g vrijedi

- $\deg(f+g) \leq \max\{\deg f, \deg g\}$,
- $\deg(f \cdot g) = \deg f + \deg g$,
- $\deg(f \circ g) = \deg f \cdot \deg g$.

Napomena 6.5. Osim realnih polinoma, možemo na identičan način promatrati i polinome nad proizvoljnim prstenom $\mathbb{K}$. Polinom nad $\mathbb{K}$ je funkcija $f : \mathbb{K} \to \mathbb{K}$ oblika

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i,$$

gdje su sada $a_0, \ldots, a_n \in \mathbb{K}$. Skup svih polinoma nad $\mathbb{K}$ označavamo sa $\mathbb{K}[x]$.
Na EM1 će najčešće biti $\mathbb{K} = \mathbb{Z}, \mathbb{R}$ ili $\mathbb{C}$.

6.2 Nultočke i dijeljenje polinoma

Definicija 6.6. Nultočka polinoma $f \in \mathbb{C}[x]$ je (kompleksni) broj α takav da je $f(\alpha) = 0$.

Definicija 6.7. Polinom $f \in \mathbb{R}[x]$ je **djeljiv** polinomom $g \in \mathbb{R}[x] \setminus \{0\}$ ako postoji polinom $h \in \mathbb{R}[x]$ takav da $f = gh$. Pišemo $g \mid f$.

Uočimo: ako je $f = gh$ i $f \neq 0$, onda je $\deg f = \deg g + \deg h$ (pa je posebno $\deg f \geq \deg g$).

Teorem 6.8 (O dijeljenju s ostatkom)**.** Neka su $f, g \in \mathbb{R}[x]$, $g \neq 0$. Tada postoje jedinstveni polinomi $q, r \in \mathbb{R}[x]$ takvi da je $f = qg + r$, pri čemu je $r = 0$ ili $0 \leq \deg r < \deg g$.
Ista tvrdnja vrijedi i za polinome iz $\mathbb{Q}[x]$ i $\mathbb{C}[x]$.

Primjer 6.9. Odredimo ostatak pri dijeljenju polinoma $f(x) = x^3 - 2x^2 + x + 3$ polinomom $g(x) = x^2 + 2x - 1$.

$$\begin{array}{l} (\ x^3 - 2x^2 + \ x\ + 3) : (x^2 + 2x - 1) = x - 4 \\ \underline{-x^3 - 2x^2 + \ x} \\ \quad -4x^2 + 2x\ + 3 \\ \quad \underline{+4x^2 + 8x\ - 4} \\ \qquad\qquad 10x - 1 \end{array}$$

Kako je $\deg(10x - 1) = 1 < \deg g$, traženi ostatak je $10x - 1$.

Definicija 6.10. Za polinom $f \in \mathbb{R}[x]$ kažemo da je **normiran** ako mu je vodeći koeficijent jednak 1.

Definicija 6.11. Neka su $f, g \in \mathbb{R}[x] \setminus \{0\}$. **Najveća zajednička mjera** polinoma f i g je normirani polinom $h \in \mathbb{R}[x]$ najvećeg stupnja takav da su i f i g djeljivi s h. Pišemo $h = M(f, g)$.

Primjer 6.12. Odredimo najveću zajedničku mjeru polinoma

$$f(x) = x^4 + x^3 + 2x^2 + x + 1,$$
$$g(x) = x^3 - 2x^2 + x - 2.$$

To možemo napraviti na dva načina:

(I) Primijetimo da je

$$f(x) = (x^2 + 1)(x^2 + x + 1) \quad \text{i} \quad g(x) = (x^2 + 1)(x - 2).$$

Kako polinom $x^2 + 1$ dijeli i f i g, znamo da $M(f, g)$ mora biti normirani polinom stupnja ≥ 2. Očito, $\deg M(f, g) \leq \deg g = 3$. Kada bi postojao normirani polinom $p(x) = x^3 + ax^2 + bx + c$ koji dijeli i f i g, imali bismo

$$g(x) = h(x)(x^3 + ax^2 + bx + c)$$

što je moguće samo ako je $h(x) = 1$, tj. $p = g$. No g očito ne dijeli f, pa je x^2+1 normiran polinom najvećeg mogućeg stupnja koji dijeli i f i g, dakle $M(f,g) = x^2+1$.

(II) Najveću zajedničku mjeru polinoma također možemo računati Euklidovim algoritmom, analogno kao za cijele brojeve. Redom dijelimo:

$$\begin{array}{l} (\ x^4 + x^3 + 2x^2 + x + 1) : (x^3 - 2x^2 + x - 2) = x + 3 \\ \underline{-x^4 + 2x^3 - x^2 + 2x} \\ \quad 3x^3 + x^2 + 3x + 1 \\ \quad \underline{-3x^3 + 6x^2 - 3x + 6} \\ \quad\quad 7x^2 + 7 \end{array}$$

$$\begin{array}{l} (\ x^3 - 2x^2 + x - 2) : (7x^2 + 7) = \frac{1}{7}x - \frac{2}{7} \\ \underline{-x^3 - x} \\ \quad -2x^2 - 2 \\ \quad \underline{+2x^2 + 2} \\ \quad\quad 0 \end{array}$$

Zadnji ne-nul ostatak je $7x^2+7$. Da bismo dobili najveću zajedničku mjeru, trebamo normirati taj polinom, tj. podijeliti ga s vodećim koeficijentom. Dakle, $M(f,g) = \frac{1}{7}(7x^2+7) = x^2+1$.

Zadatak 6.2 Dokažite da je ostatak pri dijeljenju polinoma f polinomom $x-\alpha$ jednak $f(\alpha)$.

Teorem 6.13 (Bezout)**.** Broj $\alpha \in \mathbb{C}$ je nultočka polinoma $f \in \mathbb{C}[x]$ ako i samo ako je f djeljiv polinomom $x-\alpha$.

Dokaz teorema 6.13. Prema zadatku 6.2 vrijedi

$$f(x) = q(x)(x-\alpha) + f(\alpha), \qquad \forall x \in \mathbb{C}.$$

Ako je $f(\alpha) = 0$, onda prema gornjem izrazu polinom $x-\alpha$ dijeli polinom f. Obratno, ako $x-\alpha$ dijeli f, onda je $f(\alpha) = 0$, tj. α je nultočka od f. □

Zadatak 6.3 Neka je $f(x) = 3x^5 + x^4 + x^3 + x^2 - x + 1$ i $g(x) = x^3 - ax^2 - ax - 1$. Dokažite da $M(f,g)$ nije djeljiva polinomom $x+1$ ni za koji $a \in \mathbb{R}$.

Zadatak 6.4 Dokažite da je polinom $f(x) = (x^2+x-1)^{2n} + (x^2-x-1)^{2n} - 2$ djeljiv polinomom $g(x) = x^2 - x$ za sve $n \in \mathbb{N}$.

Hornerov algoritam

Hornerov algoritam je efikasan algoritam za računanje vrijednosti polinoma f u zadanoj točki α (ili dijeljenje polinoma f polinomom $x-\alpha$). Štoviše, može se pokazati da je to optimalan algoritam za izvrednjavanje polinoma.
Neka je

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

gdje je $\alpha \in \mathbb{R}$. Prema teoremu o dijeljenju s ostatkom i Bezoutovom teoremu postoji polinom

$$q(x) = b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$$

takav da je

$$f(x) = q(x)(x-\alpha) + f(\alpha), \qquad \forall x \in \mathbb{R}.$$

Uvrštavanjem formula za $f(x)$ i $q(x)$ dobivamo

$$\begin{aligned} a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 &= (b_{n-1}x^{n-1} + \cdots + b_1 x + b_0)(x-\alpha) + f(\alpha) \\ &= b_{n-1}x^n + (b_{n-2} - \alpha b_{n-1})x^{n-1} + \cdots + (b_0 - \alpha b_1)x + (f(\alpha) - \alpha b_0). \end{aligned}$$

Prema teoremu o jednakosti polinoma, slijedi

$$\begin{aligned} a_n &= b_{n-1} & \Rightarrow \quad & b_{n-1} = a_n \\ a_{n-1} &= b_{n-2} - \alpha b_{n-1} & \Rightarrow \quad & b_{n-2} = a_{n-1} + \alpha b_{n-1} \\ &\vdots & \Rightarrow \quad & \vdots \\ a_k &= b_{k-1} - \alpha b_k & \Rightarrow \quad & b_{k-1} = a_k + \alpha b_k \\ &\vdots & \Rightarrow \quad & \vdots \\ a_1 &= b_0 - \alpha b_1 & \Rightarrow \quad & b_0 = a_1 + \alpha b_1 \\ a_0 &= f(\alpha) - \alpha b_0 & \Rightarrow \quad & f(\alpha) = a_0 + \alpha b_0 \end{aligned}$$

Dakle, vrijednost $f(\alpha)$ i koeficijente b_i možemo izračunati iz α i koeficijenata a_i jednostavnim množenjem i zbrajanjem. Ovo se može kompaktno zapisati tablično:

	a_n	a_{n-1}	$\ldots$	a_k	$\ldots$	a_1	a_0
α	b_{n-1}	b_{n-2}	$\ldots$	b_{k-1}	$\ldots$	b_0	$f(\alpha)$

Primjer 6.14. Izračunajmo $f(3)$ ako je $f(x) = 3x^3 - 2x^2 + 8x - 5$. Za račun ćemo koristiti Hornerov algoritam.
Redom popunjavamo tablicu. Najprije zapišimo ono što nam je poznato: koeficijente a_i i $\alpha = 3$.

	3	-2	8	-5
3	b_2	b_1	b_0	$f(3)$

Prema formuli, b_2 je jednak a_3, pa ga prepišemo iz gornjeg reda:

	3	-2	8	-5
3	3	b_1	b_0	$f(3)$

Sada računamo $b_1 = \alpha \cdot b_2 + a_2 = 3 \cdot 3 - 2$ i zapisujemo u tablicu:

	3	-2	8	-5
3	3	7	b_0	$f(3)$

Nastavljamo postupak dok ne popunimo cijelu tablicu:

	3	-2	8	-5
3	3	7	29	82

Iz tablice čitamo da je $f(3) = 82$.

Zadatak 6.5 Podijelite $f(x) = 2x^5 - x^3 + x + 8$ s $g(x) = x - 2$.

Zadatak 6.6 Odredite ostatak pri dijeljenju polinoma $f(x) = x^{100} + 3x^{99} + x^2 - 3x + 9$ polinomom $g(x) = x^2 + 2x - 3$.

Zadatak 6.7 Polinom $f(x) = x^3 + ax^2 - 3x + b$ pri dijeljenju polinomom $x - 2$ daje ostatak 6, a pri dijeljenju polinomom $x + 1$ ostatak 0. Odredite koeficijente a i b.

Zadatak 6.8 Polinom f pri dijeljenju s $x + 1$ daje ostatak 4, a pri dijeljenju s $x^2 + 1$ daje ostatak $2x + 3$. Odredite ostatak pri dijeljenju polinoma f s $(x + 1)(x^2 + 1)$.

Zadatak 6.9 Odredite sve polinome $f \in \mathbb{R}[x]$ koji zadovoljavaju

$$x f(x-1) = (x-3) f(x), \qquad \forall x \in \mathbb{R}.$$

6.3 Kratnost nultočke i derivacija polinoma

Definicija 6.15. Neka je $f \in \mathbb{C}[x]$ i $k \in \mathbb{N}_0$. Za $\alpha \in \mathbb{C}$ kažemo da je k-**struka** nultočka (ili nultočka **kratnosti** k) polinoma f ako je f djeljiv polinomom $(x-\alpha)^k$, ali nije djeljiv polinomom $(x-\alpha)^{k+1}$.

Primjer 6.16. Odredimo kratnost nultočke $\alpha = 2$ polinoma $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$.
Računamo Hornerovim algoritmom:

	1	-5	7	-2	4	-8
2	1	-3	1	0	4	0

Vidimo da je $f(x) = (x-2)(x^4 - 3x^3 + x^2 + 4)$. Podijelimo sada kvocijent s $x-2$:

	1	-3	1	0	4
2	1	-1	-1	-2	0

Vidimo da je $f(x) = (x-2)^2(x^3 - x^2 - x - 2)$. Nastavimo postupak:

	1	-1	-1	-2
2	1	1	1	0

Imamo i $f(x) = (x-2)^3(x^2+x+1)$. Konačno, kako je $2^2+2+1 = 7 \neq 0$, vidimo da $(x-2)^4 \nmid f$. Dakle, 2 je nultočka polinoma f kratnosti 3.

Teorem 6.17 (Osnovni teorem algebre)**.** Neka je $f \in \mathbb{C}[x]$, $\deg f \geq 1$. Tada postoji $\alpha \in \mathbb{C}$ takav da je $f(\alpha) = 0$, tj. α je nultočka polinoma f.

Korolar 6.18. Svaki polinom $f \in \mathbb{C}[x]$ stupnja $n \geq 1$ se može na jedinstven način zapisati kao produkt n polinoma prvog stupnja. Preciznije, ako je $a_n \in \mathbb{C}$ vodeći koeficijent od f, onda postoje $\alpha_1, \alpha_2 \ldots, \alpha_n \in \mathbb{C}$ takvi da je

$$f(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \qquad \forall x \in \mathbb{C}.$$

Iz korolara 6.18 slijedi da se svaki polinom $f \in \mathbb{C}[x]$ stupnja $n \geq 1$ može zapisati u obliku

$$f(x) = a_n(x-\alpha_1)^{k_1}(x-\alpha_2)^{k_2}\cdots(x-\alpha_p)^{k_p},$$

pri čemu su $\alpha_1, \ldots, \alpha_p \in \mathbb{C}$ međusobno različite nultočke polinoma f s kratnostima $k_1, \ldots, k_p$, te vrijedi $\sum_{i=1}^{p} k_i = n$.

Nadalje, svaki polinom $f \in \mathbb{R}[x]$ se može zapisati u obliku

$$f(x) = a_n(x-\alpha_1)^{k_1}\cdots(x-\alpha_s)^{k_s}(x^2+\beta_1 x+\gamma_1)^{r_1}\cdots(x^2+\beta_t x+\gamma_t)^{r_t},$$

gdje su $\alpha_1,\ldots,\alpha_s,\beta_1,\ldots,\beta_t,\gamma_1,\ldots,\gamma_t \in \mathbb{R}$, te vrijedi $2\sum_{i=1}^{t} r_i + \sum_{j=1}^{s} k_j = n$.

Korolar 6.19. (1) Svaki polinom $f \in \mathbb{C}[x]$ stupnja $n \geq 1$ ima točno n nultočaka, pri čemu svaku nultočku brojimo onoliko puta kolika joj je kratnost.

(2) Ako se polinomi $f, g \in \mathbb{C}[x]$ stupnja najviše n podudaraju u barem $n+1$ točaka, onda je $f = g$.

Definicija 6.20. Neka je $f \in \mathbb{C}[x]$, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. **Derivaciju polinoma** f definiramo kao polinom $f' \in \mathbb{C}[x]$ dan s

$$f'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

Također, induktivno možemo definirati n-tu derivaciju polinoma: $f^{(1)} = f'$, $f^{(2)} = f''$ itd., općenito

$$f^{(n+1)} = (f^{(n)})', \qquad \forall n \in \mathbb{N}.$$

Propozicija 6.21 (Svojstva derivacije)**.** Neka su $f, g \in \mathbb{C}[x]$ te $\alpha, \beta \in \mathbb{C}$. Tada vrijedi

(1) $(\alpha f + \beta g)' = \alpha f' + \beta g'$,

(2) $(fg)' = f'g + fg'$,

(3) $(f \circ g)' = (f' \circ g)g'$.

Propozicija 6.22. Ako je $\alpha \in \mathbb{C}$ nultočka kratnosti $k \geq 2$ polinoma $f \in \mathbb{C}[x]$, onda je α nultočka kratnosti $k-1$ polinoma f'.

Dokaz propozicije 6.22. Ako je $\alpha \in \mathbb{C}$ nultočka kratnosti $k \geq 2$ polinoma $f \in \mathbb{C}[x]$, tada postoji polinom $q \in C[x]$ takav da je

$$f(x) = q(x)\cdot(x-\alpha)^k.$$

Deriviranjem gornje jednakosti dobivamo

$$\begin{aligned} f'(x) &= q'(x)\cdot(x-\alpha)^k + q(x)\cdot k\cdot(x-\alpha)^{k-1} \\ &= (x-\alpha)^{k-1}\big(q'(x)\cdot(x-\alpha)+k\cdot q(x)\big), \end{aligned}$$

iz čega vidimo da $(x-\alpha)^{k-1}$ dijeli f'. Kada bi $(x-\alpha)^k$ dijelio f, iz posljednje jednakosti bi slijedilo da

$$(x-\alpha) \mid q'(x)\cdot(x-\alpha)+k\cdot q(x),$$

odnosno

$$(x-\alpha) \mid q(x),$$

što je nemoguće jer bi tada α bila nultočka kratnosti $k+1$ polinoma f. □

Zadatak 6.10 Dokažite da polinom x^n-1 nema višestrukih nultočaka.

Zadatak 6.11 Odredite nužne i dovoljne uvjete na koeficijente polinoma

$$p(x) = ax^5+bx^4+cx^3+dx^2+ex+f$$

da bi on bio djeljiv polinomom $g(x)=x^3-3x^2+3x-1$.

Zadatak 6.12 Odredite koeficijente a i b polinoma $f(x)=x^4+ax^3-2x^2+b$ tako da bude djeljiv polinomom $(x-2)^2$.

Zadatak 6.13 Odredite ostatak pri dijeljenju polinoma $f(x)=x^{100}-x^{50}+1$ polinomom $g(x)=x^2-2x+1$.

Zadatak 6.14 Dokažite da je polinom $f(x)=x^{2n}-nx^{n+1}+nx^{n-1}-1$ djeljiv polinomom $g(x)=x^3-x^2-x+1$ za svaki $n\in\mathbb{N}$.

Zadatak 6.15 Odredite sve polinome $f\in\mathbb{R}[x]$ koji zadovoljavaju

$$(x+1)f(x)=x^3+1, \quad \forall x\in\mathbb{R}.$$

Zadatak 6.16 Odredite sve polinome $f\in\mathbb{R}[x]$ koji zadovoljavaju

$$f(x^2-3)=x^2f(x-1), \quad \forall x\in\mathbb{R}. \qquad (\star)$$

6.4 Cjelobrojne i racionalne nultočke polinoma

Teorem 6.23. Neka je f polinom s cjelobrojnim koeficijentima koji ima racionalnu nultočku $\alpha = \frac{p}{q} \in \mathbb{Q}$, $M(p,q) = 1$. Tada p dijeli slobodni koeficijent, a q vodeći koeficijent polinoma f.

Dokaz teorema 6.23. Neka je

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

pri čemu su $a_n, \ldots, a_0 \in \mathbb{Z}$, $a_n \neq 0$. Prema pretpostavci teorema je $f\left(\frac{p}{q}\right) = 0$, tj.

$$0 = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Množenjem s q^n dobivamo

$$0 = a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_n p q^{n-1} + a_0 q^n.$$

Kako q očito dijeli sve pribrojnike osim prvog, mora dijeliti i $a_n p_n$, a kako su p i q relativno prosti, slijedi $q \mid a_n$. Isto tako, p dijeli sve pribrojnike osim posljednjeg, pa analogno zaključujemo $p \mid a_0$. □

Napomena 6.24. Ako polinom $f \in \mathbb{Z}[x]$ ima cjelobrojnu nultočku α, tada iz teorema 6.23 slijedi da α dijeli slobodni koeficijent od f.

Zadatak 6.17 Odredite nultočke polinoma $f(x) = x^4 - 2x^3 - 5x^2 + 4x + 6$.

Zadatak 6.18 Odredite nultočke polinoma $f(x) = 2x^3 - x^2 - 6x + 3$.

Zadatak 6.19 Odredite koeficijente a i b polinoma $f(x) = x^4 + x^3 - 18x^2 + ax + b$ ako je poznato da on ima trostruku cjelobrojnu nultočku.

Zadatak 6.20 Nađite polinom s cjelobrojnim koeficijentima kojemu je nultočka broj $\alpha = \sqrt{2} + \sqrt[3]{3}$.

Lema 6.25. Neka je f polinom s cjelobrojnim koeficijentima i $k \in \mathbb{Z}$ cijeli broj. Tada dijeljenjem polinoma f polinomom $x - k$ ponovno dobivamo polinom s cjelobrojnim koeficijentima.

Dokaz leme 6.25. Neka je $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $q(x) = b_{n-1}x^{n-1} + \ldots b_1 x + b_0$ i

$$f(x) = (x-k)q(x), \qquad \forall x \in \mathbb{R}.$$

Prema Hornerovom algoritmu, za koeficijente $b_{n-1}, \ldots, b_0$ polinoma q vrijedi $b_{n-1} = a_n$ i

$$b_i = a_{i+1} + kb_{i+1}, \qquad \forall i \in \{n-2, \ldots, 0\}.$$

Odavde vidimo da su koeficijenti $b_{n-1}, \ldots, b_0$ također cijeli brojevi. □

Zadatak 6.21 Neka je f polinom s cjelobrojnim koeficijantima. Dokažite: ako su $f(0)$ i $f(1)$ neparni brojevi, onda f nema cjelobrojnih nultočaka.

Zadatak 6.22 Dokažite da ne postoji polinom f s cjelobrojnim koeficijentima takav da je $f(0) = 2$ i $f(2) = 5$.

Zadatak 6.23 Neka je f polinom s cjelobrojnim koeficijentima i neka su $a, b, c \in \mathbb{Z}$ međusobno različiti brojevi takvi da je $f(a) = f(b) = f(c) = 3$. Dokažite da ne postoji $d \in \mathbb{Z}$ takav da je $f(d) = 2$.

Zadatak 6.24 Odredite sve nultočke polinoma

$$f(x) = x^5 - 2x^4 - 5x^3 + 8x^2 - 16x - 40$$

ako znate da je jedna od njih $x_1 = 1 - i\sqrt{3}$.

Zadatak 6.25 Zadana su dva polinoma

$$f(x) = x^3 - (a+4)x^2 + (4a+3)x - 3a,$$

$$g(x) = x^3 - 9x^2 + 26x - 24.$$

Odredite sve $a \in \mathbb{R}$ takve da je njihova najveća zajednička mjera $M(f,g)$ polinom stupnja 2.

6.5 Viéteove formule

Neka je

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

te neka su $x_1, \ldots, x_n \in \mathbb{R}$ sve njegove nultočke (ne nužno različite). Tada prema korolaru 6.18 vrijedi

$$f(x) = a_n(x - x_1)(x - x_2)\cdots(x - x_n).$$

Množenjem svih zagrada u posljednjem izrazu te izjednačavanjem koeficijenata vidimo da mora vrijediti

$$\begin{aligned}
a_0 &= (-1)^n a_n x_1 x_2 \cdots x_n \\
a_1 &= (-1)^{n-1} a_n \big(x_2 x_3 \cdots x_n + x_1 x_3 \cdots x_n + \cdots + x_1 x_2 \cdots x_{n-1}\big), \\
&\vdots \\
a_{n-2} &= a_n \big(x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n + x_2 x_3 + \cdots + x_2 x_n + \cdots + x_{n-1} x_n\big), \\
a_{n-1} &= -a_n \big(x_1 + x_2 + \cdots + x_n\big).
\end{aligned}$$

Posebno, ako je polinom f normiran, tj. ako je $a_n = 1$, dobivamo sljedeće formule:

$$\begin{gathered}
x_1 + x_2 + \cdots + x_n = -a_{n-1} \\
x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n + x_2 x_3 + \cdots + x_2 x_n + \cdots + x_{n-1} x_n = a_{n-2} \\
\vdots \\
x_2 x_3 \cdots x_n + x_1 x_3 \cdots x_n + \cdots + x_1 x_2 \cdots x_{n-1} = (-1)^{n-1} a_1 \\
x_1 x_2 \cdots x_n = (-1)^n a_0
\end{gathered}$$

Zadatak 6.26 Odredite površinu trokuta kojemu su duljine stranica nultočke polinoma

$$f(x) = x^3 + ax^2 + bx + c.$$

Zadatak 6.27 Dokažite: ako polinom $f(x) = x^3 - px + q$ s realnim koeficijentima ima tri realne međusobno različite nultočke, onda je $p > 0$.

Zadatak 6.28 Riješite sustav jednadžbi

$$\begin{cases}
x + y + z = 9, \\
xy + yz + zx = 27, \\
\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1.
\end{cases}$$

Definicija 6.26. Jednadžbu koja nakon zamjene bilo kojih dviju varijabli ostaje ista nazivamo **simetričnom**.
Sustav takvih jednadžbi nazivamo **simetričnim sustavom**.

Primjer 6.27. Uočimo da su izrazi $x+y+z$, $xy+yz+zx$ i xyz iz Viéteovih formula simetrični. Nadalje, svaki simetrični izraz u tri varijable može se izraziti pomoću ta tri osnovna simetrična izraza. Primjerice:

$$\begin{aligned} x^3+y^3+z^3 &= (x+y+z)(x^2+y^2+z^2)-xy^2-xz^2-yx^2-yz^2-zx^2-zy^2 \\ &= (x+y+z)\big((x+y+z)^2-2(xy+yz+zx)\big)-xy(x+y+z) \\ &\qquad -yz(x+y+z)-zx(x+y+z)+3xyz \\ &= (x+y+z)^3-3(x+y+z)(xy+yz+zx)+3xyz. \end{aligned}$$

Zadatak 6.29 Riješite sustav

$$\begin{cases} x+y+z=2, \\ x^2+y^2+z^2=14, \\ x^3+y^3+z^3=20. \end{cases}$$

Zadatak 6.30 Riješite sustav

$$\begin{cases} xyz=1, \\ x+y+z=xy+yz+zx, \\ x^3+y^3+z^3=\frac{73}{8}. \end{cases}$$

6.6 Rastav na parcijalne razlomke

Prisjetimo se: racionalna funkcija je funkcija oblika

$$\frac{f(x)}{g(x)}$$

pri čemu su $f,g\in\mathbb{R}[x]$ polinomi. Ovakve funkcije često je korisno izraziti kao sumu što jednostavnijih racionalnih funkcija. Tehnika kojom to postižemo je **rastav na parcijalne razlomke**.
Ako je $\deg f\geq\deg g$, prvi korak je primjena teorema o dijeljenju s ostatkom. Time dobivamo polinome q i r takve da je

$$\frac{f(x)}{g(x)}=q(x)+\frac{r(x)}{g(x)},$$

pri čemu je $\deg r<\deg g$. Dakle, problem se svodi na prikaz racionalne funkcije $\frac{r}{g}$ u željenom obliku. Stoga će nas postupak koji slijedi uglavnom zanimati za slučaj $\deg f<$

$\deg g$. Također, možemo pretpostaviti da je g normiran (u suprotnom podijelimo i brojnik i nazivnik vodećim koeficijentom od g).
Neka g ima sljedeću faktorizaciju:

$$g(x) = (x-\alpha_1)^{k_1} \cdots (x-\alpha_s)^{k_s} (x^2+\beta_1 x+\gamma_1)^{r_1} \cdots (x^2+\beta_t x+\gamma_t)^{r_t},$$

gdje su $\alpha_1, \ldots, \alpha_s$ međusobno različite realne nultočke od g, a $x^2+\beta_i x+\gamma_i$, $i \in \{1, \ldots, r\}$ međusobno različiti polinomi bez realnih nultočaka koji odgovaraju parovima konjugirano kompleksnih nultočaka od g.
Za svaki faktor oblika $(x-\alpha_i)^{k_i}$ rastav na parcijalne razlomke sadržavat će pribrojnike

$$\frac{A_{i1}}{x-\alpha_i} + \frac{A_{i2}}{(x-\alpha_i)^2} + \cdots + \frac{A_{ik_i}}{(x-\alpha_i)^{k_i}}.$$

Također, za svaki faktor oblika $(x^2+\beta_i x+\gamma_i)^{r_i}$ rastav na parcijalne razlomke sadržavat će pribrojnike

$$\frac{B_{i1}x+C_{i1}}{x^2+\beta_i x+\gamma_i} + \frac{B_{i2}x+C_{i2}}{(x^2+\beta_i x+\gamma_i)^2} + \cdots + \frac{B_{ir_i}x+C_{ir_i}}{(x^2+\beta_i x+\gamma_i)^{r_i}}.$$

Primjer 6.28. Rastav na parcijalne razlomke funkcije

$$\frac{f(x)}{g(x)} = \frac{x^2+3x+5}{(x-1)^5(x^2+x+2)^3}$$

bit će oblika

$$\frac{f(x)}{g(x)} = \frac{A}{x-1} + \frac{B}{(x-1)^2} + \frac{C}{(x-1)^3} + \frac{D}{(x-1)^4} + \frac{E}{(x-1)^5} + \frac{Fx+G}{x^2+x+2} + \frac{Hx+I}{(x^2+x+2)^2} + \frac{Jx+K}{(x^2+x+2)^3}.$$

Pri tome su $A, B, C, \ldots, J, K \in \mathbb{R}$ koeficijenti koje je potrebno odrediti.

Zadatak 6.31 Rastavite na parcijalne razlomke

$$\frac{3x^2-2}{x^3-x}.$$

Zadatak 6.32 Rastavite na parcijalne razlomke

$$\frac{1}{x^3+x^2-x-1}.$$

Zadatak 6.33 Rastavite na parcijalne razlomke

$$\frac{14x^2-51x+43}{x^3-7x^2+17x-15}.$$

Zadatak 6.34 Rastavite na parcijalne razlomke

$$\frac{6x^3-29x^2+100x-64}{(x^2-4x+13)^2}.$$

Zadatak 6.35 Rastavite na parcijalne razlomke

$$\frac{15x^2+26x-5}{x^3+3x^2-4}.$$

Upute za rješavanje zadataka

Uputa za Z6.1 Prvi uvjet kaže da je $f(x) = ax^3 + bx^2 + cx + d$ za neke nepoznate koeficijente $a, b, c, d \in \mathbb{R}$. Iskoristite drugi i treći uvjet kako biste dobili sustav jednadžbi iz kojeg je moguće odrediti te koeficijente.

Uputa za Z6.2 Iskoristite teorem o dijeljenju polinoma s ostatkom. Koji je stupanj ostatka? Uvrstite pogodnu vrijednost varijable x kako biste dobili vezu $f(\alpha)$ i ostatka.

Uputa za Z6.6 Iskoristite teorem o dijeljenju s ostatkom. Koji je stupanj ostatka? Uvrstite nultočke polinoma g kako biste poništili izraz uz $q(x)$ i sveli problem na rješavanje sustava jednadžbi.

Uputa za Z6.7 Iskoristite Bezoutov teorem.

Uputa za Z6.9 Dokažite da su 0, 1 i 2 nultočke traženog polinoma f, tj. da vrijedi $f(x) = x(x-1)(x-2)g(x)$ za neki polinom x. Što iz uvjeta zadatka možete zaključiti o polinomu g? Iskoristite činjenicu da je jedini polinom s beskonačno mnogo nultočaka nulpolinom.

Uputa za Z6.10 Višestruka nultočka nekog polinoma mora biti nultočka njegove derivacije.

Uputa za Z6.11 Uočite da je $g(x) = (x-1)^3$, pa $g \mid f$ ako i samo ako je 1 nultočka od p kratnosti barem 3.

Uputa za Z6.12 Koeficijenti a i b moraju biti takvi da 2 bude barem dvostruka nultočka od f, tj. $f(2) = f'(2) = 0$.

Uputa za Z6.13 Uvrstite pogodne vrijednosti varijable x u izraz dobiven primjenom teorema o dijeljenju s ostatkom. Isto možete učiniti s derivacijom tog izraza.

Uputa za Z6.14 Pokažite da su sve nultočke polinoma g ujedno i nultočke polinoma f.

Uputa za Z6.15 Iskoristite teorem o dijeljenju s ostatkom.

Uputa za Z6.16 Najprije odredite stupanj polinoma, a zatim njegove koeficijente.

Uputa za Z6.17 Prvo odredite cjelobrojne nultočke.

Uputa za Z6.18 Prvo odredite racionalne nultočke.

Uputa za Z6.19 Trostruka nultočka polinoma mora biti nultočka njegove prve i druge derivacije.

Uputa za Z6.21 Pretpostavite da je $k \in \mathbb{Z}$ nultočka polinoma f. Tada je $f(x) = (x-k)q(x)$. Uvrstite $x = 0$ i $x = 1$ i promatrajte parnost.

Uputa za Z6.22 Promatrajte parnost od $f(0)$ i $f(2)$.

Uputa za Z6.25 Odredite nultočke polinoma g. $M(f,g)$ će biti stupnja 2 akko f i g imaju točno dvije zajedničke nultočke.

Uputa za Z6.26 Iskoristite Heronovu formulu: $P = \sqrt{s(s-a)(s-b)(s-c)}$, gdje je $s = \frac{1}{2}(a+b+c)$.

Uputa za Z6.28 Koristeći Viéteove formule pronađite polinom kojemu su x, y i z nultočke.

Rješenja zadataka

Rješenje 6.1 Kako je traženi polinom stupnja 3, tražimo ga u obliku

$$f(x) = ax^3 + bx^2 + cx + d.$$

Uvrštavanjem $x = 0$ u gornji izraz dobivamo

$$f(0) = d,$$

odakle prema prvom uvjetu slijedi $d = 0$.
Sada uvrstimo f u treći uvjet, te dobivamo da za svaki $x \in \mathbb{R}$ mora vrijediti

$$ax^3 + bx^2 + cx - a(x-1)^3 - b(x-1)^2 - cx = x^2,$$

odakle nakon sređivanja izraza slijedi

$$3ax^2 + (2b - 3a)x + a - b + c = x^2.$$

Prema teoremu o jednakosti polinoma, izjednačavanjem koeficijenata uz odgovarajuće potencije slijedi

$$\begin{cases} 3a = 1, \\ 2b - 3a = 0, \\ a - b + c = 0. \end{cases}$$

Rješavanjem ovog sustava dobivamo

$$a = \frac{1}{3}, \quad b = \frac{1}{2}, \quad c = \frac{1}{6},$$

odnosno

$$f(x) = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x.$$

Rješenje 6.2 Prema teoremu o dijeljenju polinoma s ostatkom vrijedi

$$f(x) = q(x) \cdot (x - \alpha) + r(x), \qquad \forall x \in \mathbb{C}$$

pri čemu je $\deg r < \deg(x - \alpha) = 1$, tj. r je konstantni polinom $r(x) = a$. Uvrštavanjem $x = \alpha$ u gornju jednakost dobivamo $a = f(\alpha)$, što je upravo tražena tvrdnja.

Rješenje 6.3 S obzirom na to da je

$$f(-1) = -3+1-1+1+1+1 = 0$$

i

$$g(-1) = -1-a+a-1 = -2,$$

za bilo koji $a \in \mathbb{R}$, zaključujemo kako polinom $x+1$ dijeli f, ali ne dijeli g. Stoga ni $M(f,g)$ ne može biti djeljiva polinomom $x+1$; u suprotnom bismo imali $x+1 \mid M(f,g)$, pa $x+1 \mid g$.

Rješenje 6.4 Kako je $g(x) = x(x-1)$, polinom g dijeli f ako i samo ako polinomi x i $x-1$ dijele f, što je prema Bezoutovom teoremu ekvivalentno s time da je $f(0) = f(1) = 0$. Direktnim računanjem vidimo da je

$$f(0) = (-1)^{2n} + (-1)^{2n} - 2 = 0$$

i

$$f(1) = 1^{2n} + (-1)^{2n} - 2 = 0,$$

pa $g \mid f$ za sve $n \in \mathbb{N}$.

Rješenje 6.5 Računamo Hornerovim algoritmom:

	2	0	-1	0	1	8
2	2	4	7	14	29	66

Dakle, $f(x) = (2x^4 + 4x^3 + 7x^2 + 14x + 29)(x-2) + 66$.

Rješenje 6.6 Koristeći teorem o dijeljenju polinoma s ostatkom, možemo zapisati

$$f(x) = q(x) \cdot g(x) + r(x), \qquad \forall x \in \mathbb{C} \tag{$*$}$$

pri čemu je $\deg r < \deg g = 2$. Dakle, ostatak tražimo u obliku

$$r(x) = ax + b,$$

gdje su $a, b \in \mathbb{R}$. Kako je $g(x) = (x-1)(x+3)$, u izraz $(*)$ uvrštavamo $x = -3$ i $x = 1$ i dobivamo:

$$f(-3) = q(-3)(-3-1)(-3+3) - 3a + b = -3a + b,$$
$$f(1) = q(1)(1-1)(1-3) + a + b = a + b.$$

S druge strane, imamo

$$f(-3) = (-3)^{100} + 3\cdot(-3)^{99} + (-3)^2 - 3\cdot(-3) + 9 = 27,$$
$$f(1) = 1^{100} + 3\cdot 1^{99} + 1^2 - 3\cdot 1 + 9 = 11,$$

pa dobivamo sustav

$$\begin{cases} -3a + b = 27 \\ a + b = 11 \end{cases}$$

čije rješenje je

$$a = -4, \qquad b = 15.$$

Dakle, traženi ostatak je

$$r(x) = -4x + 15.$$

Rješenje 6.7 Iz uvjeta zadatka, prema Bezoutovom teoremu vrijedi $f(2) = 6$ i $f(-1) = 0$. S druge strane, direktnim računom dobivamo

$$f(2) = 8 + 4a - 6 + b = 4a + b + 2,$$
$$f(-1) = -1 + a + 3 + b = a + b + 2,$$

što nam daje sustav

$$\begin{cases} 4a + b = 4 \\ a + b = -2. \end{cases}$$

Rješavanjem sustava dobivamo

$$a = 2, \qquad b = -4.$$

Rješenje 6.8 Prema uvjetu zadatka vrijedi

$$f(x) = q_1(x)(x+1) + 4, \qquad \forall x \in \mathbb{C} \tag{$\star$}$$

i

$$f(x) = q_2(x)(x^2+1) + 2x + 3, \qquad \forall x \in \mathbb{C}. \tag{$\triangle$}$$

Uvrštavanjem $x = -1$ u ($\star$) dobivamo $f(-1) = 4$, a uvrštavanjem $x = \pm i$ u ($\triangle$) dobivamo $f(\pm i) = \pm 2i + 3$.

Prema teoremu o dijeljenju polinoma s ostatkom vrijedi

$$f(x) = q(x)\cdot(x+1)(x^2+1) + (ax^2+bx+c) \qquad \forall x \in \mathbb{C},$$

za neke $a, b, c \in \mathbb{C}$. Kako su nultočke polinoma $(x+1)(x^2+1)$ brojevi $x_1 = -1$, $x_2 = i$ i $x_3 = -i$, uvrštavanjem tih vrijednosti u gornju jednakost dobivamo sustav

$$\begin{cases} a - b + c = 4 \\ -a + bi + c = 2i + 3 \\ -a - bi + c = -2i + 3. \end{cases}$$

Rješenje sustava je

$$a = \frac{3}{2}, \qquad b = 2, \qquad c = \frac{9}{2},$$

pa je traženi ostatak $r(x) = \frac{3}{2}x^2 + 2x + \frac{9}{2}$.

Rješenje 6.9 Uvrstimo nekoliko vrijednost za x u gornju relaciju:

$\boxed{x=0}$ Dobivamo $0 = 3f(0)$, tj. $f(0) = 0$, pa zaključujemo da $x \mid f$.

$\boxed{x=3}$ Dobivamo $3f(2) = 0$, tj. $f(2) = 0$, pa zaključujemo da $x-2 \mid f$.

$\boxed{x=1}$ Dobivamo $f(0) = -2f(1)$, pa kako je $f(0) = 0$ slijedi $f(1) = 0$. Dakle, $x-1 \mid f$.

Dakle, ako postoji, traženi polinom f je oblika

$$f(x) = x(x-1)(x-2)g(x),$$

za neki polinom $g \in \mathbb{R}[x]$. Uvrštavanjem ovog izraza u početnu relaciju dobivamo

$$x(x-1)(x-2)(x-3)g(x-1) = (x-3)x(x-1)(x-2)g(x), \qquad \forall x \in \mathbb{R}.$$

Za sve vrijednosti varijable x različite od $0, 1, 2, 3$ izraz $x(x-1)(x-2)(x-3)$ s obje strane će se skratiti, pa slijedi

$$g(x-1) = g(x), \qquad \forall x \in \mathbb{R} \setminus \{0,1,2,3\}.$$

Posebno, imamo $g(3) = g(4) = g(5) = g(6) = \ldots$, tj. $g(3) = g(n)$, $\forall n \in \mathbb{N} \setminus \{1,2\}$. Promotrimo polinom $h(x) = g(x) - g(3)$. Za svaki prirodan broj $n \geq 3$ vrijedi $h(n) = g(n) - g(3) = 0$, pa su svi prirodni brojevi veći od 2 nultočke polinoma h. To je moguće samo ako je h nulpolinom, a u tom slučaju je $g(x) = h(x) + g(3) = g(3)$ konstantni polinom. Dakle, ako je f polinom koji zadovoljava uvjet zadatka, on mora biti oblika

$$f(x) = C \cdot x(x-1)(x-2)$$

za neku konstantu $C \in \mathbb{R}$. Direktnom provjerom lako vidimo da zaista svaki takav polinom zadovoljava traženu jednakost.

Rješenje 6.10 Kada bi neka od nultočki bila višestruka, tj. kratnonsti barem 2, tada bi ona ujedno bila i nultočka polinoma

$$f'(x) = nx^{n-1}.$$

Jedina nultočka ovog polinoma je $x = 0$, a kako to nije nultočka polaznog polinoma, zaključujemo da polinom nema višestrukih nultočaka.

Rješenje 6.11 Kako je $g(x) = (x-1)^3$, polinom p će biti djeljiv polinomom g ako i samo ako je 1 barem trostruka nultočka polinoma p. To je pak ekvivalentno s time da je 1 nultočka polinoma p, p' i p''. Imamo

$$p'(x) = 5ax^4 + 4bx^3 + 3cx^2 + 2dx + e \quad \text{i}$$
$$p''(x) = 20ax^3 + 12bx^2 + 6cx + 2d,$$

pa iz $p(1) = p'(1) = p''(1) = 0$ dobivamo sustav

$$\begin{cases} a+b+c+d+e+f = 0, \\ 5a+4b+3c+2d+e = 0, \\ 10a+6b+3c+d = 0. \end{cases}$$

Kako imamo tri jednadžbe i šest nepoznanica, rješenje sustava će biti parametrizirana familija s tri slobodna parametra, npr. a, b i c. Preostali koeficijenti moraju zadovoljavati

$$d = -10a - 6b - 3c, \qquad e = 15a + 8b + 3c \quad \text{i} \quad f = -26a - 15b - 7c.$$

Rješenje 6.12 Da bi f bio djeljiv s $(x-2)^2$, $x = 2$ mora biti njegova barem dvostruka nultočka. Stoga mora biti $f(2) = f'(2) = 0$. Kako je

$$f'(x) = 4x^3 + 3ax^2 - 4x,$$

dobivamo sustav

$$\begin{cases} 8a+b+8 = 0, \\ 12a+24 = 0 \end{cases}$$

čije rješenje je

$$a = -2 \quad \text{i} \quad b = 8.$$

Rješenje 6.13 Uočimo da je $g(x) = (x-1)^2$. Prema teoremu o dijeljenju s ostatkom, vrijedi

$$f(x) = q(x)(x-1)^2 + ax + b, \quad \forall x \in \mathbb{R}. \tag{$*$}$$

Odredimo koeficijente a i b. Uvrštavanjem $x = 1$ u gornju jednakost dobivamo

$$1 = f(1) = a + b.$$

Deriviranjem izraza $(*)$ dobivamo

$$100x^{99} - 50x^{49} = f'(x) = q'(x)(x-1)^2 + q(x) \cdot 2(x-1) + a,$$

pa ponovnim uvrštavanjem $x = 1$ dobivamo

$$50 = f'(1) = a.$$

Dakle, imamo sustav

$$\begin{cases} a + b = 1 \\ a = 50, \end{cases}$$

čije rješenje je

$$a = 50 \quad \text{i} \quad b = -49.$$

Konačno, traženi ostatak je $r(x) = 50x - 49$.

Rješenje 6.14 Kako je $g(x) = (x-1)^2(x+1)$, dovoljno je provjeriti da je $f(1) = f'(1) = f(-1) = 0$ za sve $n \in \mathbb{N}$. Direktnim uvrštavanjem lako vidimo da je $f(1) = f(-1) = 0$, dok je

$$f'(x) = 2nx^{2n-1} - n(n+1)x^n + n(n-1)x^{n-2},$$

pa uvrštavanjem $x = 1$ vidimo da je i $f'(1) = 0$.

Rješenje 6.15 Prema teoremu o dijeljenju polinoma s ostatkom, postoji jedinstven polinom f koji zadovoljava zadani uvjet. Kako je $x^3 + 1 = (x+1)(x^2 - x + 1)$, slijedi da je jedino rješenje $f(x) = x^2 - x + 1$.

Rješenje 6.16 Najprije uočimo da nulpolinom zadovoljava zadanu jednakost, pa je jedno rješenje $f(x) = 0$.
Pretpostavimo sada da $f \neq 0$ zadovoljava zadanu jednakost i označimo $n := \deg f$. Kako je

$$\deg f(x^2 - 3) = \deg f \cdot \deg(x^2 - 3) = 2n$$

te

$$\deg x^2 f(x-1) = \deg(x^2) + \deg f \cdot \deg(x-1) = 2 + n,$$

slijedi $n = 2$. Možemo nastaviti na dva načina:

(I) Uvrštavanjem $x=0$ u $(\star)$ dobivamo $f(-3)=0$, pa slijedi $x+3 \mid f$. Nadalje, uvrštavanjem $x=-2$ dobivamo $f(1)=4f(-3)=0$, pa slijedi $x+2 \mid f$. Kako je $\deg f=2$, zaključujemo da su -3 i 1 jedine nultočke od f, pa je f oblika $f(x)=C(x-1)(x+3)$ za neku konstantu $C \in \mathbb{R}\setminus\{0\}$. Uvrštavanjem u $(\star)$ dobivamo

$$C(x^2-4)\cdot x^2 = x^2\cdot C(x-2)(x+2)$$

što zaista vrijedi za sve $x\in\mathbb{R}$. Dakle, svaki polinom tog oblika je rješenje zadatka.

(II) Kako je $\deg f=2$, polinom f je oblika $f(x)=ax^2+bx+c$, $a\neq 0$. Uvrštavanjem u $(\star)$ dobivamo

$$a(x^2-3)^2+b(x^2-3)+c = x^2\big(a(x-1)^2+b(x-1)+c\big),$$

odnosno

$$ax^4+(b-6a)x^2+9a-3b+c = ax^4+(b-2a)x^3+(a-b+c)x^2.$$

Iz teorema o jednakosti polinoma dobivamo sustav

$$\begin{cases} b-2a=0 \\ 7a-2b+c=0 \\ 9a-3b+c=0 \end{cases}$$

Kako oduzimanjem treće jednadžbe od druge dobivamo prvu, vidimo da nećemo dobiti jedinstveno rješenje. Rješenje sustava je jednoparametarska familija

$$\{(a,2a,-3a) \mid a\in\mathbb{R}\setminus\{0\}.$$

Dakle, traženi polinomi f moraju biti oblika

$$f(x)=ax^2+2ax-3a=a(x^2+2x-3), \qquad a\in\mathbb{R}\setminus\{0\}.$$

(Uočimo da je $(x-1)(x+3)=x^2+2x-3$, tj. na oba načina smo dobili isto rješenje.)
Uzevši u obzir i ranije spomenuto rješenje $f=0$, sva rješenja možemo zapisati kao

$$f(x)=C(x-1)(x+3), \qquad C\in\mathbb{R}.$$

Rješenje 6.17 Prvo potražimo moguće cjelobrojne nultočke polinoma f koristeći prethodni teorem. Ukoliko postoji cjelobrojna nultočka, tada ona mora dijeliti 6, pa su nam kandidati brojevi $\pm 1, \pm 2, \pm 3, \pm 6$. Provjerimo Hornerovim algoritmom koji od kandidata su zaista nultočke:

	1	-2	-5	4	6	
1	1	-1	-6	-2	4	✗
-1	1	-3	-2	6	0	✓

Vidimo da je $f(x) = (x+1)(x^3 - 3x^2 - 2x + 6)$, pa će sve ostale nultočke od f biti nultočke polinoma $x^3 - 3x^2 - 2x + 6$. Nastavimo provjeru s tim polinomom:

	1	-3	-2	6	
-1	1	-4	2	4	✗
2	1	-1	-4	-2	✗
-2	1	-5	-8	-10	✗
3	1	0	-2	0	✓

Dakle, imamo

$$f(x) = (x+1)(x-3)(x^2-2).$$

Kako su nultočke polinoma $x^2 - 2$ brojevi $\pm\sqrt{2}$, zaključujemo da su -1, 3, $-\sqrt{2}$ i $\sqrt{2}$ sve nultočke polinoma f.

Rješenje 6.18 Kandidati za cjelobrojne nultočke od f su ± 1 i ± 3. Imamo

	2	-1	-6	3
1	2	1	-5	-2
-1	2	-3	-3	6
3	2	5	9	30
-3	2	-7	15	-42

Pa vidimo da f nema cjelobrojnih nultočaka.
Kandidati za racionalne nultočke su brojevi $\pm\frac{1}{2}$ i $\pm\frac{3}{2}$. Kako je

	2	-1	-6	3
$\frac{1}{2}$	2	0	-6	0

imamo

$$f(x) = \left(x - \frac{1}{2}\right)(2x^2 - 6),$$

pa su nultočke polinoma f brojevi $\frac{1}{2}, -\sqrt{3}, \sqrt{3}$.

Rješenje 6.19 Neka je $\alpha \in \mathbb{Z}$ trostruka cjelobrojna nultočka polinoma f. Tada je α također nultočka polinoma

$$f'(x) = 4x^3 + 3x^2 - 36x + a,$$

te polinoma

$$f''(x) = 12x^2 + 6x - 36 = 6(2x^2 + x - 6) = 12(x+2)(x - \frac{3}{2}).$$

Kako je -2 jedina cjelobrojna nultočka polinoma f'', zaključujemo da mora biti $\alpha = -2$. Sada koristimo $f'(\alpha) = f(\alpha) = 0$ i dobivamo

$$\begin{aligned} 0 = f'(-2) &= 52 + a \\ 0 = f(-2) &= -64 - 2a + b \end{aligned}$$

odakle slijedi $a = -52$ i $b = -40$.

Rješenje 6.20 Imamo

$$\begin{aligned} & \alpha = \sqrt{2} + \sqrt[3]{3} \\ \iff \quad & \sqrt[3]{3} = \alpha - \sqrt{2} \\ \iff \quad & 3 = \alpha^3 - 3\sqrt{2}\alpha^2 + 6\alpha - 2\sqrt{2} \\ \iff \quad & (3\alpha^2 + 2)\sqrt{2} = \alpha^3 + 6\alpha - 3 \\ \implies \quad & 2(9\alpha^4 + 12\alpha^2 + 4) = \alpha^6 + 36\alpha^2 + 9 + 12\alpha^4 - 6\alpha^3 - 36\alpha \\ \iff \quad & \alpha^6 - 6\alpha^4 - 6\alpha^3 + 12\alpha^2 - 36\alpha + 1 = 0. \end{aligned}$$

Odavde vidimo da je α nultočka polinoma

$$f(x) = x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1.$$

Rješenje 6.21 Dat ćemo dva rješenja:

(I) Neka je $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Primijetimo prvo kako je prema pretpostavci zadatka

$$f(0) = a_0 \equiv 1 \pmod 2 \quad \text{i} \quad f(1) = a_n + \cdots + a_1 + a_0 \equiv 1 \pmod 2.$$

Neka je $k \in \mathbb{Z}$. Imamo dvije mogućnosti:

1°) $\boxed{k \equiv 0 \pmod 2}$ Tada je

$$f(k) \equiv a_n \cdot 0 + \cdots + a_1 \cdot 0 + a_0 = a_0 \equiv 1 \pmod 2,$$

pa k ne može biti nultočka polinoma f.

2°) $\boxed{k \equiv 1 \pmod 2}$ Tada je

$$f(k) \equiv a_n \cdot 1 + \cdots + a_1 \cdot 1 + a_0 \equiv 1 \pmod 2,$$

pa vidimo da ni u ovom slučaju k ne može biti nultočka polinoma f.

Dakle, f nema cjelobrojnih nultočaka.

(II) Pretpostavimo da je $k \in \mathbb{Z}$ nultočka polinoma f. Tada je prema Bezoutovom teoremu

$$f(x) = (x-k)q(x), \qquad (\star)$$

za neki polinom q s cjelobrojnim koeficijentima. Uvrštavanjem $x = 0$ i $x = 1$ u $(\star)$ dobivamo

$$-k \cdot q(0) = f(0) \quad \text{i} \quad (1-k)q(1) = f(1).$$

Kako su $-k$ i $1-k$ uzastopni cijeli brojevi, barem jedan od njih mora biti paran. No, to nas vodi na kontradikciju: kada bi primjerice $-k$ bio paran, budući da je $q(0)$ cijeli broj, prema gornjoj jednakosti bi i $f(0)$ trebao biti paran, što je suprotno pretpostavci zadatka. Slično, kada bi $1-k$ bio paran, i $f(1)$ bi morao biti paran. Dakle, f ne može imati cjelobrojnu nultočku.

Rješenje 6.22 Iz $f(0) = 2$ slijedi da je $f(x) = x \cdot q(x) + 2$ za neki polinom q s cjelobrojnim koeficijentima. Uvrštavanjem $x = 2$ u tu formulu dobivamo

$$f(2) = 2 \cdot q(2) + 2$$

što je paran broj, pa ne može biti $f(2) = 5$.

Rješenje 6.23 Pretpostavimo da je $d \in \mathbb{Z}$ takav da je $f(d) = 2$. Tada je

$$f(x) = (x-d)q(x) + 2, \qquad (*)$$

za neki polinom q s cjelobrojnim koeficijentima. Uvrštavanjem $x = a$ u $(*)$ dobivamo

$$3 = f(a) = (a-d)q(d) + 2,$$

odnosno $(a-d)q(d) = 1$. Kako su $a-d$ i $q(d)$ cijeli brojevi, oni moraju biti djelitelji od 1, pa je $a-d \in \{\pm 1\}$.

Analogno, nakon uvrštavanja $x = b$ i $x = c$ u $(*)$ zaključujemo $b-d, c-d \in \{\pm 1\}$. Dakle, vrijedi

$$d-a, d-b, d-c \in \{\pm 1\},$$

pa po Dirichletovom principu barem dva od ta tri broja moraju biti jednaka. No, ako je npr. $d-a = d-b$, onda je i $a = b$, što je u kontradikciji s pretpostavkom zadatka.

Rješenje 6.24 Kako je $\alpha = 1 - i\sqrt{3}$ nultočka polinoma $f \in \mathbb{R}[x]$, onda je i

$$\overline{\alpha} = 1 + i\sqrt{3}$$

također nultočka. Dijeljenjem polinoma f polinomom $(x-\alpha)(x-\overline{\alpha}) = x^2 - 2x + 4$ dobivamo polinom

$$q(x) = x^3 - 9x - 10.$$

Nultočke ovog polinoma tražimo među cjelobrojnim djeliteljima broja 10. Standardnom provjerom Hornerovim algoritmom dobivamo

	1	0	-9	-10
-2	1	-2	-5	0

tj. $q(x) = (x+2)(x^2 - 2x - 5)$. Nultočke ovog polinoma su još i

$$x_{1,2} = \frac{2 \pm \sqrt{4+20}}{2} = 1 \pm \sqrt{6}.$$

Dakle, sve nultočke polinoma f su $\{-2, 1 \pm \sqrt{6}, 1 \pm i\sqrt{3}\}$.

Rješenje 6.25 Najprije faktorizirajmo polinom g:

$$g(x) = (x-2)(x-3)(x-4).$$

Da bi $M(f,g)$ polinom stupnja 2, točno dvije nultočke polinoma g moraju biti i nultočke polinoma f. Imamo

$$f(2) = 8 - 4(a+4) + 2(4a+3) - 3a = a - 2$$
$$f(3) = 27 - 9(a+4) + 3(4a+3) - 3a = 0$$
$$f(4) = 64 - 16(a+4) + 4(4a+3) - 3a = 12 - 3a.$$

Vidimo da je 3 nultočka polinoma f za sve $a \in \mathbb{R}$. Za $a = 2$ broj 2 će također biti nultočka od f. Slično, za $a = 4$ broj 4 će također biti nultočka od f.
Dakle, polinomi f i g će imati točno dvije zajedničke nultočke akko je $a \in \{2, 4\}$.

Rješenje 6.26 Koristimo Heronovu formulu za površinu trokuta: ako su x_1, x_2, x_3 duljine stranica trokuta, tada je površina trokuta P jednaka

$$P = \sqrt{s(s-x_1)(s-x_2)(s-x_3)},$$

pri čemu je $s = \frac{1}{2}(x_1+x_2+x_3)$. Uočimo i da je $f(x) = (x-x_1)(x-x_2)(x-x_3)$, pa je $P = \sqrt{s \cdot f(s)}$. Prema Viéteovim formulama imamo $x_1+x_2+x_3 = -a$, pa je $s = -\frac{1}{2}a$.
Dakle, imamo

$$\begin{aligned} P &= \sqrt{s \cdot f(s)} \\ &= \sqrt{-\frac{1}{2}a\Big(-\frac{1}{8}a^3 + \frac{1}{4}a^3 - \frac{1}{2}ab + c\Big)} \\ &= \frac{1}{4}\sqrt{a(4ab - a^3 - 8c)}. \end{aligned}$$

Rješenje 6.27 Prema Viéteovim formulama imamo

$$\begin{aligned} x_1 + x_2 + x_3 &= 0, \\ x_1x_2 + x_2x_3 + x_3x_1 &= -p. \end{aligned}$$

Kvadriranjem prve jednakosti slijedi

$$0 = (x_1+x_2+x_3)^2 = x_1^2 + x_2^2 + x_3^2 + 2(x_1x_2 + x_2x_3 + x_3x_1),$$

odakle dobivamo

$$x_1^2 + x_2^2 + x_3^2 = 2p.$$

Kako je zbroj kvadrata realnih brojeva veći ili jednak od nule, zaključujemo $p \geq 0$. Konačno, p ne može biti jednako 0 jer bismo tada imali $x_1 = x_2 = x_3 = 0$, što je nemoguće prema pretpostavci zadatka.

Rješenje 6.28 Primijetimo prvo kako iz druge jednadžbe slijedi

$$1 = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{yz + xz + xy}{xyz} = \frac{27}{xyz},$$

pa je $xyz = 27$. Sada vidimo da x, y, z rješavaju sustav

$$\begin{cases} x + y + z = 9, \\ xy + yz + zx = 27, \\ xyz = 27, \end{cases}$$

što su upravo Viéteove formule za polinom

$$t^3 - 9t^2 + 27t - 27 = (t-3)^3.$$

Dakle, rješenje sustava su sve moguće uređene trojke (x, y, z) nultočaka navedenog polinoma. S obzirom da $t = 3$ jedina (trostruka) nultočka ovog polinoma, onda je jedino rješenje ovog sustava

$$x = y = z = 3.$$

Rješenje 6.29 Ponovno ćemo rješenje pronaći kao sve moguće trojke nultočaka polinoma koji zadovoljava odgovarajuće Viéteove formule. Kvadriranjem prve jednakosti dobivamo

$$4 = (x+y+z)^2 = 14 + 2(xy + yz + zx),$$

odakle slijedi

$$xy + yz + zx = -5.$$

Nadalje, prema formuli iz primjera 6.27 je

$$\begin{aligned} xyz &= \frac{1}{3}\left(x^3 + y^3 + z^3 - (x+y+z)^3 + 3(x+y+z)(xy+yz+zx)\right) \\ &= \frac{1}{3}\left(20 - 8 + 3 \cdot 2 \cdot (-5)\right) \\ &= -6 \end{aligned}$$

Dakle, x, y, z zadovoljavaju sustav

$$\begin{cases} x + y + z = 2, \\ xy + yz + zx = -5, \\ xyz = -6, \end{cases}$$

što su Viéteove formule za polinom

$$f(t) = t^3 - 2t^2 - 5t + 6.$$

Odredimo nultočke ovog polinoma. Kandidati za cjelobrojne nultočke su djelitelji od 6. Direktnom provjerom pomoću Hornerovog algoritma dobivamo

	1	-2	-5	6
1	1	-1	-6	0

Pa je $f(t) = (t-1)(t^2-t-6)$. Preostale nultočke polinoma f su

$$t_{1,2} = \frac{1 \pm \sqrt{1+24}}{2} = \frac{1 \pm 5}{2}$$

Dakle, skup nultočaka polinoma f je $\{-2,1,3\}$, pa imamo 6 različitih rješenja ovog sustava:

$$(x,y,z) \in \big\{(-2,1,3),(-2,3,1),(1,-2,3),(1,3,-2),(3,-2,1),(3,1,-2)\big\}.$$

Rješenje 6.30 Označimo sa $a = x+y+z = xy+yz+zx$. Rješenja sustava x,y,z ćemo tražiti među nultočkama polinoma oblika

$$f(t) = t^3 - at^2 + at - 1.$$

Primijetimo odmah kako je $f(1) = 1-a+a-1 = 0$, tj. $t = 1$ je jedna nultočka ovog polinoma. Dakle, ako je (x,y,z) rješenje sustava, jedna od varijabli će biti jednaka 1. Zbog simetričnosti možemo bez smanjenja općenitosti uzeti $x = 1$. Tada imamo sustav

$$\begin{cases} yz = 1, \\ 1+y+z = y+z+yz, \\ 1+y^3+z^3 = \frac{78}{3}, \end{cases}$$

odnosno

$$\begin{cases} yz = 1, \\ y^3+z^3 = \frac{65}{8}. \end{cases}$$

Iz prve jednadžbe imamo $z = \frac{1}{y}$ (uočimo da $y = 0$ ne može biti rješenje!), pa uvrštavanjem u drugu jednadžbu dobivamo

$$y^6 - \frac{65}{8}y^3 + 1 = 0.$$

Supstitucijom $t = y^3$ dobivamo kvadratnu jednadžbu čija rješenja su

$$t_1 = 8 \quad \text{i} \quad t_2 = \frac{1}{8},$$

odakle slijedi

$$y_1 = 2 \quad \text{i} \quad y_2 = \frac{1}{2}.$$

Konačno, imamo

$$z_1 = \frac{1}{2} \quad \text{i} \quad z_2 = 2.$$

Dakle, rješenja su

$$(x,y,z) \in \left\{\left(1,2,\frac{1}{2}\right),\left(1,\frac{1}{2},2\right),\left(\frac{1}{2},2,1\right),\left(\frac{1}{2},2,1\right),\left(2,\frac{1}{2},1\right),\left(2,1,\frac{1}{2}\right)\right\}.$$

Rješenje 6.31 Imamo $g(x) = x^3 - x = x(x-1)(x+1)$, pa rastav na parcijalne razlomke tražimo u obliku

$$\frac{3x^2-2}{x^3-x} = \frac{A}{x} + \frac{B}{x-1} + \frac{C}{x+1}.$$

Množenjem jednakosti s $x^3 - x$ dobivamo

$$A(x^2-1) + B(x^2+x) + C(x^2-x) = 3x^2 - 2,$$

odnosno

$$(A+B+C)x^2 + (B-C)x - A = 3x^2 - 2.$$

Izjednačavanjem odgovarajućih koeficijenata dobivamo sustav

$$\begin{cases} A+B+C = 3 \\ B-C = 0 \\ -A = -2, \end{cases}$$

čije rješenje je

$$A = 2, \quad B = C = \frac{1}{2}.$$

Dakle, rastav na parcijalne razlomke glasi

$$\frac{3x^2-2}{x^3-x} = \frac{2}{x} + \frac{1}{2}\frac{1}{x-1} + \frac{1}{2}\frac{1}{x+1}.$$

Rješenje 6.32 Imamo $g(x) = x^3 + x^2 - x - 1 = (x-1)(x+1)^2$, pa rastav tražimo u obliku

$$\frac{1}{x^3+x^2-x-1} = \frac{A}{x-1} + \frac{B}{x+1} + \frac{C}{(x+1)^2}.$$

Množenjem s $(x-1)(x+1)^2$ dobivamo

$$A(x+1)^2 + B(x+1)(x-1) + C(x-1) = 1.$$

Uvrštavanjem $x = \pm 1$ u gornju jednadžbu dobivamo

$$4A = 1 \quad \text{i} \quad -2C = 1,$$

tj. $A=\frac{1}{4}$ i $B=-\frac{1}{2}$. konačno, uvrštavanjem $x=0$ dobivamo

$$A-B-C=1,$$

odakle slijedi $B=-\frac{1}{4}$. Dakle, traženi rastav je

$$\frac{1}{x^3+x^2-x-1}=\frac{1}{4(x-1)}-\frac{1}{4(x+1)}-\frac{1}{2(x+1)^2}.$$

Rješenje 6.33 Imamo $g(x)=x^3-7x^2+17x-15=(x-3)(x^2-4x+5)$, pa rastav tražimo u obliku

$$\frac{14x^2-51x+43}{x^3-7x^2+17x-15}=\frac{A}{x-3}+\frac{Bx+C}{x^2-4x+5}.$$

Množenjem s $(x-3)(x^2-4x+5)$ dobivamo

$$A(x^2-4x+5)+(Bx+C)(x-3)=14x^2-51x+43.$$

Izjednačavanjem odgovarajućih koeficijenata (ili uvrštavanjem odgovarajućih vrijednosti) dobivamo sustav čije rješenje je

$$A=8,\quad B=6,\quad C=-1.$$

Dakle, rastav glasi

$$\frac{14x^2-51x+43}{x^3-7x^2+17x-15}=\frac{8}{x-3}+\frac{6x-1}{x^2-4x+5}.$$

Rješenje 6.34 Imamo $g(x)=(x^2-4x+13)^2$, pa rastav tražimo u obliku

$$\frac{6x^3-29x^2+100x-64}{(x^2-4x+13)^2}=\frac{Ax+B}{x^2-4x+13}+\frac{Cx+D}{(x^2-4x+13)^2}.$$

Rješenje je

$$\frac{6x^3-29x^2+100x-64}{(x^2-4x+13)^2}=\frac{6x-5}{x^2-4x+13}+\frac{2x+1}{(x^2-4x+13)^2}.$$

Rješenje 6.35 Imamo $g(x)=x^3+3x^2-4=(x-1)(x+2)^2$, pa rastav tražimo u obliku

$$\frac{15x^2+26x-5}{x^3+3x^2-4}=\frac{A}{x-1}+\frac{B}{x+2}+\frac{C}{(x+2)^2}.$$

Rješenje je

$$\frac{15x^2+26x-5}{x^3+3x^2-4}=\frac{4}{x-1}+\frac{11}{x+2}-\frac{1}{(x+2)^2}.$$