SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Anja Posel

TEHNIKE U RJEŠAVANJU MATEMATIČKIH PROBLEMA

Diplomski rad

Voditelj rada:
prof. dr. sc. Ljiljana Arambašić

Zagreb, 2022.

Ovaj diplomski rad obranjen je dana ____________________ pred ispitnim povjerenstvom u sastavu:

1. ____________________________, predsjednik
2. ____________________________, član
3. ____________________________, član

Povjerenstvo je rad ocijenilo ocjenom _______________.

Potpisi članova povjerenstva:

1. ____________________________
2. ____________________________
3. ____________________________

Iskreno se zahvaljujem svojoj mentorici prof. dr. sc. Ljiljani Arambašić na suradnji, susretljivosti i podršci tijekom izrade diplomskog rada. Hvala Vam na prijateljskom pristupu i što ste uvijek našli vremena za mene te svojim korisnim savjetima upotpunili ovaj rad.

Veliko hvala mojim roditeljima i obitelji na bezuvjetnoj ljubavi i potpori te velikom razumijevanju, bez vas ovo ne bi bilo moguće.

Zahvaljujem se prijateljima što su bili uz mene u dobrim i teškim trenucima te na nezaboravnim doživljajima tijekom studiranja.

Sadržaj

Uvod

U različitim svakodnevnim situacijama susrećemo se s problemima koje pokušavamo riješiti na različite načine. Problemi su pitanja na koja ne možemo odmah dati odgovor, često su otvorenog tipa, apstraktni, a ponekad i teško rješivi te zahtijevaju od nas promišljanje i istraživanje. U ovom radu proučavat ćemo matematičke probleme. Rješavanje matematičkih problema jedan je od najvažnijih ciljeva matematičkog obrazovanja. Ono ne samo da potiče kreativnost, sustavnost, preciznost, apstraktno i kritičko promišljanje, već omogućuje razvoj matematičkih znanja i vještina te samopouzdanje, koncentraciju i hrabrost, kojima će se učenici koristiti u daljnjem osobnom, društvenom i profesionalnom životu. Rješavanjem velikog broja različitih problema učenici usvajaju razne tehnike i metode koje im kasnije mogu poslužiti za rješavanje drugih problema. Učenici, rješavanjem matematičkih problema koji opisuju situacije iz stvarnog života, razvijaju pozitivan stav prema matematici te uočavaju da je matematika svuda oko nas i ima utjecaj na sve životne segmente pojedinca.

Ovaj rad započinje opisom matematičkog problema te klasifikacijama matematičkih zadataka pomoću kojih se rješavaju problemi u nastavi matematike. Opisuju se i uspoređuju nastavni sustavi, problemska i heuristička nastava pomoću kojih se učenike poučava rješavanju problema. Prema Georgeu Pólyu, vještina rješavanja problema može se poučiti i naučiti pa je u ovom radu opisana njegova metoda za univerzalno rješavanje matematičkog zadatka te su navedene heuristike i metode koje se koriste pri rješavanju. Nakon toga, slijedi rješavanje matematičkih problema iz područja nejednakosti i aritmetike. S obzirom na njihovu složenost, prije rješavanja potrebno je usvojiti određena znanja i tehnike da bi ih mogli uspješno i efikasno riješiti. Na primjer, iako mnogi zadaci iz nejednakosti na prvi pogled mogu izgledati kao da ćemo ih riješiti direktnim sređivanjem algebarskih izraza koji se u njemu pojavljuju, često nećemo uspjeti doći do rješenja na taj način. S druge strane, takvi zadaci mogu biti poseban slučaj neke poznate nejednakosti, odnosno lako su rješivi ako prepoznamo koju posebnu nejednakost trebamo uvrstiti. Zato je važno poznavati teorijsku osnovu i važne teoreme iz područja kojim se bavimo. U ovom će radu biti bitno poznavati nejednakosti između srednjih vrijednosti i Cauchy-Schwarzovu nejednakost za rješavanje zadataka iz područja nejednakosti, a za područje aritmetike važni su pojam djeljivosti, najvećeg zajedničkog djelitelja i kongruencija te osnovni teorem aritmetike.

Poglavlje 1

Rješavanje matematičkih problema

1.1 Matematički problem

Riječ *problem* izvorno je grčkog porijekla i znači: *teorijsko ili praktično pitanje koje treba riješiti, sporno pitanje, teškoća, težak zadatak, zadaća uopće, zagonetka* ([7]). Specifičnost problema je da ono što je problem za jednu osobu, nije nužno problem za drugu osobu. To je zato što ne postoje dvije osobe s jednakim sposobnostima i iskustvom, stoga bi jedna osoba mogla brže razumjeti formulaciju nekog problema te pronaći njegovo rješenje, nego neka druga. Ovdje ćemo se ograničiti na promišljanje o matematičkim problemima iako je, naravno, cilj obrazovanja osposobiti učenike za rješavanje problema različitih vrsta.

Matematičko obrazovanje sastoji se od nastavnih sadržaja, matematičkog jezika i vještina te kognitivnog razvoja učenika. Kako bi mogli uspješno razumjeti i riješiti problemski zadatak, pogotovo "zadatak s riječima", trebamo razumjeti matematički jezik te moći prevoditi simbole i izraze s matematičkog na svoj materinski jezik i obrnuto. Vještine su sposobnosti stečene vježbom niza osnovnih aritmetičkih operacija i algoritama potrebnih za rješavanje nekog problemskog zadatka. One se upotrebljavaju u svim matematičkim domenama: *Brojevi, Algebra i funkcije, Oblik i prostor, Mjerenje* te *Podatci, statistika i vjerojatnost*. S druge strane, matematički procesi su načini kreativne upotrebe vještina u novim situacijama. Matematički procesi uključuju prikazivanje i komunikaciju, povezivanje, logičko mišljenje, argumentiranje i zaključivanje, primjenu tehnologiju te rješavanje problema i matematičko modeliranje.

Prije nego što opišemo rješavanje problema u nastavi matematike, istaknimo tri riječi: *metoda*, *odgovor* i *rješenje*. Riječ *metoda* predstavlja sredstva koja se koriste da se dobije odgovor, što općenito uključuje jednu ili više strategija rješavanja problema. S druge strane, koristimo riječ *odgovor* da označimo broj, količinu ili neki drugi pojam koji se traži u zadanom problemu. Konačno, *rješenje* je cijeli proces rješavanja problema, uključujući metodu dobivanja odgovora i sam odgovor.

U nastavi matematike, problemi i problemske situacije najčešće se rješavaju kroz problemske zadatke. Zadatak je složen matematički objekt i njegov sastav nije uvijek jednostavno analizirati ([6]). Rješavanje zadataka jedna je od najčešćih uloga učenika na nastavi matematike. Primjerenim izborom i korištenjem zadataka u nastavi matematike znatno doprinosimo oblikovanju učenikovih osnovnih matematičkih znanja, umijeća, vještina i navika te doprinosimo razvoju matematičkih sposobnosti i stvaralačkog mišljenja. Kurnik izdvaja pet osnovnih sastavnica zadatka: uvjeti, cilj, teorijska osnova, rješavanje te osvrt ([6]).

Uvjeti su sastavni dio svakog zadatka i to su poznate i nepoznate veličine i objekti te uvjeti koji opisuju veze između poznatih i nepoznatih veličina i objekata. Da bi razumjeli zadatak važno je poznavati uvjete.

Cilj zadatka najčešće je lako uočljiv. To je pronalaženje rješenja, tj. određivanje nepoznatih veličina, svojstava i veza među njima ili izvođenje zaključaka i opravdavanje postavljenih tvrdnji.

Kako bi otkrili postupak rješavanja zadatka potrebno je imati **teorijsku osnovu**, matematička znanja i vještine, usko povezane uz uvjete i cilj zadatka. Odnose između danih i traženih veličina otkrivamo proučavanjem i analizom uvjeta te primjenom određenih teorijskih činjenica.

Prijelaz od uvjeta do rješenja zadatka prethodno otkrivenim postupkom nazivamo **rješavanje** zadatka i time se ostvaruje cilj zadatka.

Na kraju rješavanja zadatka, u **osvrtu**, provjerava se točnost dobivenog rješenja, promišlja o drugim načinima za rješavanje zadatka, ispituje postupak rješavanja zadatka i slično. Ova sastavnica je važna zato što svrha rješavanja zadatka nije samo pronaći rješenje, već o zadatku treba promisliti čime učenici razvijaju svoje matematičke sposobnosti i vještine.

Prema složenosti i težini, zadaci se dijele u dvije velike skupine: **standardni zadaci** i **nestandardni zadaci** ([6]).

Kod standardnih zadataka su sve sastavnice poznate. Kod takvih zadataka uvjeti su precizno i jasno postavljeni, cilj i potrebna teorijska osnova za rješavanje zadatka lako je uočljiva te je postupak rješavanja zadatka otprije poznat i teče glatko. Oni služe kao sredstvo boljeg razumijevanja i bržeg usvajanja novih matematičkih sadržaja, ali ne doprinose razvoju kreativnih sposobnosti učenika. Hoće li učenici uspjeti riješiti takav zadatak ovisi o tome koliko su spretni u primjeni određene tehnike, ali ne moraju razmišljati koju tehniku trebaju primijeniti.

S druge strane, kod nestandardnih zadataka barem jedna sastavnica zadatka je nepoznata. Rješavajući nestandardne zadatke, učenici razvijaju logičko mišljenje, kreativnost, samostalnost i dosjetljivost. Ukoliko nisu poznate dvije ili više sastavnica zadatka, tada govorimo o **problemskim zadacima**. Učenici se rjeđe susreću s problemskim zadacima na nastavi matematike, no vrlo često se zadaju na natjecanjima iz matematike. Kod problemskih zadataka metoda rješavanja nije unaprijed poznata te često postoji više načina za njihovo rješavanje. Za rješavanje problemskog zadatka na više načina, učeniku je potrebna veća količina prethodno stečenog znanja, a učenikovo se znanje produbljuje i proširuje novim znanjima te se povećava njegova aktivnost i interes za matematiku ([11]).

Sljedeći zadatak je primjer standardnog zadatka.

Zadatak 1. *Izračunajte* 8694^3 *bez primjene džepnog računala.*

Ovdje učenici znaju kako postupiti, trebaju samo pažljivo množiti.

Idući zadatak nam pokazuje kako nas rješavanje standardnog zadatka navodi na promišljanje te traženje kraćeg i jednostavnijeg rješenja.

Zadatak 2. *Izračunajte*

$$\frac{1}{2}+\frac{1}{6}+\frac{1}{12}+\cdots+\frac{1}{9900}.$$

Na prvi pogled, ovo je još jedan primjer standardnog zadatka u kojem moramo pažljivo zbrojiti razlomke. No, to će biti dugotrajan i zahtjevan proces u kojem učenici mogu lako pogriješiti. Ukoliko zadane razlomke zapišemo u sljedećem obliku

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{99\cdot 100},$$

možemo uočiti da prvih nekoliko razlomaka možemo zapisati kao

$$\begin{aligned}\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}&=\frac{2}{3},\\ \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}&=\frac{3}{4},\\ \frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\frac{1}{4\cdot 5}&=\frac{4}{5}.\end{aligned}$$

Dakle, možemo pretpostaviti da za sve pozitivne cijele brojeve n vrijedi

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}.$$

Sada tu tvrdnju treba još dokazati. Ukoliko su se učenici već susreli s takvim zadacima, znaju da se tvrdnja dokazuje pomoću metode matematičke indukcije, no ako nisu, moraju isprobavati više strategija i trebat će im više vremena da bi otkrili pravi način dokazivanja.

Prema cilju, zadaci se dijele na odredbene i dokazne. Cilj **odredbenog zadatka** je pronaći nepoznatu veličinu, odnosno objekt, a cilj **dokaznog zadatka** je pokazati istinitost neke postavljene tvrdnje ([6]). Dakle, prethodni primjer je primjer odredbenog zadatka koji smo pretvorili u dokazni da bi olakšali rješavanje zadatka. Učenici često mogu naslutiti ili pogoditi odgovor u nekom zadatku, no njihovo rješenje nije potpuno dok ga ne mogu dokazati. Neke zadatke je teško dokazati, pogotovo učenicima, no bitno je da ih potičemo na promišljanje i dokazivanje tvrdnji jer je to ono što matematiku izdvaja od drugih disciplina.

Kako bi učenici bili uspješniji u rješavanju problemskih zadataka, bitno je da poznaju metode rješavanja. Poznavanjem većeg broja metoda, veća je šansa da će učenik brže i lakše znati riješiti problemski zadatak. Kurnik, u djelu *Posebne metode rješavanja matematičkih problema* ([11]), nabraja i opisuje neke od metoda rješavanja matematičkih problema.

1.2 Problemska nastava

Jedno od najvažnijih pitanja suvremene metodike nastave matematike je pitanje razvoja stvaralačkog mišljenja i sposobnosti učenika te priprema učenika za rješavanje problema u daljnjem životu. Odgovor na ovo pitanje nastavnik matematike nalazi u samim načelima nastave matematike, nastavnim i znanstvenim metodama koje se primjenjuju u nastavnom procesu te u nastavnim sustavima ([7]). Sva načela, nastavne metode i nastavni sustavi usko su povezani i dio suvremene nastave matematike. Nastavni sustav, **problemska nastava**, posebno je važan za rješavanje ovog pitanja i za ostvarenje jednog od odgojno-obrazovnih ciljeva poučavanja matematike, **rješavanje problema i problemskih situacija**.

Učenje putem rješavanja problema osnovna je ideja problemske nastave. Da bi nastavnik obradio neki problem na nastavi matematike, najprije treba zainteresirati učenike za njegovo rješavanje stvaranjem problemske situacije. Stvorena problemska situacija učeniku treba biti primjerena s obzirom na dob, psihički razvoj i stvarne matematičke sposobnosti učenika. Nastavnik može stvoriti problemsku situaciju na nekoliko načina ([7]):

1. Nastavnik jasno i precizno postavlja probleme učenicima.

2. Nastavnik stvara situaciju u kojoj se od učenika zahtijeva da sami shvate i formuliraju problem koji se u toj situaciji nalazi.

3. Nastavnik stvara situaciju s više ili manje jasno naznačenim problemom koji tijekom analize treba učenike dovesti do novog problema koji je on predvidio.

4. Nastavnik stvara situaciju s više ili manje jasno naznačenim problemom koji tijekom analize učenike dovodi do novog problema koji on nije u potpunosti predvidio.

Najjednostavniji način je prvi jer je jasno iskazan problem, a u ostalim načinima ima više nepoznanica i od učenika se traži veća angažiranost. U posljednjem načinu nastavnik mora biti pripravan na nepredviđene učeničke pretpostavke, a učenici moraju biti posebno kreativni kako bi riješili danu problemsku situaciju. Unatoč tome, problemska nastava ima puno prednosti: učenici grade svoje znanje i vještine pomoću vlastitog iskustva, veća motiviranost učenika, primjerena mogućnost grupnog rada, istraživački pristup rješavanja problema, razvoj kritičkog mišljenja, bolje shvaćanje biti i zakonitosti, povećanje količine znanja, trajnost stečenog znanja, veća primjenjivost stečenih znanja.

Kada nastavnik uspješno stvori problemsku situaciju i zainteresira učenike za njezino rješavanje, učenici moraju aktivno i samostalno raditi, pravilno izabrati izvore za proučavanje, izdvojiti potrebne teorijske činjenice, misaono ih razraditi, postaviti i provjeriti hipoteze te jezično oblikovati i zapisati rezultate svoga rada kako bi uspješno riješili problemsku situaciju. Nastavnik ih u ovom nastavnom sustavu savjetuje i pomaže pri izboru izvora, ukazuje na potrebne teorijske činjenice, raspravlja s učenikom o dobivenim rezultatima te pripomaže učenicima postavljujući pitanja ukoliko naiđu na poteškoće. Takav način nastave matematike zahtjevan je i za učenika i za nastavnika.

S obzirom na sve navedeno, metodika nastave matematike razradila je shemu prema kojoj se oblikuje i priprema nastavni sat u problemskoj nastavi ([7]):

1. Stvaranje nastavne problemske situacije
2. Postavljanje problema koji niče iz dane problemske situacije
3. Proučavanje uvjeta
4. Rješavanje postavljenog problema
5. Razmatranje dobivenog rješenja i iskazivanje novog znanja
6. Proučavanje dobivenog rješenja i traženje drugih načina rješavanja
7. Proučavanje mogućih proširenja i poopćenja postavljenog problema
8. Zaključci izvršenog rada

Nastavnici mogu korisiti ovu shemu kako bi pripremili nastavni sat, no moraju imati na umu da je svaki problem jedinstven i ne može se svim problemima pristupiti na ovaj način pa će morati prilagoditi shemu.

S obzirom na složenost i težinu, za primjenu problemske nastave potrebno je više vremena i dobra priprema nastavnika. Zato nije primjenjiva na sve matematičke sadržaje, već nastavnik mora odabrati primjerene one matematičke sadržaje koji su primjereni za ovaj oblik nastave. Za preostale nastavne sadržaje učenicima može postaviti problemske zadatke kako bi postupno uveo problemsku nastavu u nastavu matematike. Jedan takav problemski zadatak dan je u sljedećem pitanju ([7]).

"Ako je opseg pravokutnika zadan, što možete reći o njegovoj površini?"

Nastavnik može stvoriti sljedeću problemsku situaciju da bi učenici odgovorili na prethodno pitanje. *Promotrite pravokutnike zadanog opsega O s različitim duljinama stranica. Ispitajte kako površina takvih pravokutnika ovisi o opsegu O.*

Nakon što je stvorio problemsku situaciju, nastavnik očekuje da će učenici krenuti s promatranjem konkretnog slučaja pravokutnika. Na primjer, neka je zadan pravokutnik opsega $O = 10$. U sljedećoj tablici dano je nekoliko mogućih duljina stranica a, b pravokutnika i njihova površina P.

O	a	b	P
10	1	4	4
10	2	3	6
10	$\frac{3}{2}$	$\frac{7}{2}$	$\frac{21}{4}$
10	$\frac{4}{3}$	$\frac{11}{3}$	$\frac{44}{9}$
10	$\frac{5}{2}$	$\frac{5}{2}$	$\frac{25}{4}$

Ukoliko učenici sami ne odaberu pravokutnik s jednakim stranicama, odnosno kvadrat, nastavnik ih pitanjima navodi da promotre i kvadrat. Ako pogledamo posljednji stupac u tablici vidimo da je površina pravokutnika najveća kada su stranice jednake, odnosno kada je kvadrat. To je za učenike važan trenutak, trenutak "otkrića". Dakle, otkrili su da bi mogla vrijediti sljedeća tvrdnja: *"Od svih pravokutnika zadanog opsega najveću površinu ima kvadrat."* No, sada još tu tvrdnju trebaju dokazati. Postoji nekoliko načina: primjenom aritmetičko-geometrijske nejednakosti, modeliranjem problema kvadratnom funkcijom i traženjem njenog maksimuma te metodom razlikovanja slučaja. Mi ćemo ovdje navesti samo prvi način, primjenom aritmetičko-geometrijske nejednakosti.

Neka je zadan pravokutnik sa stranicama duljine a i b. Njegov opseg je jednak $O = 2(a + b)$, a površina $P = ab$. Duljina stranice kvadrata s istim opsegom kao pravokutnik jednaka je $\frac{O}{4}$, a njegova površina iznosi

$$P' = \left(\frac{O}{4}\right)^2 = \left(\frac{2(a+b)}{4}\right)^2 = \left(\frac{a+b}{2}\right)^2.$$

Želimo dokazati da je $P' \geq P$. Ukoliko promotrimo površine pravokutnika $P = ab$ i kvadrata $P' = \left(\frac{a+b}{2}\right)^2$, vidimo da nam je potrebna veza između aritmetičke sredine $\frac{a+b}{2}$ i geometrijske sredine ab, odnosno aritmetičko-geometrijska nejednakost $\frac{a+b}{2} \geq \sqrt{ab}$ koju ćemo dokazati kasnije u radu.

Primjenom aritmetičko-geometrijske nejednakosti dobivamo

$$\left(\frac{a+b}{2}\right)^2 \geq ab,$$
$$\left(\frac{O}{4}\right)^2 \geq P,$$
$$P' \geq P.$$

Ukoliko učenici imaju problema s početnom problemskom situacijom, nastavnik ju može pojednostaviti tako da odmah iskaže tvrdnju i nakon toga je na učenicima da ju samo dokažu. Može se dogoditi da se učenici, u procesu spoznaje, prisjete da pravokutnik i kvadrat u ravnini imaju svoje analogone kvadra i kocku u prostoru. Tada mogu sami stvoriti novu problemsku situaciju *"Promatrajte skup kvadara zadanog oplošja O koji imaju volumen V. Ispitajte odnos oplošja O i volumena V."*, odnosno konkretnu tvrdnju *"Od svih kvadara zadanog oplošja najveći volumen ima kocka."*.

1.3 George Pólya i Pólyini koraci

George Pólya je mađarsko-američki matematičar te pedagog i metodičar koji je živio i radio tijekom 20. stoljeća. Uz mnoge doprinose matematici na području kombinatorike i vjerojatnosti, teorije brojeva te kompleksne analize, njegov najveći doprinos je u području edukacije matematike, odnosno metodike nastave matematike. Pólya se zalagao za heuristički pristup učenja i smatrao da se poučavanje matematike temelji na rješavanju problema te da vještina rješavanja problema nije urođena, već nešto što se može naučiti i uvježbati. U svom djelu, *Kako ću riješiti matematički zadatak* ([14]), izlaže svoju metodu za univerzalno rješavanje matematičkog zadatka te rješavanje matematičkog zadatka dijeli u četiri faze:

1. Razumijevanje zadatka

2. Stvaranje plana

3. Izvršavanje plana

4. Osvrt

Iako smo redom naveli četiri faze, za neke zadatke možda neće biti jednostavno uzastopno prolaziti kroz njih kako bi ih riješili, već možemo preskočiti neku fazu te se kasnije vratiti na nju.

Kako bi učenici mogli riješiti matematički zadatak, najprije ga trebaju razumjeti i shvatiti što tekst zadatka govori. Učenik treba uočiti dijelove zadatka, tj. prepoznati što je u zadatku zadano, a što treba odrediti te koji su uvjeti. Zato je važno da učenici dobro pročitaju tekst zadatka, po potrebi i više puta, čak i za vrijeme rješavanja. Ukoliko učenici imaju poteškoća s razumijevanjem zadatka, nastavnik im može pomoći postavljanjem sljedećih pitanja: *Što je nepoznato? Što je zadano? Kako glasi uvjet?* S mlađim učenicima, potrebno je ponovno pročitati tekst zadatka te ih zamoliti da formuliraju zadatak svojim riječima. Nakon što su odgovorili na ova pitanja, učenici crtaju crtež ukoliko je potreban te na njemu ističu zadane i nepoznate podatke te uvode prikladne oznake ([14]).

U sljedećoj fazi rješavanja zadatka, učenici smišljaju plan kako riješiti dani matematički zadatak. Ovaj proces može biti dugotrajan i zahtjevan, a ovisi o učenikovom matematičkom znanju i vještinama te prethodno stečenom iskustvu. Kako bi učenici uspješno smislili plan za rješavanje zadatka, moraju se prisjetiti ranije riješenih zadataka ili dokazanih teorema vezanih uz dani zadatak. Nastavnik im u tome može pomoći postavljanjem sljedećih pitanja: *Znaš li neki slični zadatak? Promotri nepoznanicu! Nastoj se sjetiti nekog tebi poznatog zadatka koji sadrži istu ili sličnu nepoznanicu! Evo zadatka koji je sličan tvom, a već je riješen! Možeš li ga upotrijebiti? Možeš li zadatak drugačije izraziti?* Učenik može smisliti ili riješiti neki sličan zadatak kako bi lakše smislio plan rješavanja i u tome mu mogu pomoći neke od sljedećih metoda ([14]):

- **generalizacija**, tj. rješavanje općenitijeg zadatka, odnosno zadatka čiji je specijalni slučaj zadani zadatak

- **specijalizacija**, tj. rješavanje posebnog slučaja zadanog zadatka

- **analogija**, tj. rješavanje sličnog zadatka

Nakon što učenici smisle plan rješavanja zadatka, samo izvršenje plana je lako, pogotovo ako su ga smislili sami ili uz minimalnu pomoć nastavnika. Primjenom ranije stečenih tehnika i vještina za rješavanje zadatka učenici provode plan te moraju biti svjesni svakog koraka u rješavanju i u ispravnost istog. Dakle, bitno je da je svaki korak učeniku jasan te da ga kontrolira ([14]).

U većini slučajeva nakon što učenici riješe neki zadatak, prelaze na novi zadatak bez da se osvrnu na postupak ili provjere rješenje zadatka, što nije dobro. Zbog toga nikako ne smiju zanemariti posljednju fazu: *Osvrt*. U posljednjoj fazi, učenici provjeravaju svaki korak u rješenju zadatka, pronalaze pogreške ukoliko one postoje te se pitaju postoji li neki drugi način rješavanja zadatka koji je kraći ili jednostavniji. Isto tako, mogu se pitati može li se rješenje zadatka primijeniti na nekom sličnom zadatku ili u nekim specijalnim slučajevima . Time učvršćuju svoje znanje i razumijevanje problema ([14]).

1.4 Heuristička nastava

Uz problemsku nastavu, za razvijanje sposobnosti rješavanja problema, važna je i **heuristička nastava**. Iako je njena djelotvornost slabija od one problemske nastave, i dalje se ostvaruje većina ciljeva suvremene nastave matematike. Bitno je naglasiti da se heuristička nastava može, u potpunosti ili djelomično, primijeniti na svakom nastavnom satu matematike. U ovom je nastavnom sustavu aktivnost i samostalnost učenika smanjena, ali sposobnost umnog rada učenika razvija se putem nastavnikovog misaonog vođenja. Heuristička nastava nastala je iz potrebe da se uvođenjem samostalnog rada učenika prevlada predavačka nastava te time poboljša i sam nastavni proces. Nastala je početkom prvog desetljeća 20. stoljeća te se tijekom vremena razvijala i usavršavala ([9]).

Prema Kurniku ([9]), postoje smjernice za primjenu heurističke nastave:

- Zadržati prividnost igre. Uvažavati slobodu učenika. Podržavati privid njegovoga vlastitog otkrivanja matematičke istine. Izbjegavati zamorne vježbe pamćenja u početnom obrazovanju učenika jer to potiskuje njegove urođene osobine. Poučavati oslanjajući se na interes prema matematičkom sadržaju koji se proučava.
- Ne izlagati određeni dio matematike u potpuno gotovom obliku. Takvim se postupanjem dolazi u raskorak s osnovnim načelima nastave. Razvijati umni rad, a ne zahtjevati učenje napamet. Pridržavati se načela primjerenih teškoća.
- Razvijanje stvaralačkih sposobnosti učenika glavni je zadatak nastave matematike.
- Heuristička metoda je takva nastavna metoda u kojoj nastavnik ne priopćuje učenicima gotove činjenice i istine, nego ih navodi na samostalno otkrivanje odgovarajućih tvrdnji i pravila.
- Heuristička metoda sastoji se u tome da nastavnik pred razred postavlja problem, a onda pomoću odgovarajućih prikladnih pitanja vodi učenika do rješenja.

Osnovu za stjecaje znanja i sposobnosti u heurističkoj nastavi predstavljaju samostalni rad i aktivnost učenika, a nastavnik ih svojim poučavanjem misaono vodi do razumijevanja i shvaćanja matematičkog sadržaja. U ovom nastavnom sustavu izrazito je bitna komunikacija nastavnika i učenika, tj. **heuristički razgovor**. Nastavnik svojim pitanjima upućuje učenike da u izvorima nalaze činjenice na osnovu kojih nastavnikovim misaonim vođenjem dolaze do shvaćanja poopćenja, a slobodan razgovor i rasprava omogućuju učenicima postavljanje pitanja. No, heuristička nastava ima i određene mane: nemogućnost misaonog vođenja svih učenika zbog pomanjkanja vremena i različite brzine shvaćanja, nemogućnost neposredne komunikacije sa svim učenicima, komunikacija s povučenim učenicima je otežana i često izostaju njihova pitanja te nepotpuna povratna informacija o proučenom matematičkom sadržaju ([9]).

1.5 Heuristike

Odluke u svakodnevnom životu donosimo pomoću grubih procjena koje ne možemo nazvati *metodama*. Pomoću podataka i iskustva od prije, nastojimo odokativno procijeniti najbolje rješenje, npr. na putu do škole biramo najbrži put, najbrže prijevozno sredstvo, itd. **Heuristika** je postupak koji vodi prema otkriću ili ga potiče, tj. pomoću različitih heuristika pokušavamo pronaći metodu kojom možemo pronaći rješenje problema, pa tako i matematičkog. Heuristika je mlada znanstvena grana, a upravo ju je Pólya pokušao okarakterizirati kao posebnu granu spoznaje u nastavi matematike. Naziv potječe od Arhimedovog uzvika "HEUREKA!" (pronašao sam, otkrio sam) kada je otkrio zakon o uzgonu tijela uronjenog u tekućinu ([9]). Treba još naglasiti da se korištenjem heuristike ne osigurava ispravan način rješavanja zadatka, ali navodi učenike prema otkrivanju rješenja. Upravo u Pólyinoj drugoj fazi iz knjige *Kako ću riješiti matematički zadatak* ([14]) opisanoj u trećem potpoglavlju, koristimo razne heuristike kako bi pronašli odgovarajuću metodu za rješavanje matematičkog zadatka.

Neke od poznatih heuristika nabrojane su i opisane u ([12]) i ([14]):

1. **Traženje uzorka:** Provjeravamo pojavljuje li se u problemu neki uzorak. Ako se neki uzorak često pojavljuje, vrlo je vjerojatno da će se opet ponoviti. Poteškoća koja se može javiti u ovoj heuristici je pronaći uzorak, no jednom kada se pronađe uzorak, rješavanje problema je lako.

2. **Korištenje različitih reprezentacija (crtanje slike, korištenje tablice, fizički model, ...):** Kada je to moguće, bez obzira da li je zadatak geometrijski ili ne, poželjno je nacrtati sliku, graf ili organizirati podatke u tablicu. Time omogućavamo lakšu organizaciju podataka te brže i lakše uočavamo veze između danih podataka i dolazimo do rješenja zadatka.

3. **Rješavanje ekvivalentnog problema:** Ukoliko ne znamo riješiti neki problem, bitno je smisliti neki ekvivalentni problem u jednostavnijem obliku i i koji znamo riješiti, što nam može pomoći u rješavanju početnog problema.

4. **Izmjena problema:** Ako ne znamo riješiti problem, možemo ga izmijeniti u problem koji znamo riješiti, a čije rješenje podrazumijeva rješenje početnog problema.

5. **Odabiranje prikladnog matematičkog jezika:** Jedan od prvih koraka u rješavanju matematičkog problema je zapisivanje problema matematičkim jezikom i simbolima.

6. **Rastav na slučajeve:** Rastavljanjem problema na slučajeve rješavanje nekog težeg problema svodi se na rješavanje nekoliko jednostavnijih problema. ([11])

7. **Rješavanje unatrag:** Rješavanje problema unatrag izvodi se obrnutim kronološkim redom, tj. od posljednjeg izvršenog koraka prema prvom. Započinjemo postavljanjem cilja, tj. očekivanog rezultata ili rješenja problema. Nakon primjene heuristike, provjeravamo rješenje problema tako da krenemo od prvog prema završnom koraku.

8. **Dokaz kontradikcijom:** Dokaz kontradikcijom izvodimo tako da pretpostavimo suprotno od onog što je pretpostavljeno u problemu i raznim operacijama dolazimo do zaključka da je naša suprotna pretpostavka netočna, tj. da vrijedi dana pretpostavka.

9. **Specijalizacija:** Specijalizacija je prijelaz s razmatranja danog skupa objekata na odgovarajuće razmatranje njegova podskupa. Kod nekih problema jednostavnije je promatrati specijalni, lakši problem od početnog te nam rješavanje specijalnog problema pomaže u rješavanju početnog, općenitijeg problema. ([10])

10. **Generalizacija:** Generalizacija ili poopćavanje je prijelaz s razmatranja danog skupa objekata na odgovarajuće razmatranje njegova nadskupa. Osnova generalizacije je induktivni način zaključivanja, tj. zaključivanje od pojedinačnog prema općem. Kod nekih problema jednostavnije je rješavanje općenitijeg problema te rješenje općenitijeg problema primjenjujemo na početni, specijalni slučaj. ([10])

11. **Analiza i sinteza:** Analiza je znanstvena metoda istraživanja koja se zasniva na raščlanjivanju cjeline na dijelove, proučavanju dijelova i izvođenju zaključaka o cjelini na temelju dobivenih rezultata. Analizom problem svodimo na jednostavnije probleme i tvrdnje koje su ili očigledne ili se jednostavno dokazuju. Sinteza je znanstvena metoda istraživanja koja se zasniva na povezivanju proučenih dijelova u cjelinu koje rješava postavljeni problem. ([10])

12. **Metoda pokušaja i pogreške:** Metoda pokušaja i pogreške, tzv. metoda uzastopnih približavanja sastoji se od niza pokušaja da se dođe do rješenja postavljenog problema. U svakom pokušaju nastoji se ispraviti pogreška nastala u prethodnom pokušaju i pri tome se općenito pogreška smanjuje te se u svakom sljedećem pokušaju približava rješenju danog problema. ([11])

Poglavlje 2

Nejednakosti

Nejednakosti su korisne u gotovo svim područjima matematike, a problemi nejednakosti su među najljepšima. Među svim mogućim nejednakostima koje bismo mogli razmotriti, usredotočit ćemo se samo na dvije: nejednakosti između srednjih vrijednosti i Cauchy-Schwarzovu nejednakost. Osim toga, razmotrit ćemo različite algebarske i geometrijske tehnike te analitičke tehnike u rješavanju nejednakosti. Nejednakosti najčešće rješavamo algebarski ili geometrijski. Mnogi dokazi nejednakosti su kratki i sažeti te se iz njih može mnogo naučiti, no nisu napisani metodički te nedostaje objašnjenje i razrada strategije koja bi se mogla primijeniti u sličnim zadacima. Nabrojimo neke strategije koje možemo primijeniti u raznim dokazima nejednakosti ([4] i [8]):

1. Način dokazivanja je očigledan, prirodan i sam se nameće, pa odmah prelazimo na dokaz ili primjenom jednostavnih i posebnih nejednakosti koje se lako pamte.

2. Podsjeća li vas izraz na neku poznatu nejednakost? Primjenom poznatih nejednakosti možemo dokazati veliki broj nejednakosti.

3. Ako nejednakost treba dokazati za sve prirodne brojeve n veće od nekog broja n_0, najčešće korisitimo metodu matematičke indukcije.

4. Ako se u zadanoj nejednakosti pojavljuju stranice trokuta a, b, c pri analizi i dokazivanju moramo pripaziti na nejednakost trokuta $b + c > a, a + c > b, a + b > c$.

   Ako nejednakost trokuta zapišemo na sljedeći način $b + c - a > 0, a + c - b > 0, a + b - c > 0$, te uvedemo supstitucije $x = b + c - a, y = a + c - b, z = a + b - c$, tada je $x > 0, y > 0, z > 0$ i vrijedi

   $$a = \frac{y+z}{2}, \quad b = \frac{x+z}{2}, \quad c = \frac{x+y}{2}.$$

   Tako često pojednostavljujemo izračunavanje i dokazivanje tražene nejednakosti. Ovdje smo duljine stranica trokuta a, b, c, odnosno pozitivne realne brojeve za koje trebamo uzeti u obzir nejednakost trokuta, zamijenili s pozitivnim realnim brojevima x, y, z.

Ukoliko nijednu ovu strategiju ne možemo odmah primijeniti, možemo zadanu nejednakost pojednostaviti raznim transformacijama: množenje nejednakosti zajedničkim nazivnikom, prebacivanje članova na istu stranu, množenje zagrada, dodavanje i oduzimanje novih članova, množenje nejednakosti brojem različitim od 0, drugačije grupiranje članova, izlučivanje zajedničkih faktora, potenciranje ili supstitucija.

2.1 Nekoliko uvodnih primjera

Slijede zadaci u kojima primjenjujemo prethodno navedene strategije u točkama $1, 3$ i 4, dok ćemo strategiju iz točke 2 primijeniti u sljedećim potpoglavljima *Srednje vrijednosti* i *Cauchy-Schwarzova nejednakost*.

Zadatak 2.1.1. *Dokažite nejednakost*

$$\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\cdots\frac{999999}{1000000}<\frac{1}{1000}.$$

Rješenje:
Označimo s x lijevu stranu nejednakosti. Tada očito vrijedi

$$x=\frac{1}{2}\cdot\frac{3}{4}\cdot\frac{5}{6}\cdots\frac{999999}{1000000}<\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\cdots\frac{1000000}{1000001}.$$

Pogledajmo recipročnu vrijednost od x

$$\frac{1}{x}=\frac{2}{1}\cdot\frac{4}{3}\cdot\frac{6}{5}\cdots\frac{1000000}{999999},$$

i uočimo da je

$$\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\cdots\frac{1000000}{1000001}=\frac{1}{x}\cdot\frac{1}{1000001}$$

što nam daje

$$x<\frac{1}{x}\cdot\frac{1}{1000001}.$$

Očito vrijedi

$$x^2<\frac{1}{1000001}<\frac{1}{1000000},$$

pa korjenovanjem dobivamo traženu nejednakost.

Zadatak 2.1.2. *Neka je $n \in \mathbb{N}$. Dokažite da za sve realne brojeve $x_k \in \langle -1, \infty \rangle, k = 1, 2, \ldots, n$, koji su istog predznaka, vrijedi*

$$(1 + x_1)(1 + x_2) \cdots (1 + x_n) \geq 1 + x_1 + x_2 + \ldots + x_n,$$

pri čemu jednakost vrijedi ako i samo ako je $n = 1$.

Rješenje:
Za $n = 1$ očito je da vrijedi jednakost u gornjoj nejednakosti. Kako bi dokazali strogu nejednakost za $n \geq 2$ koristit ćemo metodu matematičke indukcije po n.
(**Baza**) Za $n = 2$ imamo

$$(1 + x_1)(1 + x_2) > 1 + x_1 + x_2,$$

tj. $1 + x_1 + x_2 + x_1 x_2 > 1 + x_1 + x_2$, što očito vrijedi.
(**Pretpostavka**) Pretpostavimo da za neki $n \in \mathbb{N}$ vrijedi nejednakost

$$(1 + x_1)(1 + x_2) \cdots (1 + x_n) > 1 + x_1 + x_2 + \ldots + x_n,$$

za sve $x_1, \ldots, x_n \in \langle -1, \infty \rangle$.
(**Korak**) Dokažimo sad da nejednakost vrijedi i za $n + 1$ brojeva $x_1, \ldots, x_{n+1} \in \langle -1, \infty \rangle$, tj. da vrijedi

$$(1 + x_1)(1 + x_2) \cdots (1 + x_n)(1 + x_{n+1}) > 1 + x_1 + x_2 + \ldots + x_n + x_{n+1}.$$

Na lijevu stranu nejednakosti primijenimo pretpostavku indukcije i dobivamo

$$\begin{aligned}
(1 + x_1)(1 + x_2) \cdots (1 + x_n)(1 + x_{n+1}) &> (1 + x_1 + x_2 + \ldots + x_n)(1 + x_{n+1}) \\
&= 1 + x_1 + x_2 + \ldots + x_n + x_{n+1} \\
&+ x_{n+1}(1 + x_1 + x_2 + \ldots + x_n) \\
&> 1 + x_1 + x_2 + \ldots + x_n + x_{n+1} + x_{n+1}
\end{aligned}$$

što vrijedi zbog uvjeta $x_i x_j > 0$ za $i, j = 1, \ldots, n$. Prema principu matematičke indukcije, slijedi tvrdnja.

Zadatak 2.1.3. *Neka je $n \in \mathbb{N}$ te $a_1, \ldots, a_n \in \mathbb{R}$ takvi da je $a_i \geq 1, i = 1, \ldots, n$. Dokažite da vrijedi*

$$(1 + a_1)(1 + a_2) \cdots (1 + a_n) \geq \frac{2^n}{n + 1}(1 + a_1 + a_2 + \ldots + a_n).$$

Rješenje:
Metoda matematičke indukcije je strategija koja se prirodno nameće, ali ako transformiramo lijevu stranu nejednakosti na sljedeći način

$$\begin{aligned}
(1 + a_1)(1 + a_2) \cdots (1 + a_n) &= 2^n \left(\frac{1}{2} + \frac{a_1}{2}\right)\left(\frac{1}{2} + \frac{a_2}{2}\right) \cdots \left(\frac{1}{2} + \frac{a_n}{2}\right) \\
&= 2^n \left(1 + \frac{a_1 - 1}{2}\right)\left(1 + \frac{a_2 - 1}{2}\right) \cdots \left(1 + \frac{a_n - 1}{2}\right),
\end{aligned}$$

onda možemo primijeniti prethodni zadatak. Tada imamo

$$(1+a_1)(1+a_2)\cdots(1+a_n) \geq 2^n \left(1 + \frac{a_1-1}{2} + \frac{a_2-1}{2} + \ldots + \frac{a_n-1}{2}\right).$$

Vidimo da nam je na desnoj strani zadane nejednakosti u nazivniku $n+1$ te da je

$$\begin{aligned} 1 + \frac{a_1-1}{2} + \frac{a_2-1}{2} + \ldots + \frac{a_n-1}{2} &\geq 1 + \frac{a_1-1}{n+1} + \frac{a_2-1}{n+1} + \ldots + \frac{a_n-1}{n+1} \\ &= \frac{1}{n+1}\left(1 + a_1 + a_2 + \ldots + a_n\right). \end{aligned}$$

Odavde slijedi tvrdnja.

Zadatak 2.1.4. *Neka su* $a, b, c \in [0, 1]$. *Pokažite da je*

$$\frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c) \leq 1.$$

Rješenje:

Prvi pokušaj rješavanja ovog zadatka je vjerojatno svođenje na zajednički nazivnik i nada da će se izraz pojednostaviti. Međutim, dobit ćemo prilično kompliciran izraz. Pokušajmo drugačije. Prvo, zbog simetričnosti izraza s obzirom na a, b, c, bez smanjenja općenitosti možemo pretpostaviti da je $0 \leq a \leq b \leq c \leq 1$. Sada zbog, $b+c+1 \leq a+b+1$ i $c+a+1 \leq a+b+1$, slijedi

$$\frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} \leq \frac{a+b+c}{a+b+1},$$

pa je dovoljno dokazati da vrijedi

$$\frac{a+b+c}{a+b+1} + (1-a)(1-b)(1-c) \leq 1.$$

Kako bismo pribrojnike slijeva "spojili", uočimo da vrijedi

$$\frac{a+b+c}{a+b+1} = \frac{a+b+1}{a+b+1} + \frac{c-1}{a+b+1} = 1 + \frac{c-1}{a+b+1},$$

pa lijevu stranu gornje nejednakosti možemo zapisati kao

$$\frac{a+b+c}{a+b+1} + (1-a)(1-b)(1-c) = 1 - \frac{1-c}{a+b+1} + (1-a)(1-b)(1-c).$$

Sada, ako izlučimo $\frac{1-c}{a+b+1}$ iz posljednja dva pribrojnika, dobivamo

$$\frac{a+b+c}{a+b+1} + (1-a)(1-b)(1-c) = 1 - \frac{(1-c)}{a+b+1}\left(1 - (1+a+b)(1-a)(1-b)\right).$$

Zbog $0 \leq a, b, c \leq 1$ vrijedi sljedeće

$$\begin{aligned}(1+a+b)(1-a)(1-b) &\leq (1+a+b+ab)(1-a)(1-b)\\ &= (1+a)(1+b)(1-a)(1-b)\\ &= (1-a^2)(1-b^2)\\ &\leq 1,\end{aligned}$$

pa vrijedi i tražena nejednakost.

Zadatak 2.1.5. *Ako su a, b, c duljine stranica trokuta, dokažite da je*

$$a^2 + b^2 + c^2 < 2(ab + ac + bc).$$

Rješenje:
Kao što smo objasnili na početku ovog poglavlja u točki 4, uvođenjem susptitucija $x = b + c - a, y = a + c - b, z = a + b - c$, vrijedi

$$a = \frac{y+z}{2}, \quad b = \frac{x+z}{2}, \quad c = \frac{x+y}{2}.$$

Zbog nejednakosti trokuta još je $x > 0, y > 0, z > 0$. Tada se zadatak svodi na provjeru da vrijedi

$$\left(\frac{y+z}{2}\right)^2 + \left(\frac{x+z}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 < 2\left(\frac{y+z}{2} \cdot \frac{x+z}{2} + \frac{y+z}{2} \cdot \frac{x+y}{2} + \frac{x+z}{2} \cdot \frac{x+y}{2}\right).$$

Raspisivanjem gornje nejednakosti dobivamo

$$\frac{2(x^2 + y^2 + z^2 + xy + yz + xz)}{4} < \frac{2}{4}\left(x^2 + y^2 + z^2 + 3(xy + yz + xz)\right),$$

tj. $2(xy + yz + xz) > 0$, što očito vrijedi jer su x, y, z pozitivni realni brojevi.

2.2 Srednje vrijednosti

Definicija 2.2.1. *Neka je $a = (a_1, \ldots, a_n)$ n-torka pozitivnih realnih brojeva.*

Aritmetička sredina *$A_n(a)$ brojeva $a_1, \ldots, a_n$ je broj*

$$A_n(a) = \frac{a_1 + \ldots + a_n}{n},$$

geometrijska sredina *$G_n(a)$ brojeva $a_1, \ldots, a_n$ je broj*

$$G_n(a) = \sqrt[n]{a_1 \cdots a_n},$$

kvadratna sredina *$K_n(a)$ brojeva $a_1, \ldots, a_n$ je broj*

$$K_n(a) = \sqrt{\frac{a_1^2 + \ldots + a_n^2}{n}},$$

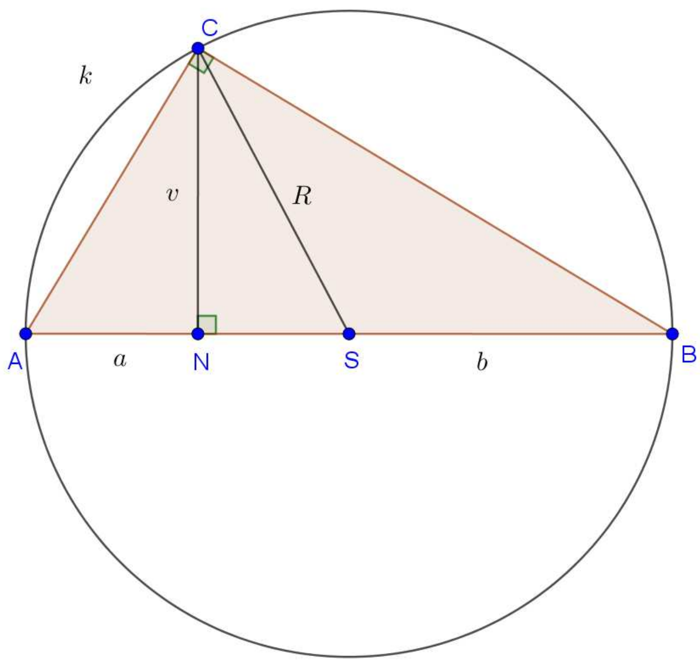
harmonijska sredina *$H_n(a)$ brojeva $a_1, \ldots, a_n$ je broj*

$$H_n(a) = \frac{n}{\frac{1}{a_1} + \ldots + \frac{1}{a_n}}.$$

Sada ćemo dokazati neke veze između navedenih srednjih vrijednosti. Da bi nam bilo jednostavnije i kraće za pisati, uvedimo kratice:

- AG nejednakost - nejednakost između aritmetičke i geometrijske sredine
- AH nejednakost - nejednakost između aritmetičke i harmonijske sredine
- AK nejednakost - nejednakost između aritmetičke i kvadratne sredine
- GH nejednakost - nejednakost između geometrijske i harmonijske sredine

Dokažimo AG nejednakost za $n = 2$ geometrijski ([3]).



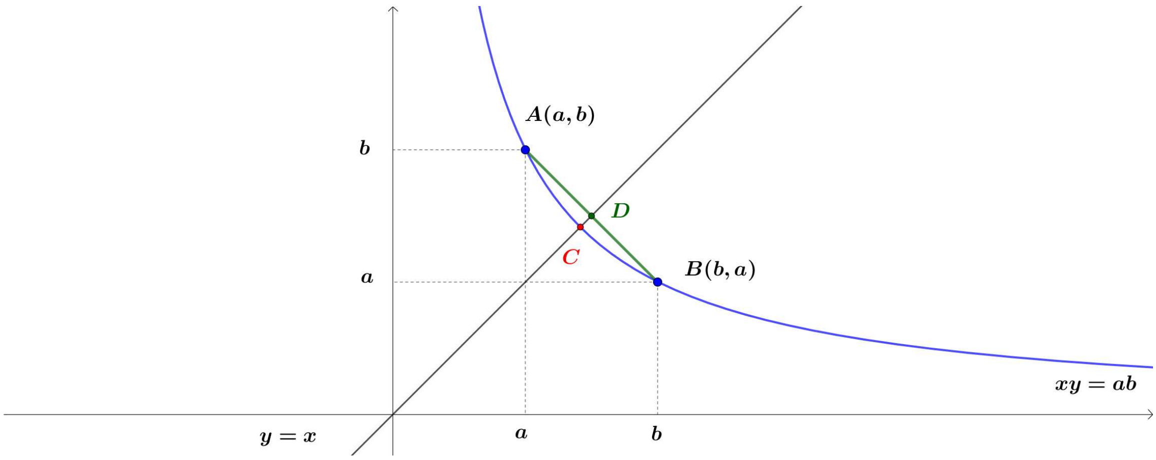
Slika 2.1: Pravokutan trokut *ABC*

Neka su $a, b > 0$. Nacrtajmo pravokutni trokut ABC s hipotenuzom AB duljine $a + b$, te kojem visina CN dijeli hipotenuzu na odsječke kao na slici 2.1.

Prema Euklidovom poučku, duljina visine v na hipotenuzu jednaka je geometrijskoj sredini njenih duljina odsječaka na hipotenuzi, tj. vrijedi $v = \sqrt{ab}$. S druge strane, polumjer kružnice opisane pravokutnom trokutu ABC jednak je polovini duljine hipotenuze, tj. vrijedi $R = \frac{a+b}{2}$. Budući da je u pravokutnom trokutu CNS hipotenuza R dulja od katete v, slijedi $\frac{a+b}{2} \geq \sqrt{ab}$, tj. vrijedi AG nejednakost. Jednakost se postiže ako i samo ako su odsječci visine na hipotenuzi jednake duljine. Zaista, da bi odsječci na hipotenuzi bili jednake duljine, radijus R opisane kružnice trokutu ABC mora se podudarati s visinom v, a to vrijedi ako i samo ako je trokut ABC jednakokračan, tj. ako i samo ako je $a = b$.

Dokažimo AG nejednakost za $n = 2$ analitički ([3]).

Skicirajmo hiperbolu $xy = ab$ u koordinatnom sustavu kao na slici 2.2. Točke $A\,(a, b)$ i



Slika 2.2: Grana hiperbole $xy = ab$

$B\,(b, a)$ pripadaju toj hiperboli. Pravac koji prolazi kroz točke A i B ima jednadžbu

$$y = -x + a + b.$$

Skicirajmo pravac $y = x$ u istom koordinatnom sustavu. Presjek hiperbole i pravca $y = x$ je točka C čije su koordinate $C\left(\sqrt{ab}, \sqrt{ab}\right)$, a presjek tetive AB i pravca $y = x$ je točka D s koordinatama $D\left(\frac{a+b}{2}, \frac{a+b}{2}\right)$. Zbog konveksnosti funkcije $f(x) = \frac{ab}{x}$, $x \in \langle 0, \infty \rangle$ graf funkcije između dviju točaka na grafu je ispod tetive koja spaja te dvije točke. Kako se točka C nalazi na hiperboli, a točka D na tetivi, zbog konveksnosti slijedi da je ordinata točke C manja ili jednaka od ordinate točke D.

Konačno, u sljedećim teoremima dokazat ćemo prethodno navedene nejednakosti za $n \in \mathbb{N}$.

Teorem 2.2.2 (AG nejednakost). *Neka je $a = (a_1, \ldots, a_n)$ n-torka pozitivnih realnih brojeva. Tada je*

$$A_n(a) = \frac{a_1 + \ldots + a_n}{n} \geq \sqrt[n]{a_1 \cdots a_n} = G_n(a), \tag{2.1}$$

pri čemu jednakost vrijedi ako i samo ako je $a_1 = \ldots = a_n$.

Dokaz. Označimo s A aritmetičku, a s G geometrijsku sredinu n pozitivnih realnih brojeva $a_1, \ldots, a_n$, dakle imamo

$$A = \frac{a_1 + \ldots + a_n}{n}, \quad G = \sqrt[n]{a_1 \cdots a_n}.$$

Dokaz provodimo metodom matematičke indukcije po n.

(**Baza**) Za $n = 2$ nejednakost (2.1) postaje

$$\frac{a_1 + a_2}{2} \geq \sqrt{a_1 a_2}, \tag{2.2}$$

što je ekvivalentno s

$$a_1 + a_2 - 2\sqrt{a_1 a_2} \geq 0,$$

odnosno

$$\left(\sqrt{a_1} - \sqrt{a_2}\right)^2 \geq 0.$$

Posljednja nejednakost očito vrijedi, a jednakost će vrijediti ako i samo ako je $a_1 = a_2$.

(**Pretpostavka**) Pretpostavimo da tvrdnja vrijedi za svakih $n - 1$ pozitivnih brojeva.

(**Korak**) Dokažimo nejednakost (2.1) za n-torku $a = (a_1, \ldots, a_n)$. Bez smanjenja općenitosti možemo pretpostaviti da je $a_1 \leq a_2 \leq \ldots \leq a_n$. Očito je

$$a_1 = \frac{\overbrace{a_1 + a_1 + \ldots + a_1}^{n\ pribrojnika}}{n} \leq A \leq \frac{\overbrace{a_n + a_n + \ldots + a_n}^{n\ pribrojnika}}{n} = a_n \tag{2.3}$$

Promotrimo sljedećih $n - 1$ brojeva: $a_2, a_3, \ldots, a_{n-1}, (a_1 + a_n - A)$. Iz nejednakosti (2.3) očito vrijedi

$$a_1 + a_n - A \geq 0,$$

pa na ovu $(n - 1)$-torku možemo primijeniti pretpostavku indukcije. Dobivamo

$$\left(\frac{a_2 + a_3 + \ldots + a_{n-1} + (a_1 + a_n - A)}{n - 1}\right)^{n-1} \geq a_2 a_3 \cdots a_{n-1}(a_1 + a_n - A).$$

Kako je

$$\begin{aligned} \frac{a_2 + a_3 + \ldots + a_{n-1} + (a_1 + a_n - A)}{n - 1} &= \frac{a_1 + a_2 + a_3 + \ldots + a_{n-1} + a_n - A}{n - 1} \\ &= \frac{nA - A}{n - 1} = A, \end{aligned}$$

slijedi da je

$$A^{n-1} \geq a_2 a_3 \cdots a_{n-1}(a_1 + a_n - A),$$

pa množenjem gornje nejednakosti s A dobivamo

$$A^n \geq A \cdot a_2 a_3 \cdots a_{n-1}(a_1 + a_n - A).$$

Sada želimo pokazati da je

$$A \cdot a_2 a_3 \cdots a_{n-1}(a_1 + a_n - A) \geq a_1 a_2 \cdots a_n = G^n.$$

Očito je dovoljno dokazati da je

$$A(a_1 + a_n - A) \geq a_1 a_n.$$

Lako vidimo da je ovaj izraz ekvivalentan s

$$(A - a_1)(a_n - A) \geq 0, \tag{2.4}$$

što je ispunjeno zbog (2.3). Prema principu matematičke indukcije, tvrdnja vrijedi za svaki prirodan broj n.

Pokažimo još da jednakost vrijedi ako i samo ako je $a_1 = \ldots = a_n$. Ako je $a_1 = \ldots = a_n$ tada jednakost očito vrijedi, pa pretpostavimo da brojevi $a_1, a_2, \ldots, a_n$ nisu svi međusobno jednaki, tj. da su barem dva broja različita. Na primjer, pretpostavimo da je $a_1 \neq a_2$. Tada je

$$\begin{aligned}
\frac{a_1 + a_2 + \ldots + a_n}{n} &= \frac{\frac{a_1+a_2}{2} + \frac{a_1+a_2}{2} + a_3 + \ldots + a_n}{n} \\
&\geq \left[\left(\frac{a_1 + a_2}{2}\right)^2 a_3 \cdots a_n\right]^{1/n} \\
&> (a_1 a_2 \cdots a_n)^{1/n},
\end{aligned}$$

jer za $a_1 \neq a_2$ imamo $\left(\sqrt{a_1} - \sqrt{a_2}\right)^2 > 0$, to jest $\frac{a_1+a_2}{2} > \sqrt{a_1 a_2}$. Dakle, jednakost u (2.1) vrijedi ako i samo ako je $a_1 = \ldots = a_n$. □

Teorem 2.2.3 (GH nejednakost). *Neka je $a = (a_1, \ldots, a_n)$ n-torka pozitivnih realnih brojeva. Tada je*

$$G_n(a) = \sqrt[n]{a_1 \cdots a_n} \geq \frac{n}{\frac{1}{a_1} + \ldots + \frac{1}{a_n}} = H_n(a), \tag{2.5}$$

pri čemu jednakost vrijedi ako i samo ako je $a_1 = \ldots = a_n$.

Dokaz. Ako primijenimo AG nejednakost na brojeve $\frac{1}{a_1}, \frac{1}{a_2}, \ldots, \frac{1}{a_n}$ dobivamo

$$\frac{\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}}{n} \geq \sqrt[n]{\frac{1}{a_1} \cdot \frac{1}{a_2} \cdots \frac{1}{a_n}} \tag{2.6}$$

Zapišimo (2.6) kao

$$\frac{\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}}{n} \geq \sqrt[n]{(a_1 \cdot a_2 \cdots a_n)^{-1}},$$

a ta nejednakost ekvivalentna je s

$$\left(\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}} \right)^{-1} \geq (a_1 \cdot a_2 \cdots a_n)^{-1/n},$$

odnosno

$$(a_1 \cdot a_2 \cdots a_n)^{1/n} \leq \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_n}},$$

a to je upravo (2.5). Znamo da jednakost u (2.6) vrijedi ako i samo ako je $\frac{1}{a_1} = \frac{1}{a_2} = \ldots = \frac{1}{a_n}$, tj. $a_1 = a_2 = \ldots = a_n$. □

Teorem 2.2.4 (AK nejednakost). *Neka je $a = (a_1, \ldots, a_n)$ n-torka pozitivnih realnih brojeva. Tada je*

$$A_n(a) = \frac{a_1 + \ldots + a_n}{n} \leq \sqrt{\frac{a_1^2 + \ldots + a_n^2}{n}} = K_n(a), \tag{2.7}$$

pri čemu jednakost vrijedi ako i samo ako je $a_1 = \ldots = a_n$.

Dokaz. Teorem dokazujemo pomoću jednakosti

$$(a_1 + a_2 + \ldots + a_n)^2 = a_1^2 + a_2^2 + \ldots + a_n^2 + 2a_1a_2 + 2a_1a_3 + \ldots + 2a_{n-1}a_n.$$

Znamo da je

$$a_i^2 + a_j^2 \geq 2a_ia_j, \qquad \forall a_i, a_j \in \mathbb{R},$$

što slijedi iz $(a_i - a_j)^2 \geq 0$ i jednakost se postiže ako i samo ako je $a_i = a_j$, pa ako zamijenimo $2a_ia_j$ s $a_i^2 + a_j^2, i, j = 1, \ldots, n, i \neq j$, dobivamo

$$(a_1 + a_2 + \ldots + a_n)^2 \leq a_1^2 + a_2^2 + \ldots + a_n^2 + (a_1^2 + a_2^2) + (a_1^2 + a_3^2) + \ldots + (a_{n-1}^2 + a_n^2),$$

tj.

$$(a_1 + a_2 + \ldots + a_n)^2 \leq n(a_1^2 + a_2^2 + \ldots + a_n^2). \tag{2.8}$$

Kako su izrazi na obje strane u (2.8) pozitivni, nejednakost možemo korjenovati te dobivamo

$$a_1 + a_2 + \ldots + a_n \leq \sqrt{n(a_1^2 + a_2^2 + \ldots + a_n^2)},$$

a dijeljenjem s n konačno dobivamo (2.7). Kako jednakost u (2.8) vrijedi ako i samo ako je $a_1 = \ldots = a_n$, onda i jednakost u (2.7) vrijedi ako i samo ako je $a_1 = \ldots = a_n$. □

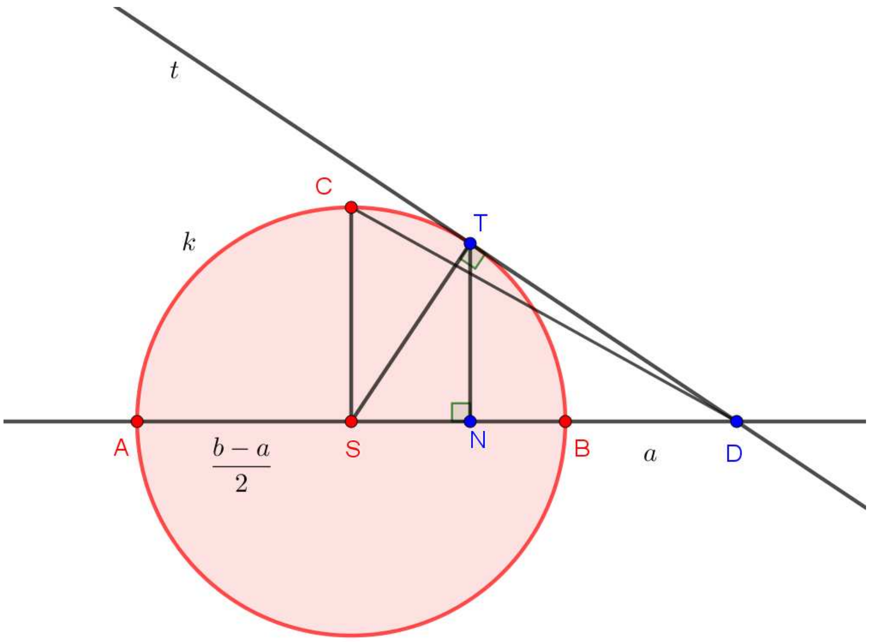
Konačno, iz prethodno navedenih teorema slijedi

Korolar 2.2.5 (**Nejednakosti između osnovnih sredina**)**.** *Neka je $a = (a_1, \ldots, a_n)$ n-torka pozitivnih realnih brojeva. Tada vrijedi*

$$H_n(a) \leq G_n(a) \leq A_n(a) \leq K_n(a). \tag{2.9}$$

Dokažimo ove nejednakosti za $n = 2$ i na geometrijski način ([5]).

Neka su a, b pozitivni realni brojevi takvi da je $a < b$. Neka je k kružnica promjera $|AB| = b - a$, S njeno središte, te D točka koja se nalazi na pravcu AB tako da je $|AD| = b$ (slika 2.3).



Slika 2.3: Nejednakosti između osnovnih sredina

Očito vrijedi $|BD| = a$. Iz točke D povucimo tangentu t na kružnicu k. Neka je T diralište tangente i kružnice. Promotrimo pravokutni trokut STD. Dužina $\overline{SD}$ mu je hipotenuza i ima duljinu

$$|SD| = |SB| + |BD| = \frac{b-a}{2} + a = \frac{a+b}{2},$$

a duljinu katete $\overline{TD}$ izračunamo pomoću Pitagorinog poučka

$$|TD| = \sqrt{|SD|^2 - |ST|^2} = \sqrt{\left(\frac{a+b}{2}\right)^2 - \left(\frac{b-a}{2}\right)^2} = \sqrt{ab}.$$

Kako je hipotenuza dulja od katete, slijedi

$$|TD| = \sqrt{ab} \leq \frac{a+b}{2} = |SD|.$$

Promotrimo sada pravokutni trokut SCD, gdje je točka C presjek kružnice i polumjera iz središta S okomitog na promjer AB. Hipotenuza $\overline{CD}$ ima duljinu

$$|CD| = \sqrt{\left(\frac{b-a}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2} = \sqrt{\frac{a^2+b^2}{2}}.$$

Kako je hipotenuza dulja od katete, slijedi

$$|SD| = \frac{a+b}{2} \leq \sqrt{\frac{a^2+b^2}{2}} = |CD|.$$

Na kraju, ako je točka N nožište visine iz vrha T u pravokutnom trokutu STD, tada iz sličnosti trokuta TDN i STD, slijedi $|ND| : |ST| = |TD| : |SD|$, tj.

$$|ND| = \frac{2ab}{a+b} = \frac{2}{\frac{1}{a} + \frac{1}{b}}.$$

Kako je hipotenuza dulja od katete u pravokutnom trokut TND, slijedi

$$|ND| = \frac{2}{\frac{1}{a} + \frac{1}{b}} \leq \sqrt{ab} = |TD|.$$

Dakle, pokazali smo da vrijedi

$$\frac{2}{\frac{1}{a} + \frac{1}{b}} \leq \sqrt{ab} \leq \frac{a+b}{2} \leq \sqrt{\frac{a^2+b^2}{2}},$$

tj. $H_2(a) \leq G_2(a) \leq A_2(a) \leq K_2(a)$.

Sada navodimo nekoliko zadataka u kojima primjenjujemo dokazane nejednakosti. U potpoglavlju Cauchy-Schwarzova nejednakost također se nalaze takvi zadaci.

Zadatak 2.2.6. *Ako su a, b, c pozitivni brojevi takvi da vrijedi $(1 + a)(1 + b)(1 + c) = 8$, dokažite da vrijedi $abc \leq 1$.*

Rješenje:
U ovom zadatku nejednakost je jednostavna, a uvjet je složen. Zato trebamo krenuti od transformacija uvjeta i pokušati dobiti umnožak abc. Raspišimo lijevu stranu uvjeta i grupirajmo pribrojnike na sljedeći način

$$(1 + a)(1 + b)(1 + c) = 1 + (a + b + c) + (ab + bc + ca) + abc.$$

Ako primjenimo AG nejednakost redom na a, b, c i na ab, bc, ca, dobivamo

$$\frac{a + b + c}{3} \geq (abc)^{\frac{1}{3}}$$

i

$$\frac{ab + bc + ca}{3} \geq (abc)^{\frac{2}{3}},$$

pri čemu jednakost vrijedi ako i samo ako je $a = b = c$. Sada slijedi,

$$8 = 1 + (a + b + c) + (ab + bc + ca) + abc \geq 1 + 3(abc)^{\frac{1}{3}} + 3(abc)^{\frac{2}{3}} + abc,$$

tj. $1 + 3(abc)^{\frac{1}{3}} + 3(abc)^{\frac{2}{3}} + abc \leq 8$. Uočimo da lijevu stranu nejednakosti možemo zapisati kao kub zbroja brojeva 1 i $(abc)^{\frac{1}{3}}$ pa dobivamo

$$\left[1 + (abc)^{\frac{1}{3}}\right]^3 \leq 8.$$

Sada, kornjenovanjem dobivamo $1 + (abc)^{\frac{1}{3}} \leq 2$, tj. $(abc)^{\frac{1}{3}} \leq 1$, pa vrijedi i zadana nejednakost.

Pronalaženje ekstremnih vrijednosti funkcija najčešće se rješava pomoću derivacija, ali u nekim problemima njihovo pronalaženje je brže primjenom AG nejednakosti. Sada ćemo dokazati tvrdnju navedenu u potpoglavlju 1.2 ovog rada.

Zadatak 2.2.7. *Dokažite da je kocka kvadar s najvećim volumenom uz zadano oplošje, te minimalnim oplošjem uz zadani volumen.*

Rješenje:
Neka su $a, b, c > 0$ duljine bridova kvadra. Tada je volumen kvadra $V = abc$, a njegovo oplošje $O = 2(ab + bc + ca)$. Ako izraz za volumen napišemo u obliku

$$V^2 = a^2b^2c^2 = (ab)(bc)(ca),$$

možemo primijeniti AG nejednakost i tako dobivamo

$$V^2 = (ab)(bc)(ca) \leq \left(\frac{ab + bc + ca}{3}\right)^3 .$$

Primijetimo da je

$$\left(\frac{ab + bc + ca}{3}\right)^3 = \left(\frac{2(ab + bc + ca)}{6}\right)^3 = \left(\frac{O}{6}\right)^3 ,$$

čime smo dobili relaciju između oplošja i volumena kvadra, tj. za sve $a, b, c > 0$ vrijedi

$$6V^{\frac{2}{3}} \leq O,$$

pri čemu jednakost vrijedi ako i samo ako je $ab = bc = ca$, to jest, ako i samo ako je $a = b = c$. Dakle, ako je zadano oplošje kvadra O, volumen će biti najveći kada je $V = \left(\frac{O}{6}\right)^{\frac{3}{2}}$, tj. ako vrijedi $a = b = c$, odnosno kada je kvadar kocka. Nadalje, ako je zadan volumen kvadra V, oplošje će biti najmanje ako je $O = 6V^{\frac{2}{3}}$, odnosno kada je kvadar kocka.

2.3 Cauchy-Schwarzova nejednakost

Prije nego što iskažemo i dokažemo teorem o Cauchy-Schwarzovoj nejednakosti, podsjetimo se definicije unitarnog prostora i norme ([1]).

Definicija 2.3.1. *Neka je V vektorski prostor nad poljem $\mathbb{F}$. Skalarni produkt ili skalarno množenje na V je preslikavanje $\langle\cdot,\cdot\rangle : V \times V \to \mathbb{F}$ koje ima sljedeća svojstva:*

1. $\langle x, x\rangle \geq 0$ *za svaki* $x \in V$,
2. $\langle x, x\rangle = 0$ *ako i samo ako je* $x = 0$,
3. $\langle x_1 + x_2, y\rangle = \langle x_1, y\rangle + \langle x_2, y\rangle$ *za sve* $x_1, x_2, y \in V$,
4. $\langle \alpha x, y\rangle = \alpha \langle x, y\rangle$ *za sve* $\alpha \in \mathbb{F}$ *i* $x, y \in V$,
5. $\langle x, y\rangle = \overline{\langle y, x\rangle}$ *za sve* $x, y \in V$.

Broj $\langle x, y\rangle$ nazivamo sklarni produkt vektora x i y. Vektorski prostor na kojem je zadan skalarni produkt nazivamo unitarni prostor. Ponekad kažemo da je uređeni par $(V, \langle\cdot,\cdot\rangle)$ unitarni prostor.

Definicija 2.3.2. *Neka je V unitarni prostor nad poljem $\mathbb{F}$. Norma na V (inducirana skalarnim produktom) je funkcija definirana kao*

$$\|\cdot\| : V \to \mathbb{R}, \quad \|x\| = \sqrt{\langle x, x\rangle}.$$

Realni broj $\|x\|$ nazivamo norma ili duljina elementa $x \in V$.

Teorem 2.3.3 (Cauchy-Scwarzova nejednakost). *Neka je V unitarni prostor nad poljem $\mathbb{F}$. Za sve $x, y \in V$ vrijedi*

$$|\langle x, y\rangle| \leq \|x\| \, \|y\|,$$

pri čemu jednakost vrijedi ako i samo ako su x i y linearno zavisni vektori.

Dokaz. Ako je $x = 0$ ili $y = 0$, tvrdnja očito vrijedi.

Pretpostavimo da su $x, y \neq 0$. Sada x možemo rastaviti na međusobno ortogonalne komponente od kojih je jedna kolinearna s y, odnosno nalazimo $\alpha \in \mathbb{F}$ tako da je $x = (x - \alpha y) + \alpha y$ i $(x - \alpha y) \perp y$. Iz uvjeta ortogonalnosti dobivamo α

$$\langle x - \alpha y, y\rangle = 0 \Rightarrow \alpha = \frac{\langle x, y\rangle}{\|y\|^2},$$

pa x možemo zapisati kao

$$x = \left(x - \frac{\langle x, y\rangle}{\|y\|^2} y\right) + \frac{\langle x, y\rangle}{\|y\|^2} y.$$

Zbog ortogonalnosti komponenata možemo primijeniti Pitagorin poučak pa dobivamo

$$\|x\|^2 = \|x - \frac{\langle x, y\rangle}{\|y\|^2} y\|^2 + \|\frac{\langle x, y\rangle}{\|y\|^2} y\|^2 \geq \|\frac{\langle x, y\rangle}{\|y\|^2} y\|^2 = \frac{|\langle x, y\rangle|^2}{\|y\|^2},$$

odakle slijedi tražena nejednakost.

Ako vrijedi $|\langle x, y\rangle| = \|x\|\,\|y\|$, tada u prethodnoj nejednakosti moramo imati jednakost, odnosno mora biti $x - \frac{\langle x,y\rangle}{\|y\|^2} y = 0$, tj. x i y moraju biti linearno zavisni. Obratno, ako su x i y linearno zavisni, očito vrijedi $|\langle x, y\rangle| = \|x\|\,\|y\|$. □

Idući teorem je je specijalni slučaj Cauchy-Schwarzove nejednakosti u unitarnom prostoru $\mathbb{R}^n$, promatranom uz standardni skalarni produkt.

Teorem 2.3.4. *Neka su $a = (a_1, a_2, \ldots, a_n), b = (b_1, b_2, \ldots, b_n)$ dane n-torke realnih brojeva. Tada je*

$$\left|\sum_{i=1}^{n} a_i b_i\right| \leq \sqrt{\sum_{i=1}^{n} a_i^2} \sqrt{\sum_{i=1}^{n} b_i^2}, \tag{2.10}$$

pri čemu jednakost vrijedi ako i samo ako su n-torke a i b proporcionalne, tj. postoji realni broj $\lambda \in \mathbb{R}$ takav da je

$$b_i = \lambda a_i, \quad i = 1, \ldots, n.$$

Dokaz. Promotrimo kvadratnu funkciju $P(x) = \sum_{i=1}^{n} (a_i x + b_i)^2$. Tada je

$$\begin{aligned} P(x) &= (a_1 x + b_1)^2 + (a_2 x + b_2)^2 + \ldots + (a_n x + b_n)^2 \\ &= (a_1^2 + a_2^2 + \ldots + a_n^2)x^2 + 2(a_1 b_1 + a_2 b_2 + \ldots + a_n b_n)x + (b_1^2 + b_2^2 + \ldots + b_n^2) \\ &= \left(\sum_{i=1}^{n} a_i^2\right) x^2 + 2\left(\sum_{i=1}^{n} a_i b_i\right) x + \sum_{i=n}^{n} b_i^2. \end{aligned}$$

Primijetimo da je $P(x) \geq 0, \forall x \in \mathbb{R}$, pa za diskriminantu D vrijedi $D \leq 0$, a kako je

$$\begin{aligned} D &= \left(-2\sum_{i=1}^{n} a_i b_i\right)^2 - 4\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=n}^{n} b_i^2\right) \\ &= 4\left(\sum_{i=1}^{n} a_i b_i\right)^2 - 4\left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=n}^{n} b_i^2\right), \end{aligned}$$

slijedi

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=n}^{n} b_i^2\right),$$

što je upravo nejednakost (2.10).

Jednakost vrijedi ako i samo ako je $D = 0$, tj. ako i samo ako funkcija P ima dvostruku realnu nultočku. Dakle, ako i samo ako postoji $x_0 \in \mathbb{R}$ tako da vrijedi

$$\sum_{i=1}^{n}(a_i x_0 + b_i)^2 = 0 \Leftrightarrow a_i x_0 + b_i = 0, \quad i = 1, \ldots, n,$$

$$\Leftrightarrow b_i = -a_i x_0, \qquad i = 1, \ldots, n,$$

odnosno n-torke a i b su proporcionalne. □

Sada slijede zadaci u kojima je jedan od način rješavanja primjena Cauchy-Schwarzove nejednakosti.

Zadatak 2.3.5. *Dokažite da za sve pozitivne brojeve $a, b, c \in \mathbb{R}$ vrijedi*

$$a^2 + b^2 + c^2 \geq ab + bc + ca.$$

Rješenje:

1. način: Kako je zadana nejednakost simetrična s obzirom na brojeve a, b, c, bez smanjenja općenitosti, možemo pretpostaviti da je $a \geq b \geq c$. Prebacimo sve na lijevu stranu nejednakosti

$$a^2 + b^2 + c^2 - ab - bc - ca \geq 0,$$

pa faktoriziramo na sljedeći način

$$a(a - b) + b(b - c) + c(c - a) \geq 0.$$

Uočimo da su prva dva pribrojnika nenegativni, dok je posljednji manji ili jednak nuli. Sada posljednji izraz transformiramo na sljedeći način

$$a(a - b) + b(b - c) + c(c - b + b - a) \geq 0,$$

što nam daje

$$a(a - b) + b(b - c) - c(a - b) - c(b - c) \geq 0,$$

i faktoriziranjem dobivamo

$$(a - b)(a - c) + (b - c)^2 \geq 0,$$

što očito vrijedi. Uočimo da je tražena nejednakost ekvivalentna gornjoj nejednakosti.
Iz posljednje nejednakosti vidimo da jednakost vrijedi ako i samo ako je $a = b = c$.

2. način:

S obzirom da se ovdje pojavljuju kvadrati brojeva a, b, c, kao i njihovi mješoviti umnošci, za očekivati je da će nam pomoći formule za kvadrat binoma. Također, uočimo simetričnost nejednakosti s obzirom na a, b, c. Množenjem tražene nejednakosti s 2 i prikladnim grupiranjem pribrojnika dobijemo

$$(a-b)^2 + (b-c)^2 + (c-a)^2 \geq 0,$$

što je očito zadovoljeno.
3. način:
Primijenimo Cauchy-Schwarzovu nejednakost na desnu stranu nejednakosti i dobivamo traženo

$$ab + bc + ca \leq \sqrt{a^2 + b^2 + c^2} \cdot \sqrt{b^2 + c^2 + a^2} = a^2 + b^2 + c^2.$$

Zadatak 2.3.6. *Dokažite da za sve $n \in \mathbb{N}$, te $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$ vrijedi nejednakost*

$$\sqrt{a_1^2 + b_1^2} + \sqrt{a_2^2 + b_2^2} + \ldots + \sqrt{a_n^2 + b_n^2} \geq \sqrt{(a_1 + \ldots + a_n)^2 + (b_1 + \ldots + b_n)^2}.$$

Rješenje:
Ovu nejednakost ćemo dokazati metodom matematičke indukcije.
(**Baza**) Za $n = 2$ nejednakost glasi

$$\sqrt{a_1^2 + b_1^2} + \sqrt{a_2^2 + b_2^2} \geq \sqrt{(a_1 + a_2)^2 + (b_1 + b_2)^2}.$$

Kvadriranjem i reduciranjem članova dobivamo

$$2\sqrt{(a_1^2 + b_1^2)(a_2^2 + b_2^2)} \geq 2a_1a_2 + 2b_1b_2,$$

pa dijeljenjem s 2 i ponovnim kvadriranjem dobivamo

$$(a_1^2 + b_1^2)(a_2^2 + b_2^2) \geq (a_1a_2 + b_1b_2)^2,$$

što je upravo Cauchy-Schwarzova nejednakost.
(**Pretpostavka**) Pretpostavimo da za neki $n \in \mathbb{N}$, te sve $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$ vrijedi nejednakost

$$\sqrt{a_1^2 + b_1^2} + \sqrt{a_2^2 + b_2^2} + \ldots + \sqrt{a_n^2 + b_n^2} \geq \sqrt{(a_1 + \ldots + a_n)^2 + (b_1 + \ldots + b_n)^2}.$$

(**Korak**) Dokažimo da nejednakost vrijedi i za proizvoljne $a_1, \ldots, a_{n+1}, b_1, \ldots, b_{n+1} \in \mathbb{R}$, tj. da vrijedi

$$\begin{aligned}\sqrt{a_1^2 + b_1^2} + \sqrt{a_2^2 + b_2^2} + \ldots + \sqrt{a_n^2 + b_n^2} + \sqrt{a_{n+1}^2 + b_{n+1}^2}& \\ \geq \sqrt{(a_1 + \ldots + a_n + a_{n+1})^2 + (b_1 + \ldots + b_n + b_{n+1})^2}&.\end{aligned}$$

Na prvih n pribrojnika s lijeve strane primijenimo pretpostavku indukcije i dobivamo

$$\begin{aligned}\sqrt{a_1^2+b_1^2}+\sqrt{a_2^2+b_2^2}+\ldots+\sqrt{a_n^2+b_n^2}+\sqrt{a_{n+1}^2+b_{n+1}^2}&\\ \geq \sqrt{(a_1+\ldots+a_n)^2+(b_1+\ldots+b_n)^2}+\sqrt{a_{n+1}^2+b_{n+1}^2}&.\end{aligned}$$

Uočimo sada da desna strana ima oblik kao u našoj nejednakosti za slučaj $n = 2$, što smo već dokazali u bazi indukcije. Prema tome, vrijedi

$$\begin{aligned}\sqrt{(a_1+\ldots+a_n)^2+(b_1+\ldots+b_n)^2}+\sqrt{a_{n+1}^2+b_{n+1}^2}&\\ \geq \sqrt{(a_1+\ldots+a_n+a_{n+1})^2+(b_1+\ldots+b_n+b_{n+1})^2}&.\end{aligned}$$

Tako dobivamo

$$\begin{aligned}\sqrt{a_1^2+b_1^2}+\sqrt{a_2^2+b_2^2}+\ldots+\sqrt{a_n^2+b_n^2}+\sqrt{a_{n+1}^2+b_{n+1}^2}&\\ \geq \sqrt{(a_1+\ldots+a_n+a_{n+1})^2+(b_1+\ldots+b_n+b_{n+1})^2}&.\end{aligned}$$

Prema principu matematičke indukcije tvrdnja vrijedi za svaki prirodan broj $n \geq 2$.

Iako je Cauchy-Schwarzova nejednakost jednostavna za primjenu, u nekim zadacima je teško odrediti na koje izraze primijeniti ovu nejednakost kako bi dobili ono što želimo. Takav slučaj je u sljedeća dva zadatka koji su se pojavili na Hrvatskoj matematičkoj olimpijadi, prvi 2018., a drugi 2010. godine. Isto tako, sljedeća dva zadatka su primjer uvjetne nejednakosti u kojima je dani uvjet koji se pri dokazivanju mora barem jednom iskoristiti.

Zadatak 2.3.7. *Neka su a, b, c pozitivni realni brojevi takvi da je $a + b + c = 2$. Dokažite da vrijedi*

$$\frac{(a-1)^2}{b}+\frac{(b-1)^2}{c}+\frac{(c-1)^2}{a} \geq \frac{1}{4}\left(\frac{a^2+b^2}{a+b}+\frac{b^2+c^2}{b+c}+\frac{c^2+a^2}{c+a}\right).$$

Rješenje:

Promotrimo prva dva pribrojnika s lijeve strane jednakosti i zapišimo ih na sljedeći način

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

Zbroj kvadrata neka dva broja podsjeća nas na izraz pod korijenom u Cauchy-Schwarzovoj nejednakosti

$$\left(\frac{a-1}{\sqrt{b}}\right)\cdot x+\left(\frac{b-1}{\sqrt{c}}\right)\cdot y \leq \sqrt{\left(\frac{a-1}{\sqrt{b}}\right)^2+\left(\frac{b-1}{\sqrt{c}}\right)^2}\sqrt{x^2+y^2},$$

gdje su x i y realni brojevi. Sada moramo odabrati brojeve x i y takve da se s lijeve strane gornje nejednakosti pojednostavi izraz. Očito će $x = \sqrt{b}$ i $y = \sqrt{c}$ biti dobar odabir, te slijedi

$$\sqrt{\left(\frac{a-1}{\sqrt{b}}\right)^2 + \left(\frac{b-1}{\sqrt{c}}\right)^2}\sqrt{\left(\sqrt{b}\right)^2 + \left(\sqrt{c}\right)^2} \geq \frac{a-1}{\sqrt{b}} \cdot \sqrt{b} + \frac{b-1}{\sqrt{c}} \cdot \sqrt{c} = a + b - 2,$$

pa onda vrijedi i

$$\frac{(a-1)^2}{b} + \frac{(b-1)^2}{c} \geq \frac{(2-a-b)^2}{b+c} = \frac{c^2}{b+c}$$

jer je $c = 2 - a - b$. Analogno, dobivamo

$$\frac{(b-1)^2}{c} + \frac{(c-1)^2}{a} \geq \frac{(2-b-c)^2}{c+a} = \frac{a^2}{c+a},$$

$$\frac{(a-1)^2}{b} + \frac{(b-1)^2}{c} \geq \frac{(2-a-b)^2}{b+c} = \frac{b^2}{a+b}.$$

Zbrajanjem gornjih nejednakosti dobivamo

$$\frac{(a-1)^2}{b} + \frac{(b-1)^2}{c} + \frac{(c-1)^2}{a} \geq \frac{1}{2}\left(\frac{c^2}{b+c} + \frac{a^2}{c+a} + \frac{b^2}{a+b}\right).$$

Uočimo da vrijedi sljedeće

$$\begin{aligned}\frac{c^2}{b+c} + \frac{a^2}{c+a} + \frac{b^2}{a+b} - \frac{b^2}{b+c} - \frac{c^2}{c+a} - \frac{a^2}{a+b} &= \frac{c^2-b^2}{b+c} + \frac{a^2-c^2}{c+a} + \frac{b^2-a^2}{a+b} \\ &= c - b + a - c + b - a = 0,\end{aligned}$$

tj. vrijedi

$$\frac{c^2}{b+c} + \frac{a^2}{c+a} + \frac{b^2}{a+b} = \frac{b^2}{b+c} + \frac{c^2}{c+a} + \frac{a^2}{a+b}.$$

Sada desnu stranu zadane nejednakosti možemo zapisati kao

$$\begin{aligned}\frac{1}{4}\left(\frac{a^2+b^2}{a+b} + \frac{b^2+c^2}{b+c} + \frac{c^2+a^2}{c+a}\right) &= \frac{1}{4}\left(2 \cdot \frac{b^2}{a+b} + 2 \cdot \frac{c^2}{b+c} + 2 \cdot \frac{a^2}{c+a}\right) \\ &= \frac{1}{2}\left(\frac{b^2}{a+b} + \frac{c^2}{b+c} + \frac{a^2}{c+a}\right),\end{aligned}$$

pa vrijedi i zadana nejednakost.

Zadatak 2.3.8. *Neka su a, b, c pozitivni realni brojevi takvi da je $a + b + c = 3$. Dokažite da je*

$$\frac{a^4}{b^2+c} + \frac{b^4}{c^2+a} + \frac{c^4}{a^2+b} \geq \frac{3}{2}.$$

Rješenje:

1. način: Zapišimo lijevu strane zadane nejednakosti u sljedećem obliku

$$\frac{a^4}{b^2+c} + \frac{b^4}{c^2+a} + \frac{c^4}{a^2+b} = \left(\frac{a^2}{\sqrt{b^2+c}}\right)^2 + \left(\frac{b^2}{\sqrt{c^2+a}}\right)^2 + \left(\frac{c^2}{\sqrt{a^2+b}}\right)^2.$$

Sada opet, slično kao u prethodnom zadatku, možemo primijeniti Cauchy-Schwarzovu nejednakost. Tako dobivamo

$$\begin{aligned}
&\left(\left(\frac{a^2}{\sqrt{b^2+c}}\right)^2 + \left(\frac{b^2}{\sqrt{c^2+a}}\right)^2 + \left(\frac{c^2}{\sqrt{a^2+b}}\right)^2\right)\left(\left(\sqrt{b^2+c}\right)^2 + \left(\sqrt{c^2+a}\right)^2 + \left(\sqrt{a^2+b}\right)^2\right)\\
&\quad\geq \left(\frac{a^2}{\sqrt{b^2+c}} \cdot \sqrt{b^2+c} + \frac{b^2}{\sqrt{c^2+a}} \cdot \sqrt{c^2+a} + \frac{c^2}{\sqrt{a^2+b}} \cdot \sqrt{a^2+b}\right)^2\\
&\quad= \left(a^2+b^2+c^2\right)^2,
\end{aligned}$$

tj. vrijedi

$$\frac{a^4}{b^2+c} + \frac{b^4}{c^2+a} + \frac{c^4}{a^2+b} = \frac{\left(a^2+b^2+c^2\right)^2}{(a^2+b^2+c^2)+(a+b+c)}.$$

Iz uvjeta zadatka sada slijedi

$$\frac{a^4}{b^2+c} + \frac{b^4}{c^2+a} + \frac{c^4}{a^2+b} \geq \frac{\left(a^2+b^2+c^2\right)^2}{(a^2+b^2+c^2)+3}. \tag{2.11}$$

Kako znamo koliko je $a + b + c$, a želimo donju granicu za $a^2 + b^2 + c^2$, primjenom AK nejednakosti na a, b, c dobivamo

$$\sqrt{\frac{a^2+b^2+c^2}{3}} \geq \frac{a+b+c}{3} = 1,$$

odakle slijedi

$$a^2 + b^2 + c^2 \geq 3.$$

Uvedimo supstituciju $x = a^2 + b^2 + c^2$, $x \geq 3$. Iz nejednakosti (2.11) vidimo da je dovoljno dokazati da nejednakost

$$\frac{x^2}{x+3} \geq \frac{3}{2},$$

vrijedi za sve $x \geq 3$. Uočimo da je, uz uvjet $x \geq 3$, nejednadžba $\frac{x^2}{x+3} \geq \frac{3}{2}$ ekvivalentna kvadratnoj nejednadžbi $2x^2 - 3x - 9 \geq 0$. Rješenja kvadratne jednadžbe $2x^2 - 3x - 9 = 0$ su $x_1 = 3$ i $x_2 = \frac{-3}{2}$. Slijedi, $2x^2 - 3x - 9 \geq 0$ za sve $x \geq 3$.

2. način: Uočimo simetričnost nejednakosti s obzirom na a, b, c i pokušajmo svaki pribrojnik s lijeve strane nejednakosti ograničiti varijablama a, b ili c.

Promotrimo prvi pribrojnik i uočimo da ako primijenimo AG nejednakost na $\frac{a^4}{b^2+c}$ i $\frac{b^2+c}{4}$ dobivamo

$$\frac{a^4}{b^2+c} + \frac{b^2+c}{4} \geq 2\sqrt{\frac{a^4}{b^2+c} \cdot \frac{b^2+c}{4}} = 2\sqrt{\frac{a^4}{4}} = a^2,$$

tj. ograničili smo ga varijablom a.

Analogno dobivamo $\dfrac{b^4}{c^2+a} + \dfrac{c^2+a}{4} \geq b^2$ i $\dfrac{c^4}{a^2+b} + \dfrac{a^2+b}{4} \geq c^2$.

Zbrajanjem tih triju nejednakosti dobivamo

$$\left(\frac{a^4}{b^2+c} + \frac{b^4}{c^2+a} + \frac{c^4}{a^2+b}\right) + \left(\frac{b^2+c}{4} + \frac{c^2+a}{4} + \frac{a^2+b}{4}\right) \geq a^2 + b^2 + c^2,$$

tj.

$$\frac{a^4}{b^2+c} + \frac{b^4}{c^2+a} + \frac{c^4}{a^2+b} \geq \frac{3}{4}\left(a^2+b^2+c^2\right) - \frac{1}{4}(a+b+c).$$

Sada iz uvjeta zadatka slijedi

$$\frac{a^4}{b^2+c} + \frac{b^4}{c^2+a} + \frac{c^4}{a^2+b} \geq \frac{3}{4}\left(a^2+b^2+c^2\right) - \frac{1}{4} \cdot 3. \tag{2.12}$$

Primjenom AK nejednakosti i kvadriranjem dobivamo

$$a^2 + b^2 + c^2 \geq 3.$$

Uvrštavanjem gornje nejednakosti u nejednakost (2.12) dobivamo

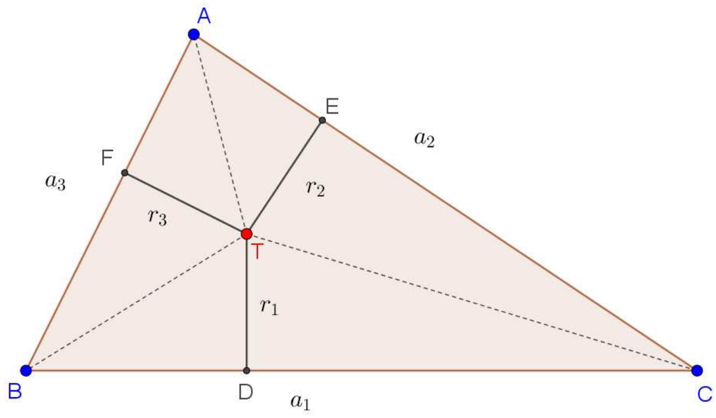
$$\frac{a^4}{b^2+c} + \frac{b^4}{c^2+a} + \frac{c^4}{a^2+b} \geq \frac{3}{4} \cdot 3 - \frac{3}{4} = \frac{6}{4} = \frac{3}{2},$$

tj. vrijedi tražena nejednakost.

Zadatak 2.3.9. *Neka je dan trokut ABC sa stranicama duljina a_1, a_2, a_3 te točka T unutar njega. Neka su r_1, r_2, r_3 redom udaljenosti te točke od stranica trokuta te R polumjer trokutu opisane kružnice. Dokažite da tada vrijedi nejednakost*

$$\sqrt{r_1} + \sqrt{r_2} + \sqrt{r_3} \leq \sqrt{\frac{a_1^2 + a_2^2 + a_3^2}{2R}},$$

te da jednakost vrijedi ako i samo ako je trokut ABC jednakostraničan, a točka T središte trokutu upisane kružnice.



Slika 2.4: Trokut ABC

Rješenje:
Iz zadane nejednakosti vidimo da lijevu stranu moramo ograničiti duljinama stranica trokuta i polumjerom opisane kružnice tom trokutu, pa zapišimo lijevu stranu nejednakosti na sljedeći način

$$\begin{aligned}\sqrt{r_1}+\sqrt{r_2}+\sqrt{r_3} &= \sqrt{r_1a_1\cdot\frac{1}{a_1}}+\sqrt{r_2a_2\cdot\frac{1}{a_2}}+\sqrt{r_3a_3\cdot\frac{1}{a_3}}\\ &= \sqrt{r_1a_1}\cdot\sqrt{\frac{1}{a_1}}+\sqrt{r_2a_2}\cdot\sqrt{\frac{1}{a_2}}+\sqrt{r_3a_3}\cdot\sqrt{\frac{1}{a_3}}.\end{aligned}$$

Primijenimo sada Cauchy-Schwarzovu nejednakost i dobivamo

$$\begin{aligned}&\sqrt{r_1a_1}\cdot\sqrt{\frac{1}{a_1}}+\sqrt{r_2a_2}\cdot\sqrt{\frac{1}{a_2}}+\sqrt{r_3a_3}\cdot\sqrt{\frac{1}{a_3}}\\ &\quad\le \sqrt{\left(\sqrt{a_1r_1}\right)^2+\left(\sqrt{a_2r_2}\right)^2+\left(\sqrt{a_3r_3}\right)^2}\cdot\sqrt{\left(\sqrt{\frac{1}{a_1}}\right)^2+\left(\sqrt{\frac{1}{a_2}}\right)^2+\left(\sqrt{\frac{1}{a_3}}\right)^2}\\ &\quad= \sqrt{a_1r_1+a_2r_2+a_3r_3}\cdot\sqrt{\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}},\end{aligned}$$

pri čemu jednakost vrijedi ako i samo ako je

$$\frac{\sqrt{a_1r_1}}{\sqrt{\frac{1}{a_1}}}=\frac{\sqrt{a_2r_2}}{\sqrt{\frac{1}{a_2}}}=\frac{\sqrt{a_3r_3}}{\sqrt{\frac{1}{a_3}}},$$

odnosno ako i samo ako je $a_1^2 r_1 = a_2^2 r_2 = a_3^2 r_3$. Uočimo da izrazi $a_1 r_1, a_2 r_2, a_3 r_3$ predstavljaju redom dvostruke vrijednosti površina trokuta BCT, CAT, ABT. Nadalje, očito je suma ove tri površine jednaka površini trokuta ABC, koja se može izračunati i pomoću formule $P = \frac{a_1 a_2 a_3}{4R}$. Prema tome, imamo

$$a_1 r_1 + a_2 r_2 + a_3 r_3 = \frac{a_1 a_2 a_3}{2R}$$

pa je

$$\begin{aligned}
\sqrt{r_1} + \sqrt{r_2} + \sqrt{r_3} &\leq \sqrt{\frac{a_1 a_2 a_3}{2R}} \cdot \sqrt{\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3}} \\
&= \sqrt{\frac{a_1 a_2 a_3}{2R}} \cdot \sqrt{\frac{a_1 a_2 + a_2 a_3 + a_3 a_1}{a_1 a_2 a_3}} \\
&= \sqrt{\frac{a_1 a_2 + a_2 a_3 + a_3 a_1}{2R}}.
\end{aligned}$$

Sada, opet prema Cauchy-Schwarzovoj nejednakosti, slijedi

$$a_1 a_2 + a_2 a_3 + a_3 a_1 \leq \sqrt{a_1^2 + a_2^2 + a_3^2} \sqrt{a_2^2 + a_3^2 + a_1^2} = a_1^2 + a_2^2 + a_3^2,$$

pri čemu jednakost vrijedi ako i samo ako je $\frac{a_1}{a_2} = \frac{a_2}{a_3} = \frac{a_3}{a_1}$, odnosno ako i samo ako je $a_1 = a_2 = a_3$. Konačno, imamo

$$\sqrt{r_1} + \sqrt{r_2} + \sqrt{r_3} \leq \sqrt{\frac{a_1^2 + a_2^2 + a_3^2}{2R}},$$

tj. vrijedi zadana nejednakost, pri čemu se jednakost postiže ako i samo ako je $a_1^2 r_1 = a_2^2 r_2 = a_3^2 r_3$ i $a_1 = a_2 = a_3$, odnosno ako i samo ako je $a_1 = a_2 = a_3$ i $r_1 = r_2 = r_3$. Dakle, jednakost vrijedi ako i samo ako je trokut ABC jednakostraničan, a točka T središte kružnice upisane tom trokutu.

Cauchy-Schwarzovu nejednakost možemo primijeniti i u pronalaženju ekstremnih vrijednosti funkcija kao u idućem zadatku.

Zadatak 2.3.10. *Neka je $S = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$. Koristeći Cauchy-Schwarzovu nejednakost u unitarnom prostoru odredite maksimalnu vrijednost funkcije $f : S \to \mathbb{R}, f(x, y, z) = 5x + 2y + 3z$, te točke iz S u kojima se ona postiže.*

Rješenje:

Neka je $a = (x, y, z) \in S$ i $b = (5, 2, 3)$. Prema teoremu 2.3.4 vrijedi

$$|5x + 2y + 3z| \leq \sqrt{x^2 + y^2 + z^2} \cdot \sqrt{5^2 + 2^2 + 3^2} = \sqrt{1} \cdot \sqrt{38} = \sqrt{38},$$

odnosno izračunali smo da maksimalna vrijednost funkcije $f(x, y, z) = 5x + 2y + 3z$ iznosi $\sqrt{38}$. Izračunajmo sada još u kojim točkama iz S se ona postiže, tj. moramo izračunati kada se postiže jednakost u gornjoj nejednakosti. Iz prethodnih teorema znamo da se jednakost postiže kada su a i b linearno zavisni, tj. vrijedi $a = \alpha b, \alpha \in \mathbb{R}$. Imamo $a = (5\alpha, 2\alpha, 3\alpha)$, a kako je $a \in S$ mora vrijediti sljedeće

$$(5\alpha)^2 + (2\alpha)^2 + (3\alpha)^2 = 1,$$

pa dobivamo da je $\alpha = \pm\frac{\sqrt{38}}{38}$. Dakle, maksimalna vrijednost se postiže u točki $\left(\frac{5\sqrt{38}}{38}, \frac{2\sqrt{38}}{38}, \frac{3\sqrt{38}}{38}\right)$, dok se u točki $\left(-\frac{5\sqrt{38}}{38}, -\frac{2\sqrt{38}}{38}, -\frac{3\sqrt{38}}{38}\right)$ postiže minimalna vrijednost.

Poglavlje 3

Aritmetika

U ovom poglavlju razmatramo tehnike rješavanja problema koje su važne u rješavanju aritmetičkih problema. Jedna od najvažnijih tehnika temelji se na osnovnom teoremu aritmetike prema kojem se svaki cijeli broj može jedinstveno napisati kao produkt prostih brojeva. Teorijska pozadina neophodna za dokaz ovog ključnog teorema zahtijeva raspravu o pojmu djeljivosti. Stoga ćemo poglavlje započeti razmatranjem problema o najvećem zajedničkom djelitelju i najmanjem zajedničkom višekratniku. Za razumijevanje istih potrebni su nam teorem o dijeljenju s ostatkom i Euklidov algoritam. Zatim iskazujemo i dokazujemo osnovni teorem aritmetike i neke posljedice tog teorema. Na kraju, uvodimo pojam kongruencija koji nam uvelike pomaže u rješavanju problema koji se tiču odnosa cijelih brojeva.

3.1 Djeljivost

Pojam djeljivosti jedan je od najjednostavnijih, ali ujedno i najvažnijih pojmova u teoriji brojeva.

Definicija 3.1.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b djeljiv s a, odnosno da a dijeli b, ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo kao $a \mid b$. Ako b nije djeljiv s a, onda pišemo $a \nmid b$. Ako $a \mid b$, onda još kažemo da je a djelitelj od b, te da je b višekratnik od a. Oznaka $a^k \| b$ će nam značiti da $a^k \mid b$, ali $a^{k+1} \nmid b$. ([2])*

Lako se pokaže da vrijede sljedeće tvrdnje.

- Ako su a i b cijeli brojevi djeljivi cijelim brojem $m, m \neq 0$, onda je s m djeljiv i njihov zbroj $a + b$ i njihova razlika $a - b$.
- Ako n dijeli dva člana u izrazu $a = b + c$, onda n dijeli sva tri člana.

- Ako je cijeli broj a djeljiv s m, i cijeli broj b djeljiv s n, onda je umnožak ab djeljiv s mn.

Osnovna metoda dokazivanja djeljivosti nekog cijelog broja b cijelim brojem a je faktoriziranje broja b u umnožak broja a i cijelog broja x. Obično se u nekim jednostavnijim problemima ovakav način faktorizacije može dobiti iz nekih osnovnih algebarskih faktorizacija (kvadrat binoma, kvadrat razlike i slično). Sljedeće dvije formule faktorizacije razlike, odnosno zbroja n-tih potencija vrlo su korisne u dokazivanju djeljivosti.

Za svaki $n \in \mathbb{N}$ vrijedi

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1}). \tag{3.1}$$

Za neparan $n \in \mathbb{N}$ vrijedi

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1}). \tag{3.2}$$

Zadatak 3.1.2. *Dokažite da je broj* $1\underbrace{0\cdots0}_{200}1$ *djeljiv brojem* 1001.

Rješenje:

Zapišimo dani broj kao $1\underbrace{0\cdots0}_{200}1 = 10^{201} + 1$ i $1001 = 10^3 + 1$. Kako je $1\underbrace{0\cdots0}_{200}1 = \left(10^3\right)^{67} + 1 = \left(10^3\right)^{67} + 1^{67}$, možemo upotrijebiti formulu (3.2) i dobivamo

$$\left(10^3\right)^{67} + 1^{67} = \left(10^3 + 1\right)\left((10^3)^{66} - (10^3)^{65} \cdot 1 + \ldots - 10^3 \cdot 1^{65} + 1^{66}\right).$$

Dakle, 1001 dijeli broj $1\underbrace{0\cdots0}_{200}1$.

Definicija 3.1.3. *Neka su b i c cijeli brojevi. Cijeli broj a se zove* zajednički djelitelj *od b i c ako $a \mid b$ i $a \mid c$. Ako je barem jedan od brojeva b i c različit od nule, tj. ako vrijedi $b^2 + c^2 > 0$, onda postoji samo konačno mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se* najveći zajednički djelitelj *od b i c i označava s $D(b, c)$ ili kraće (b, c). Slično se definira najveći zajednički djelitelj brojeva $b_1, b_2, \ldots, b_n$ koji nisu svi jednaki nuli, te se označava s $D(b_1, b_2, \ldots, b_n)$.*

Iz definicije 3.1.3 slijedi nekoliko svojstava.

Propozicija 3.1.4. *Neka su $b, c \in \mathbb{Z}$. Tada vrijedi:*

1. $D(b, c) \in \mathbb{N}$,

2. $D(\pm b, \pm c) = D(b, c)$,

3. $D(b,c) = D(c,b)$,

4. $D(b,c+bx) = D(c,b)$ *za sve* $x \in \mathbb{Z}$.

Teorem 3.1.5 (Teorem o dijeljenju s ostatkom)**.** *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je* $b = qa + r$*, pri čemu je* $0 \leq r < a$.

Ako ponavljamo primjenu teorema 3.1.5 na dva cijela broja, možemo izračunati najveći zajednički djelitelj tih dvaju brojeva.

Uzmemo pozitivne cijele brojeve b_1 i b_2 takve da vrijedi $b_1 > b_2$. Prema teoremu 3.1.5 postoje cijeli brojevi q i b_3 takvi da vrijedi

$$b_1 = qb_2 + b_3, \quad 0 \leq b_3 < b_2.$$

Lako se pokaže, koristeći propoziciju 3.1.4, da vrijedi $D(b_1,b_2) = D(b_2,b_3)$.

Ako je $b_3 = 0$, onda $b_2 \mid b_1$, pa je $D(b_1,b_2) = b_2$. Ako je pak $b_3 > 0$, možemo ponoviti postupak, koristeći b_2 i b_3 umjesto b_1 i b_2, da dobijemo cijeli broj b_4 takav da je $D(b_2,b_3) = D(b_3,b_4), b_3 > b_4 \geq 0$.

Nastavljajući na ovaj način, generirat ćemo strogo padajući niz nenegativnih cijelih brojeva

$$b_1 > b_2 > b_3 > \dots$$

takav da je $D(b_1,b_2) = D(b_2,b_3) = \dots = D(b_i,b_{i+1}), i = 1,2,3,\dots$. Budući da se takav niz ne može beskonačno smanjivati, moramo doći do ostatka b_{n+1} koji je jednak nuli i vrijedi $D(b_1,b_2) = D(b_n,b_{n+1}) = b_n$, tj. najveći zajednički djelitelj brojeva b_1 i b_2 je zadnji ostatak b_n koji je različit od nule u ovom postupku. Vrijednosti od x_0 i y_0 u izrazu $D(b_1,b_2) = b_1x_0 + b_2y_0$ mogu se dobiti izražavanjem svakog ostatka b_i kao linearne kombinacije od b i c. Postupak pronalaženja najvećeg zajedničkog djelitelja brojeva b_1 i b_2 naziva se **Euklidov algoritam**.

Prije nego pokažemo kako se taj algoritam primjenjuje na nekom primjeru, navedimo i dokažimo jedan od bitnijih teorema vezanih za ovo poglavlje:

Teorem 3.1.6. *Za prirodne brojeve a i b uvijek postoje cijeli brojevi s i t takvi da vrijedi*

$$sa + tb = D(a,b). \tag{3.3}$$

Dokaz. Dokaz ćemo provesti metodom matematičke indukcije po broju koraka potrebnih za izračunavanje najvećeg zajedničkog djelitelja pomoću Euklidovog algoritma. Bez smanjenja općenitosti, pretpostavimo da je $a > b$.

(**Baza**) Ako je potreban samo jedan korak, tada postoji cijeli broj q takav da je $a = bq$ i vrijedi $D(a,b) = b$ pa smo dokazali tvrdnju, $s = 0$, $t = 1$. Uočimo da ovaj zapis nije jedinstven, na primjer, vrijedi $D(a,b) = b = a + (1-q)b$, pa uzmemo $s = 1$ i $t = 1-q$, te smo dokazali tvrdnju.

(**Pretpostavka**) Pretpostavimo da tvrdnja vrijedi za sve parove pozitivnih cijelih brojeva koji u Euklidovom algoritmu zahtijevaju manje od k koraka.

(**Korak**) Pretpostavimo da su a i b cijeli brojevi koji zahtijevaju k koraka, $k > 1$. Prema teoremu 3.1.5, postoje cijeli brojevi q i r takvi da je

$$a = qb + r, \quad 0 < r < b.$$

Najveći zajednički djelitelj brojeva b i r možemo izračunati primjenom Euklidovog algoritma u $k - 1$ koraka, pa prema pretpostavci indukcije postoje cijeli brojevi c i d takvi da je

$$cb + dr = D(b, r).$$

Sada iz posljednje dvije jednakosti slijedi

$$\begin{aligned} D(a, b) &= D(b, r) \\ &= cb + dr \\ &= cb + d(a - qb) \\ &= da + (c - dq)b, \end{aligned}$$

i ako uzmemo $s = d$ i $t = c - dq$, dokazali smo tvrdnju teorema. □

Relacija (3.3) naziva se *Bezoutov identitet*. Posebno, ako se cijeli broj c može prikazati u obliku $c = ax + by$, tada je $D(a, b)$ djelitelj broja c, pa ako je $ax + by = 1$ za neke cijele brojeve a i b, onda je $D(a, b) = 1$, odnosno brojevi a i b su relativno prosti.

Zadatak 3.1.7. *Izračunajte cijele brojeve x i y takve da vrijedi*

$$754x + 221y = D(754, 221).$$

Rješenje:

Najprije primijenimo Euklidov algoritam kako bismo pronašli najveći zajednički djelitelj brojeva 754 i 221.

$$\begin{aligned} 754 &= 3 \cdot 221 + 91, \\ 221 &= 2 \cdot 91 + 39, \\ 91 &= 2 \cdot 39 + 13, \\ 39 &= 3 \cdot 13. \end{aligned}$$

Kako bi pronašli tražene cijele brojeve x i y, vraćamo se unatrag kroz korake Euklidovog algoritma:

$$\begin{aligned}13 &= 91 - 2 \cdot 39\\ &= 91 - 2(221 - 2 \cdot 91)\\ &= 5 \cdot 91 - 2 \cdot 221\\ &= 5(754 - 3 \cdot 221) - 2 \cdot 221\\ &= 5 \cdot 754 - 17 \cdot 221.\end{aligned}$$

Dakle, jedno rješenje je $x = 5$ i $y = -17$.

Jednadžbu $ax + by = D(a, b)$ možemo riješiti i na sljedeći način ([2]): ako je

$$\begin{aligned}&r_{-1} = a, \quad r_0 = b, \quad r_i = r_{i-2} - q_i r_{i-1},\\ &x_{-1} = 1, \quad r_0 = 0, \quad x_i = x_{i-2} - q_i x_{i-1},\\ &y_{-1} = 0, \quad r_0 = 1, \quad y_i = y_{i-2} - q_i y_{i-1},\end{aligned}$$

onda je $ax_i + by_i = r_i$, $i = -1, 0, 1, \dots, j + 1$. Posebno, vrijedi $ax_j + cy_j = D(a, b)$. Ovaj algoritam naziva se *prošireni Euklidov algoritam*.

Sada možemo rješenje iz zadatka 3.1.7 zapisati kao:

i	-1	0	1	2	3
q_i			3	2	2
x_i	1	0	1	-2	5
y_i	0	1	-3	7	-17

Dakle, $754 \cdot 5 + 221 \cdot (-17) = 13$, odnosno $x = 5$ i $y = -17$.

Zadatak 3.1.8. *Dokažite da je razlomak* $\dfrac{21n + 4}{14n + 3}$ *neskrativ za svaki* $n \in \mathbb{N}$.

Rješenje:

Trebamo dokazati da su $21n + 4$ i $14n + 3$ relativno prosti brojevi za svaki $n \in \mathbb{N}$, odnosno da je $D(21n + 4, 14n + 3) = 1$.

Pomoću Euklidovog algoritma odredimo $D(21n+4, 14n+3)$.

$$\begin{aligned} 21n+4 &= 1\cdot(14n+3)+(7n+1)\\ 14n+3 &= 2\cdot(7n+1)+1\\ 7n+1 &= (7n+1)\cdot 1 \end{aligned}$$

Dakle, $D(21n+4, 14n+3) = 1$, pa je zadani razlomak neskrativ za svaki $n \in \mathbb{N}$.

Euklidov algoritam može biti strategija i pri računanju ili sređivanju algebarskih izraza.

Zadatak 3.1.9. *Skratite razlomak*

$$\frac{x^8-x^7-3x^5+x^4+x^3+2x^2-1}{x^9-x^8-x^7-3x^6+x^5+4x^4+4x^3+x^2-2x-1}.$$

Rješenje:
Označimo s P polinom u brojniku, te s Q polinom u nazivniku. Da bi skratili razlomak, dijelit ćemo polinom u nazivniku s polinomom u brojniku jer je stupanj polinoma Q veći od stupnja polinoma P. Pri dijeljenju polinoma moramo isključiti sve vrijednosti nepoznanice x za koje je nazivnik jednak 0.

Dijeljenjem polinoma Q s P dobivamo količnik $Q_1 = x$ i ostatak $R_1 = -x^7+3x^4+2x^3+x^2-x-1$, te dijeljenjem polinoma P s R_1 dobivamo količnik $Q_2 = -x+1$ i ostatak $R_2 = 0$. Odnosno kraće zapisano

$$\begin{aligned} Q &= x\cdot P + (-x^7+3x^4+2x^3+x^2-x-1),\\ P &= (-x+1)(x^7+3x^4+2x^3+x^2-x-1). \end{aligned}$$

Najveći zajednički djelitelj polinoma P i Q je R_1, pa polinome P i Q zapišemo kao

$$P = (-x+1)R_1, \quad Q = (-x^2+x+1)R_1.$$

Dakle, vrijedi

$$\frac{P}{Q} = \frac{(-x+1)R_1}{(-x^2+x+1)R_1} = \frac{x-1}{x^2-x-1}.$$

3.2 Osnovni teorem aritmetike

Definicija 3.2.1. *Neka su $b, c \in \mathbb{Z}$. Kažemo da su brojevi b i c* relativno prosti *ako je $D(b,c) = 1$. Cijeli brojevi $b_1, b_2, \ldots, b_n$ su* relativno prosti *ako je $D(b_1, b_2, \ldots, b_n) = 1$, a* u parovima relativno prosti *ako je $D\left(b_i, b_j\right) = 1$ za sve $1 \le i < j \le n$.*

Uočimo, ako su cijeli brojevi $b_1, b_2, \ldots, b_n$ u parovima relativno prosti, onda su i relativno prosti. Obrat ne vrijedi.

Definicija 3.2.2. *Prirodan broj $p > 1$ se zove* prost *ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je* složen.

Uočimo, broj 1 nije ni prost ni složen broj.

Prosti brojevi su važni zbog sljedećeg teorema.

Teorem 3.2.3. *Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

Dokaz. Teorem ćemo dokazati metodom matematičke indukcije po n.

(**Baza**) Za $n = 2$ tvrdnja teorema vrijedi jer je broj 2 prost.

(**Pretpostavka**) Pretpostavimo da je $n > 2$ i da vrijedi tvrdnja teorema za sve m takve da je $2 \leq m < n$.

(**Korak**) Želimo dokazati da se i broj n može prikazati kao produkt prostih faktora. Ako je broj n prost, dokaz je gotov. Ako n nije prost, onda je $n = n_1 n_2$, gdje su brojevi n_1, n_2 brojevi takvi da vrijedi $1 < n_1 < n$ i $1 < n_2 < n$. Po pretpostavci indukcije, brojevi n_1 i n_2 su produkti prostih brojeva, pa slijedi da je i n produkt prostih brojeva.

Prema principu matematičke indukcije, tvrdnja vrijedi za svaki prirodan broj $n > 1$. □

Prije nego što iskažemo i dokažemo osnovni teorem aritmetike dokažimo sljedeću korisnu propoziciju.

Propozicija 3.2.4. *Neka su $a, b \in \mathbb{Z}$. Ako je p prost broj i $p \mid ab$, onda $p \mid a$ ili $p \mid b$. Općenitije, ako $p \mid a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor $a_i, i = 1, \ldots, n$.*

Dokaz. Pretpostavimo da $p \mid ab$. Ako $p \mid a$, onda smo gotovi. Sada pretpostavimo da $p \nmid a$. Tada je $D(p, a) = 1$, pa postoje cijeli brojevi s i t takvi da je $sa + tp = D(p, a) = 1$. Ako pomnožimo posljednju jednakost s b, dobivamo da je $sab + tpb = b$. Sada, zbog toga što p dijeli ab, slijedi da p dijeli b, što je i trebalo dokazati.

Općenitiju tvrdnju dokazujemo metodom matematičke indukcije po n.

(**Baza**) Za $n = 2$ pokazali smo da tvrdnja vrijedi.

(**Pretpostavka**) Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora.

(**Korak**) Sada ako $p \mid a_1(a_2 \cdots a_n)$, onda prema bazi indukcije slijedi da p dijeli a_1 ili p dijeli $a_2 \cdots a_n$. Ako $p \mid a_2 \cdots a_n$, onda po pretpostavci indukcije $p \mid a_i$ za neki $i = 2, \ldots, n$.

Prema principu matematičke indukcije, tvrdnja vrijedi za svaki prirodan broj $n > 1$. □

Iskažimo i dokažimo jedan od najkorisnijih teorema elementarne teorije brojeva.

Teorem 3.2.5 (Osnovni teorem aritmetike)**.** *Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.*

Dokaz. Pretpostavimo da n ima dvije različite faktorizacije, $n = p_1 p_2 \cdots p_r$ i $n = q_1 q_2 \cdots q_s$. Pretpostavimo da postoji p_i takav da je $p_i \neq q_j$ za sve $j = 1, \ldots, s$. Prema prepoziciji 3.2.4, p_i ne dijeli $q_1, \ldots, q_s$, odakle slijedi da p_i ne dijeli n što nije istina. Na isti način dokažemo da za svaki q_k postoji p_l takav da je $q_k = p_l$. Odavde slijedi tvrdnja. □

Iz prethodnog teorema slijedi da svaki prirodan broj n možemo prikazati u obliku

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

gdje su $p_1, p_2, \ldots, p_k$ različiti prosti brojevi, a $\alpha_1, \alpha_2, \ldots, \alpha_k$ prirodni brojevi. Takav prikaz broja n nazivamo *kanonski rastav* broja n na proste faktore. Obično rastav pišemo u rastućem poretku prostih brojeva, tj. za $p_1 < p_2 < \cdots < p_k$, te je takav kanonski rastav jedinstven.

Prije nego što navedemo nekoliko korisnih posljedica ovog teorema, definirajmo pojam *najmanjeg zajedničkog višekratnika.*

Definicija 3.2.6. *Neka su $a_1, a_2, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$. Najmanji prirodan broj c za koji vrijedi da $a_i | c$ za sve $i = 1, 2, \ldots, n$ zove se* najmanji zajednički višekratnik *i označava s $V(a_1, a_2, \ldots, a_n)$.*

Lema 3.2.7. *Svi djelitelji broja*

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

su oblika

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad 0 \leq b_i \leq a_i, i = 1, \ldots, k,$$

i svaki takav broj je djelitelj broja n. Slijedi da n ima točno $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ različitih djelitelja.

Zadatak 3.2.8 (Državno natjecanje, 4. razred, A varijanta, 2013.)**.** *Odredite sve prirodne brojeve n takve da je umnožak svih pozitivnih djelitelja broja n jednak n^3. Prikažite ih u kanonskom obliku, tj. pomoću rastava na proste faktore.*

Rješenje:
Neka su $1 = d_1 < d_2 < \ldots < d_k = n$ svi pozitivni djelitelji broja n. Prema pretpostavci je $d_1 \cdot d_2 \cdot \ldots \cdot d_{k-1} \cdot d_k = n^3$. Uočimo da vrijedi

$$d_1 \cdot d_k = d_2 \cdot d_{k-1} = d_3 \cdot d_{k-2} = n,$$

odakle zaključujemo da je umnožak svih pozitivnih djelitelja broja n jednak n^3 ako i samo ako n ima točno šest djelitelja.

Prirodni broj n možemo prikazati u obliku $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, gdje su $p_1, p_2, \ldots, p_k$ različiti prosti brojevi, a $\alpha_1, \alpha_2, \ldots, \alpha_k$ prirodni brojevi takvi da vrijedi $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_k$. Iz leme 3.2.7 slijedi da je broj djelitelja broja n jednak $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$, odnosno vrijedi

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = 6.$$

Svaki od faktora na lijevoj strani je veći od 1, pa imamo dvije mogućnosti:

$$k = 1, \alpha_1 = 5 \quad \text{ili} \quad k = 2, \alpha_1 = 2, \alpha_2 = 1.$$

Dakle, svi traženi prirodni brojevi n su oblika $n = p^5$ za neki prost broj p ili $n = p^2 q$ za različite proste brojeve p i q.

Prirodan broj a nazivamo *potpuni kvadrat* ako se može zapisati u obliku $n^2, n \in \mathbb{N}$. Iz teorema 3.2.5 slijedi sljedeća lema.

Lema 3.2.9. *Cijeli broj $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ je potpuni kvadrat ako i samo ako su svi a_i parni brojevi. Općenito, cijeli broj $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ se može napisati kao m-ta potencija nekog prirodnog broja n ako i samo ako su svi a_i djeljivi s $m, m \in \mathbb{N}$.*

Sljedeća propozicija daje koristan kriterij djeljivost.

Propozicija 3.2.10. *Neka su $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ i $b = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_l}$ prirodni brojevi dani rastavom na proste faktore. Broj a je djeljiv brojem b ako i samo ako za svaki $q_j, j \in \{1, 2, \ldots, l\}$ postoji neki $i \in \{1, 2, \ldots, k\}$ tako da je $q_j = p_i$ i $a_i \geq b_j$.*

Zadatak 3.2.11. *Dokažite da je $\sqrt{2}$ iracionalan broj.*

Rješenje:

Pretpostavimo suprotno, tj. da je $\sqrt{2}$ racionalan broj. Tada postoje cijeli brojevi r i s takvi da je $\sqrt{2} = \frac{r}{s}$, pri čemu je $D(r, s) = 1$. Kvadriranjem dobivamo $2 = \frac{r^2}{s^2}$, odnosno

$$2s^2 = r^2. \tag{3.4}$$

Slijedi da je r paran broj, dakle oblika $r = 2k, k \in \mathbb{N}$. Uvrstimo u (3.4) i nakon dijeljenja s 2 dobivamo

$$s^2 = 2k^2.$$

Analogno zaključujemo da je $s = 2l$, za neki $l \in \mathbb{N}$, ali sada iz $r = 2k$ i $s = 2l$, slijedi da je $D(r, s) = 2$, što je kontradikcija. Dakle, $\sqrt{2}$ je iracionalan broj.

Zadatak 3.2.12. *Pronađite najmanji prirodan broj n takav da je $\frac{n}{2}$ kvadrat, $\frac{n}{3}$ kub, a $\frac{n}{5}$ peta potencija nekog prirodnog broja.*

Rješenje:
Iz zadanoga vidimo da je broj n djeljiv s $2, 3$ i 5, pa n možemo zapisati kao $n = 2^a 3^b 5^c$ za neke $a, b, c \in \mathbb{N}$. Sada slijedi,

$$\frac{n}{2} = 2^{a-1}3^b5^c, \quad \frac{n}{3} = 2^a3^{b-1}5^c, \quad \frac{n}{5} = 2^a3^b5^{c-1}.$$

Iz gornjih uvjeta slijedi da $a - 1$ mora biti paran i broj a mora biti višekratnik brojeva 3 i 5, a najmanji prirodan broj koji to zadovoljava je $a = 15$. Analogno, $b - 1$ mora biti djeljiv sa 3 i broj b mora biti višekratnik brojeva 2 i 5, a najmanji prirodan broj koji to zadovoljava je $b = 10$, te $c - 1$ mora biti djeljiv sa 5 i broj c mora biti višekratnik brojeva 2 i 3, a najmanji prirodan broj koji to zadovoljava je $c = 6$. Dakle, broj $n = 2^{15}3^{10}5^6$ je traženi broj.

Zadatak 3.2.13. *Dokažite da postoji jedinstveni prirodan broj n takav da je $2^8 + 2^{11} + 2^n$ potpuni kvadrat.*

Rješenje:
Pretpostavimo da je $m \in \mathbb{N}$ takav da je $m^2 = 2^8 + 2^{11} + 2^n$. Tada je

$$2^n = m^2 - 2^8 - 2^{11} = m^2 - 2304 = m^2 - 48^2 = (m - 48)(m + 48).$$

Zbog jedinstvene faktorizacije, postoje nenegativni cijeli brojevi s i t takvi da vrijedi

$$m - 48 = 2^s, \quad m + 48 = 2^t, \quad s + t = n.$$

Stoga je $m = 2^s + 48$ i $m = 2^t - 48$, pa slijedi

$$\begin{aligned} 2^s + 48 &= 2^t - 48, \\ 2^t - 2^s &= 96, \\ 2^s(2^{t-s} - 1) &= 3 \cdot 2^5. \end{aligned}$$

Kako je broj $2^{t-s} - 1$ neparan, slijedi da je $2^{t-s} - 1 = 3$, a $2^s = 2^5$. Dakle, $s = 5$, pa imamo $2^{t-5} = 4 = 2^2$, odnosno $t = 7$, a $n = 12$.

3.3 Kongruencije

Teoriju kongruencija, poznatu i pod nazivom modularna aritmetika, uveo je Carl Friedrich Gauss u svom djelu *Disquisitiones Arithmeticae* objavljenom 1801. godine.

Parnost cijelog broja nam govori u kakvom je odnosu taj broj s brojem 2, tj. cijeli broj je paran ili neparan prema tome je li njegov ostatak pri dijeljenju s 2 jednak 0 ili 1. Ova formulacija parnosti čini prirodnim generaliziranje ideje na sljedeći način:

Za zadani cijeli broj $n \geq 2$, skup cijelih brojeva dijelimo u "klase kongruencije" prema njihovim ostatcima pri dijeljenju s n, tj. dva cijela broja smještamo u istu klasu kongruencije ako imaju isti ostatak pri dijeljenju brojem n.

Na primjer, za $n = 4$, skup cijelih brojeva je podijeljen u 4 disjunktna skupa označena mogućim ostatcima $0, 1, 2, 3$.

Za proizvoljan cijeli broj n, postojat će n klasa kongruencije, označenih mogućim ostatcima $0, 1, 2, \ldots, n-1$.

Definicija 3.3.1. *Za dva cijela broja x i y kažemo da je x* kongruentan *y modulo n i pišemo*

$$x \equiv y \pmod{n},$$

ako svaki od njih ima isti ostatak pri dijeljenju brojem n, odnosno ako je $x - y$ djeljivo s n. U protivnom, kažemo da x nije kongruentan y modulo n i pišemo $x \not\equiv y \pmod{n}$.

Kako je $x - y$ djeljivo s n ako i samo ako je djeljivo s $-n$, bez smanjenja općenitosti možemo promatrati samo pozitivne module.

Propozicija 3.3.1. *Relacija "biti kongruentan modulo n" je relacija ekvivalencije na skupu $\mathbb{Z}$, tj. za cijele brojeve x, y, z vrijedi:*
(i) $x \equiv x \pmod{n}$, *(refleksivnost)*
(ii) $x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$, *(simetričnost)*
(iii) $[x \equiv y \pmod{n} \,\&\, y \equiv z \pmod{n}\,] \Rightarrow x \equiv z \pmod{n}$. *(tranzitivnost)*

Zadatak 3.3.2. *Dokažite da svaki podskup od 55 brojeva odabranih iz skupa* $\{1, 2, \ldots, 100\}$ *mora sadržavati dva broja koja se razlikuju za 9.*

Rješenje:

Ako se dva broja razlikuju za 9, tada su oni u istoj klasi kongruencije modulo 9. Jaka forma Dirichletovog principa glasi: *Ako je m predmeta razmješteno u n kutija, onda barem jedna kutija sadrži $\lfloor \frac{m-1}{n} \rfloor + 1$ predmet, gdje je $x \mapsto \lfloor x \rfloor$ funkcija koja realnom broju x pridružuje najveći cijeli broj koji nije veći od x.* Dakle,

$$\left\lfloor \frac{55-1}{9} \right\rfloor + 1 = 6 + 1 = 7$$

brojeva od odabranih 55, nalazi se u istoj klasi kongruencije. Neka su $a_1, \ldots, a_7$ odabrani brojevi i pretpostavimo da vrijedi $a_1 < a_2 < a_3 < \ldots < a_7$. Budući da je $a_{i+1} \equiv a_i \pmod{9}$, $a_{i+1} - a_i \in \{9, 18, \ldots\}$ tvrdimo da je $a_{i+1} - a_i = 9$ za neki i. Ako to ne bi vrijedilo, tada bi za svaki i, $a_{i+1} - a_i \geq 18$, a to bi značilo da je $a_7 - a_1 \geq 6 \cdot 18 = 108$, što je nemoguće jer je $a_7 - a_1 < 100$. Dakle, dva elementa iz $a_1, \ldots, a_7$ se razikuju za 9.

U idućoj propoziciji navodimo osnovna svojstva kongruencija.

Propozicija 3.3.3. *Neka su x, y, u, v cijeli brojevi. Tada vrijedi:*
(i) Ako je $x \equiv y \pmod{n}$ i $u \equiv v \pmod{n}$, onda je $x + u \equiv y + v \pmod{n}$, $x - u \equiv y - v \pmod{n}$, $xu \equiv yv \pmod{n}$.
(ii) Ako je $x \equiv y \pmod{n}$ i $v \mid n$, onda je $x \equiv y \pmod{v}$.
(iii) Ako je $x \equiv y \pmod{n}$, onda je $xu \equiv yu \pmod{nu}$ za svaki $u \neq 0$.

Dokaz. (i) Neka je $x - y = nk$ i $u - v = nl$ gdje su $k, l \in \mathbb{Z}$. Tada je $(x + u) - (y + v) = n(k + l)$ i $(x - u) - (y - v) = n(k - l)$, pa je $x + u \equiv y + v \pmod{n}$ i $x - u \equiv y + v \pmod{n}$. Zbog $xu - yv = x(u - v) + v(x - y) = xnl + vnk = n(xl + vk)$ slijedi da je $xu \equiv yv \pmod{n}$.
(ii) Neka je $n = ve, e \in \mathbb{Z}$. Tada iz $x - y = nk$ slijedi $x - y = v \cdot ek$, pa je $x \equiv y \pmod{v}$.
(iii) Iz $x - y = nk$ slijedi $xu - yu = nu \cdot k$, pa je $xu \equiv yu \pmod{nu}$. □

Ova svojstva nam omogućuju da izvodimo aritmetiku radeći isključivo s ostatcima po modulo n.

Zadatak 3.3.4. *Neka je $N = 522 \cdot 131 + 211 \cdot 417 + 613 \cdot 919$. Bez računanja broja N, odredite:*
(a) parnost broja N,
(b) znamenku jedinice broja N,
(c) ostatak pri dijeljenju broja N brojem 7.

Rješenje: Primjenjujemo propoziciju 3.3.3.
(a) Imamo

$$522 \cdot 131 + 211 \cdot 417 + 613 \cdot 919 \equiv 0 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 \equiv 2 \equiv 0 \pmod{2}.$$

(b) Znamenka jedinice broja N je upravo ostatak pri dijeljenju broja N s 10. Zato je

$$522 \cdot 131 + 211 \cdot 417 + 613 \cdot 919 \equiv 2 \cdot 1 + 1 \cdot 7 + 3 \cdot 9 \equiv 2 + 7 + 27 \equiv 6 \pmod{10}.$$

(c) Slično kao u (a) i (b) dijelu zadatka, računamo N modulo 7

$$522 \cdot 131 + 211 \cdot 417 + 613 \cdot 919 \equiv 4 \cdot 5 + 1 \cdot 4 + 4 \cdot 2 \equiv 20 + 4 + 8 \equiv 32 \equiv 4 \pmod{7}.$$

Dakle, ostatak pri dijeljenju broja N brojem 7 je 4.

Uzastopnom primjenom propozicije 3.3.3 svojstva (i) slijedi:

Korolar 3.3.5. *Neka je P polinom s cjelobrojnim koeficijentima. Ako je $x \equiv y \pmod{n}$, onda je $P(x) \equiv P(y) \pmod{n}$.*

U modularnoj aritmetici, operacije zbrajanja, oduzimanja i množenja ponašaju se kao u običnoj aritmetici, naravno s obzirom na modulo koji razmatramo. A što je s operacijom dijeljenja? O tome nam govori sljedeća propozicija.

Propozicija 3.3.6. *Neka su $a, x, y \in \mathbb{Z}$ i $n \in \mathbb{N}$. Tada vrijedi $ax \equiv ay \pmod{n}$ ako i samo ako je $x \equiv y \pmod{\frac{n}{D(a,n)}}$. Specijalno, ako je $ax \equiv ay \pmod{n}$ i $D(a, n) = 1$, onda je $x \equiv y \pmod{n}$.*

Zadatak 3.3.7. *Neka su x i y cijeli brojevi. Dokažite da je $2x+3y$ djeljivo sa 17 ako i samo ako je $9x + 5y$ djeljivo sa 17.*

Rješenje:
Trebamo pokazati da je $2x + 3y \equiv 0 \pmod{17}$ ako i samo ako je $9x + 5y \equiv 0 \pmod{17}$. Da bismo to pokazali, trebamo pomnožiti kongruenciju $2x + 3y \equiv 0 \pmod{17}$ odgovarajućom konstantom tako da ju transformiramo u kongruenciju $9x + 5y \equiv 0 \pmod{17}$. Dakle, pitamo se postoji li konstanta c takva da vrijedi $c(2x + 3y) \equiv 9x + 5y \pmod{17}$? Da bi bilo zadovoljeno $9 \equiv 2c \pmod{17}$ možemo uzeti $c = 13$. Sada iz $2x + 3y \equiv 0 \pmod{17}$ slijedi

$$\begin{aligned} 13(2x + 3y) &\equiv 0 \pmod{17}, \\ 26x + 39y &\equiv 0 \pmod{17}, \\ 9x + 5y &\equiv 0 \pmod{17}. \end{aligned}$$

Obrnuto, pitamo se postoji li konstanta c takva da vrijedi $c(9x + 5y) \equiv 2x + 3y \pmod{17}$? Da bi vrijedilo $2 \equiv 9c \pmod{17}$ možemo uzeti $c = 4$. Sada iz $9x + 5y \equiv 0 \pmod{17}$ slijedi

$$\begin{aligned} 4(9x + 5y) &\equiv 0 \pmod{17}, \\ 36x + 20y &\equiv 0 \pmod{17}, \\ 2x + 3y &\equiv 0 \pmod{17}. \end{aligned}$$

Zadatak 3.3.8. *Koje su posljednje dvije znamenke broja 3^{1234}?*

Rješenje:
Da bi izračunali koje su posljednje dvije znamenke broja 3^{1234}, trebamo izračunati 3^{1234} modulo 100. Postoji mnogo načina na koje možemo zapisati 3^{1234} pomoću potencije broja 3. Promatrajmo neke potencije broja 3 kako bismo došli do one koja ima što je moguće manji ostatak pri dijeljenju sa 100. Imamo,

$$3^2 \equiv 9 \pmod{100}, \quad 3^4 \equiv 81 \pmod{10}, \quad 3^8 = 3^4 \cdot 3^4 \equiv 81 \cdot 81 \equiv 61 \pmod{100},$$

$$3^{10} = 3^2 \cdot 3^8 \equiv 9 \cdot 61 \equiv 49 \pmod{100}, \quad 3^{20} = 3^{10} \cdot 3^{10} \equiv 49 \cdot 49 \equiv 1 \pmod{100}.$$

Sada vidimo da je dobro da se u rastavu broja 1234 pojavljuje 20. Broj 1234 zapišemo kao $1234 = 20 \cdot 61 + 14$, pa imamo

$$3^{1234} = \left(3^{20}\right)^{61} \cdot 3^{14} \equiv 1^{61} \cdot 3^{14} \equiv 3^4 \cdot 3^{10} \equiv 81 \cdot 49 \equiv 69 \pmod{100}.$$

Dakle, posljednje dvije znamenke broja 3^{1234} su 69.

Zadatak 3.3.9. *Pokažite da postoji pozitivni višekratnik broja* 21 *koji ima posljednje tri znamenke jednake* 241.

Rješenje:
Moramo dokazati da postoji prirodan broj n takav da vrijedi

$$21n \equiv 241 \pmod{1000}.$$

Kako su brojevi 21 i 1000 relativno prosti, postoje cijeli brojevi s i t takvi da vrijedi

$$21s + 1000t = 1.$$

Pomnožimo svaku stranu gornje jednakosti s 241 i zapišimo ju na sljedeći način

$$21(241s) - 241 = -241 \cdot 1000t.$$

Zapišimo sada posljednju jednakost u obliku kongruencije

$$21 \cdot 241s \equiv 241 \pmod{1000}.$$

Ako je s pozitivan, stavimo $n = 241s$ i pokazali smo traženo. Ako s nije pozitivan, neka je $n = 241s + 1000k$, gdje je $k \in \mathbb{N}$ dovoljno veliki da n bude pozitivan (odabirom broja k na odgovarajući način možemo pretpostaviti da je n između 0 i 1000). Zbog toga slijedi

$$21n \equiv 21(241s + 1000k) \equiv 21 \cdot 241s \equiv 241 \pmod{1000},$$

tj. pokazali smo da višekratnik broja 21 ima posljednje tri znamenke 241.

Zadatak 3.3.10. *Pokažite da za bilo koji skup od n cijelih brojeva, postoji njegov podskup čiji je zbroj svih članova djeljiv s n.*

Rješenje:
Neka je zadan skup $S = \{x_1, \ldots, x_n\}$. Definiramo

$$y_1 = x_1, \quad y_2 = x_1 + x_2, \ldots, \quad y_n = x_1 + x_2 + \ldots + x_n.$$

Ako je $y_i \equiv 0 \pmod{n}$ za neki i, gotovi smo pa pretpostavimo da to nije slučaj. Tada imamo n brojeva $y_1, \ldots, y_n$ i $n-1$ klasa kongruencije modulo n, pa prema Dirichletovom principu slijedi da dva od y_i-eva moraju biti kongruentni jedan drugom po modulo n. Pretpostavimo da je $y_i \equiv y_j \pmod{n}$ za neke i, j takve da je $i < j$. Tada slijedi

$$x_{i+1} + \ldots + x_j \equiv y_j - y_i \equiv 0 \pmod{n},$$

i zadatak je riješen.

Zadatak 3.3.11. *Dokažite: ako su* $2n+1$ *i* $3n+1$ *potpuni kvadrati, tada je n djeljiv s* 40.

Rješenje:
Dovoljno je dokazati da je n višekratnik brojeva 5 i 8, odnosno da je $n \equiv 0 \pmod{5}$ i $n \equiv 0 \pmod{8}$.

Promotrimo ostatke pri dijeljenju s 5. Sljedeća tablica pokazuje da potpuni kvadrat može biti 0, 1 ili 4 modulo 5:

$x \pmod{5}$	0	1	2	3	4
$x^2 \pmod{5}$	0	1	4	4	1

Sada imamo:

$$\begin{aligned}
2n+1 \equiv 0 \pmod{5} &\implies n \equiv 2 \pmod{5}\\
2n+1 \equiv 1 \pmod{5} &\implies n \equiv 0 \pmod{5}\\
2n+1 \equiv 4 \pmod{5} &\implies n \equiv 4 \pmod{5}\\
3n+1 \equiv 0 \pmod{5} &\implies n \equiv 3 \pmod{5}\\
3n+1 \equiv 1 \pmod{5} &\implies n \equiv 0 \pmod{5}\\
3n+1 \equiv 4 \pmod{5} &\implies n \equiv 1 \pmod{5}
\end{aligned}$$

Dakle, jedina mogućnost da su i $2n+1$ i $3n+1$ potpuni kvadrati je $n \equiv 0 \pmod{5}$, odnosno n je višekratnik broja 5.

Promotrimo sada ostatke pri dijeljenju s 8. Sljedeća tablica pokazuje da potpuni kvadrat može biti 0, 1 ili 4 modulo 8:

$x \pmod{8}$	0	1	2	3	4	5	6	7
$x^2 \pmod{8}$	0	1	4	1	0	1	4	1

Kako je $2n+1$ potpun kvadrat, možemo ga zapisati kao $2n+1 = a^2$, odnosno $2n = a^2 - 1 = (a-1)(a+1)$. Brojevi $a-1$ i $a+1$ su parni jer je a neparan, pa slijedi $2n \equiv 0 \pmod 4$, odnosno $n \equiv 0 \pmod 2$. Dakle, broj n je paran. Sada imamo:

$$\begin{aligned} 2n+1 \equiv 1 \pmod 8 &\implies n \equiv 0 \pmod 8 \\ 3n+1 \equiv 0 \pmod 8 &\implies n \equiv 5 \pmod 8 \\ 3n+1 \equiv 1 \pmod 8 &\implies n \equiv 0 \pmod 8 \\ 3n+1 \equiv 4 \pmod 8 &\implies n \equiv 1 \pmod 8 \end{aligned}$$

Za $2n+1 \equiv 0, 4 \pmod 8$ ne postoji takav n jer je $2n+1$ neparan. Dakle, jedina mogućnost je opet $n \equiv 0 \pmod 8$, odnosno n je višekratnik broja 8. Konačno, n je djeljiv s 40.

Prije nego što pokažemo što su i kako se rješavaju linearne kongruencije, definirajmo potpuni sustav ostataka modulo m ([2]).

Defincija 3.3.12. *Skup $x_1, \ldots, x_m$ se zove potpuni sustav ostataka modulo m ako za svaki $y \in \mathbb{Z}$ postoji točno jedan x_j takav da je $y \equiv x_j \pmod m$. Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo m uzmemo po jedan član.*

Jasno je da postoji beskonačno mnogo potpunih sustava ostataka modulo m. U ovom radu koristit ćemo *sustav najmanjih nenegativnih ostataka* $\{0, 1, \ldots, m-1\}$.

Neka je P polinom s cjelobrojnim koeficijentima. Rješenje kongruencije $P(x) \equiv 0 \pmod n$ je svaki cijeli broj x koji je zadovoljava.

Ako je x_1 neko rješenje kongruencije $P(x) \equiv 0 \pmod n$ i vrijedi $x_2 \equiv x_1 \pmod n$, po korolaru 3.3.5 slijedi da je i x_2 rješenje te kongurencije. Takva dva rješenja x_1 i x_2 zovemo *ekvivalentnim rješenjima* i ima ih beskonačno mnogo. Zato ćemo reći da je broj rješenja kongurencije broj neekvivalentnih rješenja.

Kongurenciju oblika $ax \equiv b \pmod n$ nazivamo **linearna kongruencija**. Sljedeći teorem govori nam o njenoj rješivosti, te opisuje skup njenih rješenja ako je rješiva [2].

Teorem 3.3.13. *Neka su $a, n \in \mathbb{N}$ i $b \in \mathbb{Z}$. Kongruencija*

$$ax \equiv b \pmod n \tag{3.5}$$

ima rješenja ako i samo ako $d = D(a, n)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda kongruencija (3.5) ima točno d rješenja modulo n.

Iz teorema 3.3.13 slijedi da ako je p prost broj i a nije djeljiv s p, tada kongruencija $ax \equiv b \pmod p$ uvijek ima jedinstveno rješenje.

Linearnu kongruenciju $ax \equiv b \pmod{n}$, rješavamo pomoću *Algoritma za rješavanje linearnih kongurencija*. Najprije odredimo $d = D(a, n)$ pomoću Euklidovog algoritma te ako d dijeli b tada kongruencija $ax \equiv b \pmod{n}$ ima rješenja. Dakle, početna kongruencija ekvivalentna je $a'x \equiv b' \pmod{n'}$, gdje su $a' = \frac{a}{d}, b' = \frac{b}{d}, n' = \frac{n}{d}$. Sada je $D(a', n') = 1$, pa prema Bezoutovom identitetu (3.3) postoje brojevi $u, v \in \mathbb{Z}$ takvi da vrijedi $a'u + n'v = 1$ i pronalazimo ih pomoću proširenog Euklidovog algoritma. Uočimo, ako pomnožimo $a'u + n'v = 1$ s b', dobivamo $a'(ub') + n'(vb') = b'$, odnosno $a'(ub') \equiv b' \pmod{n'}$ i vidimo da zapravo ni ne trebamo tražiti v u proširenom Euklidovom algoritmu, ali moramo pripaziti da je uvijek $a' < n'$. Rješenje kongruencije $a'x \equiv b' \pmod{n'}$ je $x \equiv ub' \pmod{n'}$, odnosno brojevi oblika $ub' + kn', k \in \mathbb{Z}$.

Pokažimo sada primjenu ovog algoritma na primjeru.

Zadatak 3.3.14. *Riješite kongruenciju* $589x \equiv 209 \pmod{817}$.

Rješenje:
Najprije odredimo $d = D(589, 817)$ pomoću Euklidovog algoritma.

$$\begin{aligned} 817 &= 1 \cdot 589 + 228, \\ 589 &= 2 \cdot 228 + 133, \\ 228 &= 1 \cdot 133 + 95, \\ 133 &= 1 \cdot 95 + 38, \\ 95 &= 2 \cdot 38 + 19, \\ 38 &= 2 \cdot 19. \end{aligned}$$

Vidimo da ćemo imati 5 koraka u proširenom Euklidovom algoritmu i da je $d = 19$. Sada, $19 \mid 209$ pa je kongruencija $589x \equiv 209 \pmod{817}$ rješiva. Dakle, početnu kongurenciju dijelimo s 19 i dobivamo njoj ekvivalentnu

$$31x \equiv 11 \pmod{43}.$$

Vrijedi $D(31, 43) = 1$, pa je njezino rješenje jedinstveno, dok početna kongruencija ima 19 rješenja modulo 817. Pronađimo $u \in \mathbb{Z}$ pomoću proširenog Euklidovog algoritma.

i	-1	0	1	2	3	4	5
q_i			1	2	1	1	2
u_i	0	1	-1	3	-4	7	-18

Dakle, $u = -18$ pa imamo

$$31(-18 \cdot 11) \equiv 11 \pmod{43},$$

odnosno $31(-198) \equiv 11 \pmod{43}$, a kako je $-198 \equiv 17 \pmod{43}$, slijedi da je rješenje

$$x \equiv 17 \pmod{43},$$

a to su svi brojevi oblika $17 + 43k, k \in \mathbb{Z}$. Konačno, zadana kongruencija ima 19 rješenja i to su

$$x \equiv 17, 60, 103, 146, 189, 232, 275, 318, 361, 404, 447, 490, 533, 576, 619, 662, 705, 748, 791 \pmod{817}.$$

Teorem 3.3.15 (Kineski teorem o ostatcima)**.** *Ako su m i n relativno prosti prirodni brojevi, a a i b proizvoljni cijeli brojevi, tada postoji cijeli broj x takav da vrijedi*

$$x \equiv a \pmod{m},$$

$$x \equiv b \pmod{n}.$$

Općenito, ako su $m_1, m_2, \dots, m_k$ *u parovima relativno prosti prirodni brojevi, a* $a_1, a_2, \dots, a_k$ *proizvoljni cijeli brojevi, tada postoji cijeli broj x takav da vrijedi*

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, \dots, k,$$

odnosno sustav kongruencija

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \dots, \quad x \equiv a_k \pmod{m_k} \tag{3.6}$$

ima rješenje. Ako je x_0 *jedno rješenje gornjeg sustava kongruencija, onda su sva rješenja dana sa* $x \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$.

Dokaz. Promotrimo sljedećih n brojeva $a, a + m, a + 2m, \dots, a + (n - 1)m$. Svaki od njih je kongruentan s a modulo m. Štoviše, nijedan od njih dva nije kongruentan po modulu n. Zaista, ako je $a + im \equiv a + jm \pmod{n}, 0 \leq i < j < n$, tada je $(i - j)m \equiv 0 \pmod{n}$. Ali m i n su relativno prosti pa posljednja kongruencija vrijedi ako n dijeli $i - j$. Međutim, $i - j$ ne može biti višekratnik broja n zbog ograničenja na i i j pa slijedi $i = j$. Dakle, brojevi $a, a + m, a + 2m, \dots, a + (n - 1)m$ su nekim redoslijedom kongruentni brojevima $0, 1, 2, \dots, n - 1$ modulo n. Prema tome, za neki i vrijedi $a + mi \equiv b \pmod{n}$. Dokaz prvog dijela teorema je gotov ako stavimo $x = a + mi$.

Dokažimo sada drugu tvrdnju teorema. Dokaz će ujedno biti algoritam za rješavanje sustava kongruencija ([2]).

Definirajmo broj m kao umnožak modula iz sustava kongruencija (3.6), $m := m_1 \cdot m_2 \cdots m_r$, te neka je $n_j = \frac{m}{m_j}$, $j = 1, \ldots, r$. Linearna kongruencija $n_j x \equiv a_j \pmod{m_j}$ sigurno ima rješenje jer je $D(n_j, m_j) = 1$ i ono je jedinstveno (u potpunom sustavu ostataka modulo n_j). Neka je $x_j \in \mathbb{Z}$ takav da vrijedi $n_j x_j \equiv a_j \pmod{m_j}$, $j = 1, \ldots, r$. Definirajmo broj

$$x_0 := n_1 x_1 + n_2 x_2 + \ldots + n_r x_r.$$

Tada vrijedi $x_0 = 0 + \ldots + 0 + n_j x_j + 0 + \ldots + 0 \equiv a_j \pmod{m_j}$, dakle, x_0 je rješenje sustava.

Pretpostavimo da su $x, y \in \mathbb{Z}$ dva rješenja sustava. Onda je $x \equiv y \pmod{m_j}$ za svaki $j = 1, \ldots, r$. Kako su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti, onda mora vrijediti da je $x \equiv y \pmod{m}$. □

U sljedeća dva zadatka primjenjujemo algoritam iz dokaza teorema 3.3.15.

Zadatak 3.3.16. *Riješite sustav kongruencija*

$$x \equiv 4 \pmod{11}, \quad x \equiv 5 \pmod{16}, \quad x \equiv 6 \pmod{23}. \tag{3.7}$$

Rješenje:

Brojevi $m_1 = 11, m_2 = 16, m_3 = 23$ su u parovima relativno prosti pa možemo primijeniti teorem 3.3.15. Tada je $m = 11 \cdot 16 \cdot 23 = 4048$ i $n_1 = 16 \cdot 23, n_2 = 11 \cdot 23, n_3 = 11 \cdot 16$. Sada imamo tri linearne kongruencije koje rješavamo uvrštavanjem potpunog sustava najmanjih nenegativnih ostataka modulo m_j, $j = 1, 2, 3$, proširenim Euklidovim algoritmom ili transformacijama kongruencije .

(1) $16 \cdot 23x \equiv 4 \pmod{11} \iff 5x \equiv 4 \pmod{11}$. Potpuni sustav ostataka modulo 11 je $\{0, 1, \ldots, 10\}$ te ih redom uvrštavamo i dobivamo da je $x_1 = 3$.

(2) $11 \cdot 23x \equiv 5 \pmod{16} \iff 13x \equiv 5 \pmod{16}$. Ovu linearnu kongruenciju riješit ćemo pomoću proširenog Euklidovog algoritma. Brojevi 13 i 16 su relativno prosti pa postoje $u, v \in \mathbb{Z}$ takvi da je $13 \cdot u + 16 \cdot v = 1$. Euklidovim algoritmom dobivamo

$$\begin{aligned} 16 &= 1 \cdot 13 + 3, \\ 13 &= 4 \cdot 3 + 1, \\ 3 &= 3 \cdot 1, \end{aligned}$$

odnosno u proširenom Euklidovom algoritmu imamo dva koraka i dobivamo

i	-1	0	1	2
q_i			1	4
u_i	0	1	-1	5

Dakle, dobili smo $13 \cdot 5 \equiv 1 \pmod{16}$, proširimo sve s 5 jer to tražimo i dobivamo $13 \cdot 25 \equiv 5 \pmod{16}$ što je ekvivalentno $13 \cdot 9 \equiv 5 \pmod{16}$, tj. $x_2 = 9$.

(3) $11 \cdot 16x \equiv 6 \pmod{23}$. Ovu kongruenciju možemo podijeliti s 2 jer je $D(2, 23) = 1$, pa je $11 \cdot 8x \equiv 3 \pmod{23}$, što je ekvivalentno $19x \equiv 3 \pmod{23}$. Sada zbog $19 \equiv -4 \pmod{23}$ i $3 \equiv -20 \pmod{23}$, imamo $x \equiv 5 \pmod{23}$, tj. $x_3 = 5$.

Sada možemo formirati broj $x_0 = 16 \cdot 23 \cdot 3 + 11 \cdot 23 \cdot 9 + 11 \cdot 16 \cdot 5 = 4261 \equiv 213 \pmod{4048}$. Konačno, sva rješenja sustava (3.7) su $x \equiv 213 \pmod{4048}$, odnosno skup svih cijelih brojeva oblika $x = 213 + 4048k, k \in \mathbb{Z}$.

Zadatak 3.3.17. *Riješite sustav kongruencija*

$$x \equiv 5 \pmod{6}, \quad x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15}. \tag{3.8}$$

Rješenje:
Uočimo da brojevi 6, 10, 15 nisu u parovima relativno prosti pa ne možemo direktno primijeniti teorem 3.3.15. Zadani sustav ekvivalentan je sustavu

$$x \equiv 5 \pmod{2}, \quad x \equiv 3 \pmod{2}, \quad x \equiv 8 \pmod{3},$$

$$x \equiv 5 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 8 \pmod{5}.$$

Dakle, moduli su potencije prostih brojeva te sada usporedimo kongruencije koje odgovaraju istom prostom broju

$$\begin{aligned} x \equiv 5 \pmod{2}, \quad x \equiv 3 \pmod{2} \quad &\Leftrightarrow \quad x \equiv 1 \pmod{2}, \\ x \equiv 5 \pmod{3}, \quad x \equiv 8 \pmod{3} \quad &\Leftrightarrow \quad x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \quad x \equiv 8 \pmod{5} \quad &\Leftrightarrow \quad x \equiv 3 \pmod{5}. \end{aligned}$$

Prema tome, zadani sustav (3.8) ekvivalentan je sustavu

$$x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5},$$

gdje su 2, 3, 5 u parovima relativno prosti prirodni brojevi. Sada možemo primijeniti teorem 3.3.15. Tada je $m = 2 \cdot 3 \cdot 5 = 30$, te $n_1 = \frac{30}{2} = 15, n_2 = \frac{30}{3} = 10, n_3 = \frac{30}{5} = 6$, pa imamo

$$15x \equiv 1 \pmod{2} \Leftrightarrow x \equiv 1 \pmod{2} \Rightarrow x_1 = 1,$$

$$10x \equiv 2 \pmod{3} \Leftrightarrow x \equiv 2 \pmod{3} \Rightarrow x_2 = 2,$$

$$6x \equiv 3 \pmod{5} \Leftrightarrow x \equiv 3 \pmod{5} \Rightarrow x_3 = 3.$$

Ovdje je $x_0 = 15 \cdot 1 + 10 \cdot 2 + 6 \cdot 3 \equiv 23 \pmod{30}$, dakle, rješenje zadanog sustava kongruencija je

$$x \equiv 23 \pmod{30},$$

odnosno skup svih cijelih brojeva oblika $x = 23 + 30k, k \in \mathbb{Z}$.

Bibliografija

[1] Lj. Arambašić, *Linearna algebra*, Element, Zagreb, 2022.

[2] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[3] Z. Dekanić, S. Varošanec *Dokazi i primjene AG nejednakosti*, Hrvatski matematički elektronički časopis *math.e* (listopad 2006.), br. 9, dostupno na http://e.math.hr/old/indexno9.html (rujan 2022.)

[4] A. Engel, *Problem-Solving Strategies*, Springer, New York, 2009.

[5] I. Ilišević, *Geometrijski dokaz nejednakosti sredina*, Matematika i škola, 2007., 218. str.

[6] Z. Kurnik, *Matematički zadatak*, Matematika i škola 2 (2000.), br. 7, 51-58.

[7] Z. Kurnik, *Problemska nastava*, Matematika i škola 15 (2002.), br. 2, 196-202.

[8] Z. Kurnik, *Nejednakosti*, Hrvatsko matematičko društvo, Zagreb, 2004.

[9] Z. Kurnik, *Heuristička nastava*, Matematika i škola 34 (2006.), br. 2, 148-153.

[10] Z. Kurnik, *Znanstveni okviri nastave matematike*, Element, Zagreb, 2009.

[11] Z. Kurnik, *Posebne metode rješavanja matematičkih problema*, Element, Zagreb, 2010.

[12] L. Larson, *Problem-Solving Through Problems*, Springer-Verlag, New York, 1983.

[13] J. Pečarić, *Nejednakosti*, Hrvatsko matematičko društvo, Zagreb, 1996.

[14] G. Pólya, *Kako ću riješiti matematički zadatak*, Školska knjiga, Zagreb, 1966.

[15] *Matematička natjecanja*, dostupno na https://natjecanja.math.hr/ (rujan 2022.).

Sažetak

Ovaj diplomski rad sastavljen je od tri poglavlja s naslovima Rješavanje matematičkih problema, Nejednakosti i Aritmetika.

Prvo poglavlje započinje opisom pojma matematički problem te nekoliko različitih klasifikacija matematičkog zadatka. Opisan je nastavni sustav problemska nastava te su prezentirane smjernice za izvođenje nastavnog sata ovog tipa. Ukratko je opisana i metoda rješavanja matematičkog problema koju je predstavio George Pólya u svom djelu *Kako ću riješiti matematički zadatak*. Na kraju poglavlja proučen je i nastavni sustav heuristička nastava te su nabrojane i opisane heuristike koje se koriste za rješavanje matematičkih problema.

U drugom i trećem poglavlju rješavaju se matematički problemi iz područja nejednakosti i aritmetike. Prije rješavanja navedenih problema, potrebno je prisjetiti se nekoliko najvažnijih i najpoznatijih teorema iz ovog područja. Među njima su Cauchy-Schwarzova nejednakost te nejednakosti između aritmetičke, geometrijske, kvadratne i harmonijske sredine brojeva. Nadalje, nakon prisjećanja osnovnih pojmova vezanih za djeljivost brojeva, teorema o dijeljenju s ostatkom i Euklidovog algoritma, dokazan je osnovni teorem aritmetike te uveden pojam kongruencije i dokazan kineski teorem o ostatcima.

Time su usvojene određene tehnike koje omogućuju da se zadaci koji su možda teško rješivi, riješe na znatno jednostavniji način.

Summary

This master thesis is composed of three chapters with the titles Solving Mathematical Problems, Inequalities and Arithmetic.

The first chapter begins with a description of the term mathematical problem and several different classifications of a mathematical task. The problem-based teaching method is described and the guidelines for performing this type of lessons are presented. Also, the method of solving a mathematical problem, presented by George Pólya in his book *How to solve it*, is briefly described. At the end of the chapter, the heuristic teaching method is explained, and the heuristics used to solve mathematical problems are listed and described.

In the second and third chapters, mathematical problems in the field of inequality and arithmetic are solved. Before solving the mentioned problems, it is necessary to recall several of the most important and well-known theorems in these fields. Among them are the Cauchy-Schwarz inequality and inequalities between arithmetic, geometric, quadratic and harmonic means of numbers. Furthermore, after summarizing the basic concepts related to the divisibility of numbers, the divison theorem and Euclidean algorithm, the fundamental theorem of arithmetic was proved, the concept of congruences was introduced and the Chinese remainder theorem was proved.

Thereby, certain techniques have been mastered, which enable mathematical tasks that may be difficult and demanding to solve, to be solved in a much simpler way.

Životopis

Anja Posel rođena je 31. kolovoza 1995. godine u Čakovcu. Svoje djetinjstvo provela je u općini Gornji Mihaljevec gdje je 2002. godine upisala Osnovnu školu Gornji Mihaljevec. Školovanje je nastavila u Čakovcu gdje je 2010. godine upisala Gimnaziju Josipa Slavenskog Čakovec. Srednjoškolsko obrazovanje završila je 2014. godine te je iste godine upisala preddiplomski studij nastavničkog smjera na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Po završetku preddiplomskog studija 2019. godine, na istom fakultetu upisala je diplomski studij matematike nastavničkog smjera.