UNIVERZITET U BEOGRADU

MATEMATIČKI FAKULTET

ČETIRI ETAPE REŠAVANJA ZADATAKA IZ ELEMENTARNE TEORIJE BROJEVA

MASTER RAD

Autor
Tijana Spasić

Mentor
Nebojša Ikodinović

Beograd
Mart, 2017.

Sadržaj

Predgovor

Poznate etape rešavanja konstruktivnih zadataka (analiza, konstrukcija, dokaz i diskusija), na kojima se insistira u nastavi geometrije, na svim nivoima, potiču od davnina. U čuvenoj knjizi Papposa Aleksandrijskog (300. god.) „Riznica analize“ detaljno su opisane analiza i sinteza, i predložene opšte etape rešavanja bilo kog problema: 1) analiza problema, 2) rešenje problema (sinteza), 3) provera korektnosti rešenja i 4) diskusija. Za to doba, tipične probleme svakako su predstavljale geometrijske konstrukcije, pa je prirodno što je autor svoje opšte izlaganje ilustrovao ovakvim primerima. Nažalost, njegovi opšti saveti o rešavanju problema postali su uobičajeni samo u kontekstu navedenih primera. Svaka od navedenih etapa važna je pri rešavanju bilo kog matematičkog zadatka, te bi bilo veoma korisno tokom učenja matematike, u različitim kontekstima, isticati svaku od njih. Rešavanje zadataka „u etapama“ posebno treba potencirati u slučajevima kada zadaci nisu šablonski. Ovakvim zadacima obiluje elementarna teorija brojeva kojoj se u nastavi matematike posvećuje sve manje pažnje. Opšta je tendencija da se zadaci za koje ne postoje šabloni rešavanja proglase teškim i izbegavaju u redovnoj nastavi.

Ovaj rad će predstavljati zbirku raznovrsnih zadataka iz elementarne teorije brojeva koje će pratiti eksplicitno razdvojene i detaljno opisane četiri etape rešavanja:
1. Analiza: razmišljanje o onome što je dato i mogućim posledicama; o onome šta se traži i kako bi se do toga moglo stići; eventualna grafička reprezentacija zadatka; nagađanje mogućih strategija rešavanja dok se ne uoči ona prava.
2. Rešenje: ispisivanje korektnog rešenja na osnovu analize.
3. Dokaz/Provera: proveravanje korektnosti rešenja i detaljno razmatranje svakog koraka.
4. Diskusija: razmišljanje o raznim specijalnim slučajevima, o mogućim uopštenjima, o posledicama promene nekog od datih podataka itd.

Na časovima matematike uglavnom se insistira samo na rešenjima zadataka (na 2. etapi), po uzoru na udžbenike i zbirke zadataka, što u velikom broju slučajeva nije dovoljno za sticanje i podsticanje veštine rešavanja problema. Cilj rada jeste da, u slučaju elementarne teorije brojeva, ponudi opšte ideje i konkretne predloge kako bi se ovaj nedostatak mogao prevazići u školskoj praksi.

1 Pappus-ova riznica analize

Pappus iz Aleksandrije (290 g.p.n.e. - 350 g.p.n.e.) je bio jedan od poslednjih velikih matematičara Aleksandrijske škole i uopšte antičkog sveta. Iz njegovih dela saznajemo o dostignućima antičkih matematičara. O životu Pappusa se ne zna mnogo, osim ono što je sam zabeležio u svojim spisima, da je imao sina Hermodorusa i da je bio učitelj u Aleksandriji. Pappus je poznat po svom delu Kolekcija (Collectione, 340 g.p.n.e.) koja predstavlja zbornik matematike u osam tomova, od kojih je većina sačuvana. Ona obuhvata širok spektar tema kojima su se bavili najistaknutiji umovi toga vremena. Nije poznato čije sve radove je Pappus objedinio u svom delu, niti iz kog tačno perioda, ali se iz nekih izvora može zaključiti da su to dela nastala posle 411 g.p.n.e. a pre 168 g.p.n.e. Veliki značaj Kolekcije je što sadrži sistematski uređen prikaz najvažnijih rezultata do kojih su došli Pappusovi prethodnici i dodatna objašnjenja i proširenja tih otkrića. Pappusov način pisanja je jasan, sistematičan i oslobođen okova matematičkih formula i izraza. Nakon pominjanja u "Istoriji geometrijskih metoda"[1], Knjiga VII Pappusove Kolekcije izazvala je značajnu pažnju. Ova knjiga sadrži takozvanu "Riznicu analize" (u slobodnom prevodu "veština rešavanja zadataka" ili "heuristika"). U predgovoru knjige objašnjeni su pojmovi ANALIZE i SINTEZE, koje su po mišljenju mnogih najznačajnije metode u naučnim istraživanjima. Analiza uzima ono što se traži kao da je već nađeno i polazeći od toga dolazi do nečega što se uzima kao početak sinteze; jer u analizi uzimamo da je ono što se traži već učinjeno i pitamo se čija je to posledica, i opet šta je uzrok poslednjeg, i tako dalje sve dok idući ovakvim koracima ne stignemo do nečega što je već poznato ili što pripada klasi prvih načela. Ovakvu metodu nazivamo analizom kao rešavanje unazad. Sinteza je obrnut proces, u njoj uzimamo kao učinjeno to što je u analizi bilo poslednje dostignuto i sređujući u njihovom prirodnom poretku kao posledice ono što su pre bile pretpostavke i spajajući ih redom jednu za drugom konačno dolazimo do konstrukcije onoga što je bilo traženo; i to zovemo sintezom.


PAPPI
ALEXANDRINI
MATHEMATICAE
Collectiones.
A FEDERICO
COMMANDINO
VRBINATE
In Latinum Conuerſæ, & Commentarijs
Illuſtratæ.
VENETIIS,
Apud Franciſcum de Franciſcis Senenſem.
M. D. LXXXIX.

[1] M. Chasles, "Istorija geometrijskih metoda", Hayez, Brisel, 1837

2 Četiri faze rešavanja konstruktivnih zadataka iz geometrije

Geometrija je predivna i veoma primenljiva grana matematike. Trodimenzionalna. Po potrebi i n-dimenzionalna. Zahtevna po pitanju rešavanja kompleksnih problema konstrukcije figura na osnovu naizgled malog broja nepovezanih ulaznih podataka. Zar to nije ono što nam se svakodnevno dešava? Treba da osmislimo, konstruišemo rešenje, nađemo izlaz iz problema, na osnovu na prvi pogled veoma udaljenih i nepovezanih ulaznih podataka. Kako nam znanje iz geometrije može pomoći u tome?

Ispravno rešavanje geometrijskog konstruktivnog zadatka ima četiri etape:

1. Analiza – traženje puta kojim treba ići. Analiza je suštinski početak rešavanja. I tu postoji jedan trik. U analizi se obično pretpostavlja da je zadatak rešen, napravi se skica figure i onda se korak po korak, pomoćnim crtežima i razlaganjima dovode u vezu konačno rešenje i početne stavke. Zamislite da to primenjujemo u svakodnevnom životu, zamislimo da je problem rešen, zamislimo kako bi tada izgledao svet i okruženje i onda uspostavljamo veze između polaznih stavki i krajnjeg rešenja. Iznenadićete se kakvi su rezultati primene ovakvog načina razmišljanja u rešavanju drugih matematičkih problema koji nisu direktno u vezi sa geometrijom.

2. Konstrukcija – izrada na osnovu zaključaka iz analize. Konstrukcija nije ništa drugo do realizacija. Nužno je i neophodno da ono što zamislimo uspemo i praktično da izvedemo. Tu se testiraju naše ideje i neretko se dešava da se tokom konstrukcije moramo vratiti na analizu.

3. Dokaz/Provera/Rezime – potvrda da konstruisana figura zadovoljava postavljene uslove. Dokaz se uglavnom dosta oslanja na Analizu, jer se pri analiziranju mora voditi računa o osobinama figure. Za uspešan dokaz neophodno je poznavanje važnih teorema, ali i veština njihovog kombinovanja.

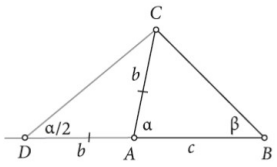
4. Diskusija – utvrđivanje uslova pod kojima je moguće izvršiti zadatu konstrukciju, kao i broja međusobno nepodudarnih figura koje zadovoljavaju te uslove. To je ujedno veza između postavke i krajnjeg rešenja i ne mora uvek da bude trivijalna.

Osnovne etape rešavanja složenijeg konstruktivnog zadatka su ilustrovane u sledećim primerima:

Primer 1.
Konstruišimo $\triangle ABC$ tako da je zbir stranica AB i AC podudaran datoj duži d, a uglovi kod temena A i B su podudarni datim uglovima α i β.

Analiza.

Nacrtajmo proizvoljan trougao ABC i označimo one njegove elemente koji se pojavljuju među datim podacima. Zadatak će biti rešen ako smislimo kako da „dopunimo" sliku i zadatak svedemo na neku jednostavniju konstrukciju.

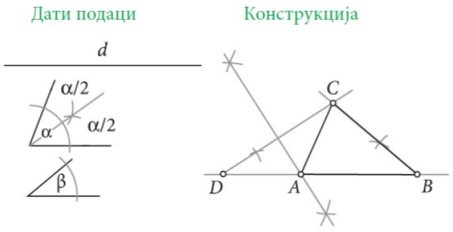


Kako nam je dat zbir $AB+AC$, od koristi će biti nadovezivanje ovih stranica. Neka je D tačka takva da je D–A–B i $DA = AC$. Tada je $DB = d$. Međutim tada su nam poznati uglovi $\triangle DBC$ koji naležu na DB :

- $\angle CDA = \frac{\alpha}{2}$, jer je $\triangle DAC$ jednakokraki, pa je $\angle CDA = \angle DCA$, ali je i $\angle CDA + \angle DCA = \alpha$ (spoljašnji ugao jednak je zbiru dva nesusedna unutrašnja ugla), te je $\angle CDA = \angle DCA = \frac{\alpha}{2}$;
- $\angle DBC = \angle ABC = \beta$.

Ovim smo konstrukciju sveli na jednostavnu konstrukciju $\triangle DBC$ (po stavu USU).

Konstrukcija.



Najpre konstruišemo $\triangle DBC$, čija je jedna stranica DB podudarna datoj duži d, a uglovi kod temena D i B su podudarni uglovima $\frac{\alpha}{2}$ i β. Nakon toga, konstruišemo simetralu s stranice DC. Označimo sa A presek simetrale s i stranice DB.

Dokaz.

Kako tačka A pripada simetrali duži DC, ona je podjednako udaljena od njenih krajeva, to jest $AD = AC$. Odavde dalje zaključujemo da je $AC + AB = DA + AB = DB$. Kako je po konstrukciji $BD = d$, sledi da je zbir stranica AB i AC trougla ABC zaista jednak datoj duži d. Takođe, $\triangle DAC$ je jednakokraki, pa je $\angle CDA = \angle DCA$. Kako je po konstrukciji $\angle CDA = \frac{\alpha}{2}$, sledi i da je $\angle DCA = \frac{\alpha}{2}$. Ugao CAB je spoljašnji ugao $\triangle DAC$ i kao takav jednak je zbiru dva nesusedna unutrašnja ugla, pa je uzimjući u obzir prethodno $\angle CAB = \angle CDA + \angle DCA = \frac{\alpha}{2} + \frac{\alpha}{2} = \alpha$. Najzad, po konstrukciji je $\angle ABC = \angle DBC = \beta$.

Diskusija.

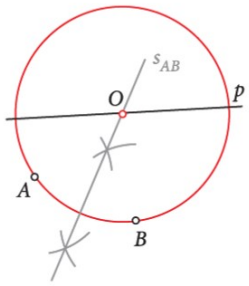
Da bi postavljeni zadatak imao rešenja, neophodno je da zbir uglova α i β bude manji od opruženog ugla. U suprotnom zadatak nema rešenja. □

Primer 2.
Neka su date dve različite tačke A i B i prava p. Konstruisati kružnicu k koja sadrži tačke A i B, a njen centar pripada pravoj p.

Analiza.

Ako tačke A i B obe pripadaju nekoj kružnici, onda su one podjednako udaljene od centra te kružnice. Dakle, centar kružnice pripada simetrali duži AB.

Konstrukcija.



Prvo konstruišemo simetralu s_{AB} duži AB. Neka je O presek simetrale s_{AB} i prave p. Kružnica $k(O, OA)$ je tražena kružnica.

Dokaz.

Prema konstrukciji, sledi da tačka A pripada kružnici $k(O, OA)$ i da se centar ove kružnice nalazi na pravoj p. Ostaje još da se dokaže da B takođe pripada ovoj kružnici. Međutim, to sledi iz činjenice da $O \in s_{AB}$, pa je $OA = OB$.

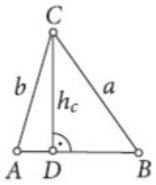
Diskusija.

Zadatak ima jedinstveno rešenje ukoliko prava odjeđena tačkama A i B nije

normalna na p. Ako jeste, zadatak nema rešenja u slučaju da simetrala s_{AB} i prava p nemaju zajedničkih tačaka, ili ima beskonačno mnogo rešenja ako je p simetrala duži AB. □

Primer 3.
Konstruisati $\triangle ABC$, ako je dato a, b i h_c.

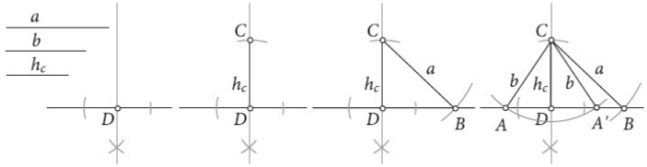
Analiza.



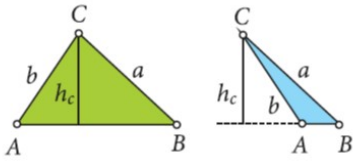
Nacrtajmo proizvoljan $\triangle ABC$ i označimo sa D podnožje visine iz temena C. Nakom konstrukcije $\triangle CDB$ (stav SSU), jednostavno je konstruisati traženi trougao.

Konstrukcija.

Konstrukcija je data na sledećoj slici:



Primećujemo da za izabrane podatke postoje dva nepodudarna trougla koja zadovoljavaju postavljene uslove:



Dokaz.

Konstruisani trougao zadovoljava uslove direktno po konstrukciji.

Diskusija.

Opisanu konstrukciju je moguće izvesti ukoliko je $h_c < a$ i $h_c < b$. U suprotnom zadatak nema rešenja. Ako su ispunjeni navedeni uslovi, zadatak ima jedinstveno rešenje ako je $a = b$, a ako a i b nisu podudarne duži, onda ima dva rešenja. □

Primer 4.

U jednom restoranu za stolom su sedele tri osobe. Dve su jele kobasicu, dve rusku salatu, a dve grožđe. Ona od njih koja nije jela kobasicu, nije jela ni rusku salatu, a ona koja nije jela grožđe, nije jela ni rusku salatu. Šta je imala za doručak svaka od te tri osobe?

Analiza.

Kako je dato u zadatku vidimo da su tačno po dve osobe jele svako od jela. Zaključak koji izvodimo iz drugog dela zadatka je da ako ona osoba koja nije jela kobasicu nije jela ni rusku salatu, to znači da ako je neko jeo rusku salatu, morao je jesti i kobasicu. Slično se izvodi zaključak da ako je neko jeo rusku salatu, morao je da jede i grožđe. To ćemo koristiti u rešenju.

Rešenje.

Neka su te tri osobe označene slovima A, B i C. Pretpostavimo da su osobe A i B jele rusku salatu. To smemo da pretpostavimo jer znamo da su tačno dve osobe jele svako jelo, pa samim tim i rusku salatu. Međutim iz Analize vidimo da su onda iste osobe A i B sigurno jele i kobasicu i sigurno jele i grožđe. Što dalje znači da osoba C nije jela ništa, jer bi u suprotnom to bila treća porcija istog jela što je u suprotnosti sa podacima datim u zadatku. Dakle rešenje je da su osobe A i B jele rusku salatu, kobasicu i grožđe, a osoba C nije jela ništa.

Provera.

Proveravamo da li naše rešenje ispunjava sve uslove zadatka. Osobe A, B i C su gosti restorana od kojih su A i B jeli rusku salatu, kobasicu i grožđe, dok C nije jela ništa. U zadatku je dato da su svako jelo jele tačno po dve osobe, što je ispunjeno i to su osobe A i B. Kako je C jedina osoba koja nije jela kobasicu i nije jela groždje, drugi deo zadatka se odnosi samo na nju i ispunjen je jer nije jela ni rusku salatu.

Diskusija.

Uslovi zadatka su bili takvi da je rešenje koje ih zadovoljava jedinstveno. Sada ćemo videti kako se broj rešenja menja uz male promene polaznih podataka. Da je u zadatku izostavljen uslov da su tačno dve osobe jele rusku salatu, ništa se ne bi promenilo i rešenje bi idalje bilo jedinstveno. Međutim da je izostavljen uslov da su tačno dve osobe jele kobasicu ili grožđe zadatak bi imao dva rešenje, zato što bi osoba C mogla ili da ne jede ništa ili da jede kobasicu tj. grožđe (zavisi koji od ta dva uslova je izostavljen). Zatim da su izostavljena oba uslova i za kobasicu i za grožđe, zadatak bi imao četiri rešenja. Osoba C bi u tom slučaju mogla da ne jede ništa, da jede samo kobasicu, samo grožđe ili kobasicu i grožđe. Dakle naš zadatak ima jedinstveno rešenje, ali uz male promene sličan zadatak bi mogao da ima i više rešenja. □

3 Predgovor zbirci

Teorija brojeva je, uz geometriju, svakako najstarija matematička disciplina. Njene temelje postavili su još starogrčki matematičari Pitagora, Euklid, Diofant i drugi. No, uprkos tome, nikako se ne može reći da je to danas potpuno istražena disciplina. Postoje čak problemi u njoj koji su postavljeni pre više od dve hiljade godina, a koji još uvek nisu rešeni. I baš to obilje problema, i to problema koji se vrlo često mogu formulisati tako da ih razume i matematičar početnik, davalo je kroz istoriju stalan podstrek daljem razvoju teorije brojeva i činilo je interesantnom novim i novim generacijama matematičara.

Već od najranijeg detinjstva deca se susreću sa pojmom broja i raznim igrama vezanim za brojeve. U početku su te igre naivne i svode se na samo korišćenje brojeva, dok kasnije kako se kao učenici upoznaju sa sve zanimljivijim osobinama brojeva, te igre postaju izazovnije i kompleksnije. U igri sa brojevima ravnopravno mogu učestvovati skoro svi kojima su poznate osnovne osobine i operacije, ali svakako da je dobra ideja recept za uspeh. Nekada su te ideje jednostavne, ali najčešće nije lako realizovati ih i pretočiti u potpuno rešenje problema.

Ova zbirka pruža mogućnost mladim matematičarima koji se interesuju za Teoriju brojeva, da probleme vezane za brojeve sagledaju na jedan drugi i možda potpuniji način. Zadaci su rešavani u četiri etape kroz koje čitalac postaje u potpunosti siguran da je rešenje tačno i jasno, a najbitnije od svega ideja je primenljiva i na druge probleme. Svako rešenje počinje analizom podataka koji su nam dati i šta iz tih podataka možemo da zaključimo koristeći se osobinama i zakonima koji su nam poznati. U ovom delu je ključno razmišljanje o problemu i pronalaženje ideje za rešavavnje. To često može da bude pokušaj da se reše neki jednostavniji slučajevi ili pak nasuprot tome, ponekad je korisno posmatrati opštiji problem od postavljenog. Drugi deo je samo rešenje problema koje predstavlja logičnu posledicu analize koju smo već izvršili. Treći deo je takozvani dokaz da rešenje ili rešenja koja smo dobili zadovoljavaju na početku zadate uslove ili provera da li je to ispunjeno, a može biti i rezime prikazanog rešenja. Ovo je jako važan deo jer služi kao provera tačnosti rešenja do koga smo došli, što bi trebalo da bude neizostavan deo rešavanja svakog, pa i matematičkog problema. Poslednja etapa je diskusija i ona se odnosi na razmatranje uslova pod kojima bi se rešenje koje smo dobili na neki način promenilo. Pitamo se šta bi bilo da su ulazni podaci bili drugačiji, kada bi opšte podatke zamenili konkretnim brojevima ili obrnuto i drugo.

Ovde ćemo morati da se osvrnemo i na problemsku nastavu kao važan vid nastave. Ona za cilj ima da pomogne učenicima da razviju fleksibilno znanje, veštinu efikasnog rešavanja problema, samostalno učenje i efikasne veštine za saradnju i unutrašnju motivaciju. Suština je da učenici identifikuju ono što već znaju, šta im je potrebno da znaju i kako i gde da pristupe novim informacijama koje ih mogu dovesti do rešavanja problema. U skladu sa tim važno je pomenuti i četiri faze rešavanja problema koje predlaže čuveni metodičar George Polya. One će nam poslužiti kako bismo lakše razumeli šta radimo u kojoj od već pomenutih faza (Analiza, Rešenje, Dokaz, Diskusija). Prva faza je razumevanje problema, analizom teksta zadatka postavljamo sebi pitanje da li smo razumeli ceo tekst i sve ono što se traži od nas kao rešenje. Pokušavamo da problem preformulišemo svojim rečima i zamislimo sliku problema, ilustrujemo problem na neki način kako bismo sebi olakšali razmišljanje

gledajući u sliku. Druga faza je razvijanje plana rešavanja zadatka. Tu postoji mnogo različitih metoda kako doći do rešenja i na učeniku je da izabere jedan pravi put i da tu ideju razradi u sledećoj fazi koja podrazumeva sprovođenje plana u delo. Neki od metoda za rešavanje zadataka su: nagađanje rešenja, pa dokaz da ono zadovoljava date uslove, eliminacija, povezivanje, crtanje slike, korišćenje modela, rešavanjem prvo jednostavnijeg slučaja, uopštavanjem problema, konkretizacijom, rezonovanjem, rešavanjem unazad i td. Svaka od ideja nam može biti korisna u različitim zadacima i nikada se ne oslanjamo samo na jedan način. Najbolja vežba za što uspešnije pronalaženje pravog puta do rešenja je uraditi što više raznovrsnih zadataka jer samo tako ćemo doći u dodir sa idejama koje ranije nismo videli i usvojićemo ih za rešavanje svih zadataka iz date grupe sličnih. Kada pronađemo pravi put do rešenja, samo rešavanje predstavlja lakši korak jer u njemu samo treba da budemo dosledni svom planu i strpljivo zapišemo rešenje. Nakon svega toga sledi četvrta faza koja je najvažnija za dalju primenu strategije rešavanja u drugim zadacima. To je osvrt na ono što smo uradili. Trudimo se da zapamtimo šta je bilo korisno u našem rešavanju, a šta se pokazalo kao nevažno. Samim tim ćemo lakše uočiti ključne delove zadatka i moguća problemska mesta u rešenju. Tako će učenici biti osposobljeni da lakše predvide koju strategiju da koriste u narednim zadacima.

Ovakav princip rešavanja zadataka je jako dobar, pogotovo za mlade matematičare, jer se na taj način razvija sistematičnost u radu i zapisu, kao i sigurnost u svoje ideje i sposobnost realizacije od ideje do rešenja. Dalje primenljivost tako nastalih rešenja je velika jer diskusija pruža mogućnost šireg sagledavanja problema što nas uvodi u svet novih zadataka sa sličnom postavkom ali drugim rezultatima do kojih se dolazi zbog male promene polaznih podataka.

U prvom delu zbirke nalaze se rešeni primeri sa detaljnim objašnjenjima, dok se u drugom delu nalaze primeri za samostalan rad i proveru stečenih znanja i veština.

4 Zbirka zadataka

4.1 Zadaci sa brojevima i dešifrovanje

Zadatak 1.

Pošto je prethodno umesto zvezdica u izrazu $1*2*3*4*5*6*7*8*9$ upisala znake $+$ ili $-$, Tanja je dobila rezultat 21. Nakon toga, Nataša je zamenila neke od ovih znakova suprotnim znacima i dobila kao rezultat broj 20. Dokazati da je jedna od njih sigurno pogrešila iako ne znamo kakvi su znaci stajali između brojeva.

Analiza:

Sagledajmo najpre dve strategije rešavanja koje direktno sugeriše formulacija zadatka.

(1) Pokušavamo da otkrijemo da li je (i ako jeste, kako) Tanja mogla da postigne zbir 21. Treba imati na umu da ako pronađemo bar jednu mogućnost, imamo još posla: treba pronaći sve moguće načine da se dobije zbir 21, a zatim razmotriti sve moguće izmene koje je Nataša mogla da napravi. Međutim, ako otkrijemo da se 21 ne može dobiti nikakvim zamenama zvezdica znacima $+$ i $\cdot$, onda smo zadatak rešili.

(2) Pokušavamo da otkrijemo da li je (i ako jeste, kako) Nataša mogla da postigne zbir 20. I u ovom slučaju, ako otkrijemo jednu mogućnost, moraćemo sve da ih nađemo, a zatim da dokažemo da se svim mogućim izmenama znakova ne može dobiti 21. Ukoliko otkrijemo da se 20 ne može dobiti, zadatak je rešen.

Primećujemo da koju god strategiju da prihvatimo, otkriće da se ne može dobiti 20 ili 21 brzo dovodi do rešenja. Zato je najkorisnije najpre ispitati da li se uopšte mogu dobiti brojevi 20 i 21.

Postoji $2^8 = 256$ mogućih zamena osam zvezdica znacima $+$ i $-$. Isprobavanje nekoliko nasumično izabranih zamena može biti od koristi.

$$\begin{gathered} 1+2-3-4+5+6-7+8-9=-1 \\ 1-2+3+4-5+6+7+8-9=13 \\ 1+2+3-4-5+6+7+8+9=27 \\ \vdots \end{gathered}$$

Na osnovu ovih nasumičnih izraza, neposredno se može nasluti da će vrednosti svih mogućih izraza biti neparni, i da je verovatno Nataša pogrešila. Preostaje samo da strogo proverimo ovo nagađanje.

(Ne)parnost zbira, odn. razlike, u zavisnosti od (ne)parnosti sabiraka, odn. umanjenika i umanjioca, pokazuje naredna tabela:

x	y	$x \pm y$		$x \pmod 2$	$y \pmod 2$	$x \pm y \pmod 2$
parno	parno	parno		0	0	0
neparno	parno	neparno	ili	1	0	1
parno	neparno	neparno		0	1	1
neparno	neparno	parno		1	1	0

Među brojevima 1, 2, 3, 4, 5, 6, 7, 8 i 9, ima pet neparnih i četiri parna, odakle zaključujemo da postavljanjem znakova + ili − između navedenih brojeva dobijamo rezultat koji mora biti neparan.

Sada preostaje samo da na osnovu ove analize, 'sintetizujemo' rešenje zadatka 'prezapisivanjem analize unazad'. U nastavku navodimo rešenje u kojem se neparnost kao invarijanta obrazlaže na donekle drugačiji način, bez direktnog pozivanja na tablice.

Rešenje:

Zamenu zvezdica znacima + ili − u izrazu $1*2*3*4*5*6*7*8*9$ možemo posmatrati i kao izbor predznaka sabircima sledećeg zbira:

$$1 + (\pm 2) + (\pm 3) + (\pm 4) + (\pm 5) + (\pm 6) + (\pm 7) + (\pm 8) + (\pm 9).$$

Kako za sve cele brojeve a i b važi:

- $a \equiv -a \pmod 2$,
- $b + a \equiv b - a \pmod 2$,

zaključujemo da kako god zamenili zvezdice sa + ili − dobijamo:

$$\begin{aligned} 1*2*3*4*5*6*7*8*9 &\equiv 1+2+3+4+5+6+7+8+9 = 45 \\ &\equiv 1 \pmod 2. \end{aligned}$$

Odavde sledi da rezultat 20 nije moguće dobiti, odnosno da je Nataša pogrešila.

Dokaz:

Strogo opravdanje korektnosti navedenog rešenja podrazumeva dokazivanje osobina celih brojeva koje smo koristili u rešenju. Navedena tvrdjenja su specijalni slučajevi teorema dokazanih u Dodatku ovog rada.

Diskusija:

Vidimo da formulacija zadatka sadrži razne nepotrebne podatke koji rešavača mogu da navedu da krene veoma zamršenim putem. Da je zadatak glasio: *Dokazati da zamenom zvezdica znacima + ili − u izrazu* $1*2*3*4*5*6*7*8*9$ *nije moguće dobiti paran broj*, rešenje bi bilo suštinski istovetno navedenom, ali se pri ovakvoj formulaciji direktno vidi kojim putem treba da krenemo. Taj put postaje trnovitiji ukoliko u postavci umesto *paran broj* navedemo neki konkretan paran broj, za koji nije očigledno da se ne može dobiti. Jedan primer takve formulacije bi bio: *Nataša je zvezdice u izrazu* $1*2*3*4*5*6*7*8*9$ *zamenila znacima + ili − i dobila je rezultat* 20. *Dokazati da je napravila grešku.* Ovde već nije neposredno uočljivo zašto nije mogla da dobije rezultat 20. Naravno, rešenje i ovako postavljenog zadatka je istovetno rešenju polaznog.

Vratimo se ponovo na formulaciju zadatka. Primetimo da rešenje datog zadatka ne odgovara na pitanje da li je moguće dobiti Tanjin rezultat 21. Istražimo gde bi nas dovela strategija (1) navedena u analizi.

Pokušajmo sada da proverimo da li je rezultat 21 koji je dobila Tanja tačan. Treba pronaći kombinaciju znakova takvih da rezultat izraza bude 21. Kako smo već pomenuli, ukoliko bi sve zvezdice bile plusevi ukupan zbir bi bio 45. Dakle

kako se trazeni broj 21 razlikuje od 45 za 24, to znači da neke pluseve treba da pretvorimo u minuseve tako da se oduzima ukupna vrednost 12. Primer za to bi bio $1+2+3+4-5+6-7+8+9$. Tako možemo primetiti da postoje tri mogućnosti za dva broja koja daju 12 (5 i 7, 4 i 8, 3 i 9), zatim tri mogućnosti za tri broja (2, 3 i 7; 2, 4 i 6; 3, 4 i 5) i nema drugih mogućnosti jer najmanje što četiri broja mogu da daju je rezultat $2+3+4+5=14$, a to je već veće od 12, pa nema potrebe razmatrati dalje.

Zadatak 2.

Marija je u stocifrenom broju 123456789012345678901...7890 precrtala sve cifre koje se nalaze na neparnim mestima. Zatim je u dobijenom pedesetocifrenom broju precrtala sve cifre koje se nalaze na neparnim mestima. Ponavljala je taj postupak sve dok nije precrtala i poslednju cifru. Koju cifru je Marija poslednju precrtala?

Analiza:

Posmatrajmo prvo jednostavniji slučaj, neka je dat broj 1234567890. Kada u ovom broju precrtamo sve cifre koje su na neparnim mestima ostaje broj 24680, zatim sa sledećim precrtavanjem ostaje broj 48, zatim 8 i to je broj koji je poslednji precrtan.

Kada bismo sada malo zakomplikovali i posmatrali broj 12345678901234567890 šta bi se dogodilo. Nakon prvog precrtavanja ostao bi broj 2468024680, zatim 48260, pa 86 i na kraju 6.

Primećujemo da se posle prvog precrtavanja sve cifre koje ostaju (nisu precrtane) nalaze na mestima čiji je redni broj deljiv sa dva. Posle drugog precrtavanja preostaće one cifre čiji je redni broj na početku bio deljiv sa četiri i tako dalje.

Rešenje:

Iz Analize zaključujemo da će u svakom precrtavanju cifre koje ostanu biti u polaznom broju na mestima čiji su redni brojevi stepeni dvojke. I to u svakom novom precrtavanju stepen dvojke se uvećava za jedan, pa će posle prvog precrtavanja to biti cifre čiji je redni broj deljiv sa 2, posle drugog sa $2^2=4$, posle trećeg sa $2^3=8$ i td. Najveći stepen dvojke koji nije veći od 100 je $64=2^6$, pa zaključujemo da će cifra koja je poslednja precrtana biti na 64-tom mestu u polaznom broju. To je baš cifra 4 i ona je poslednja precrtana.

Dokaz:

Ispravnost rešenja sledi direktno iz zaključka da su cifre koje ostaju pri precrtavanju na rednim mestima koji su stepeni dvojke i sledećeg kratkog razmatranja. Nakon prvog precrtavanja ostao je pedesetocifreni broj, sledi drugo precrtavanje nakon koga preostaje dvadesetpetocifreni broj, zatim nakon trećeg precrtavanja preostaje dvanaestocifreni broj, nakon četvrtog precrtavanja šestocifreni

broj, nakon petog precrtavanja trocifreni broj i nakon šestog precrtavanja jednocifreni broj koji predstavlja cifru koja je nakon toga poslednja precrtana, a čiji redni broj u polaznom stocifrenom broju je baš 2^6 što je 64 kao što smo i dobili u rešenju. Zaključak je da rešenje zadovoljava uslove zadatka.

Uopštimo postavljeni problem: *Polazeći od n-tocifrenog broja primenjujemo sledeći postupak dok god je moguće: precrtavamo sve cifre na neparnim mestima. Na kom mestu u polaznom broju se nalazi cifra koja će poslednja biti precrtana?* Poslednja precrtana cifra se u polaznom broju nalazi na m-tom mestu, gde je m najveći prirodan broj takav da je $2^m \leq n$.

Diskusija:

Da je broj zadat u zadatku bio bilo koji drugi broj sa bilo koliko cifara, na sličan način bismo odredili redni broj tražene cifre u polaznom broju, kao najveći stepen dvojke koji nije veći od broja cifara polaznog broja.

Zadatak 3.

Na stolu se nalazi 25 šibica. Mirko i Slavko uzimaju naizmenično jednu, dve ili tri šibice. Gubi onaj igrač koji kada dođe na red više ne može da uzme ni jednu šibicu. Kako da igrač obezbedi sebi pobedu u ovoj igri?

Analiza:

Primetimo da jedini način da igrač bude siguran u pobedu je da u pretposlednjem uzimanju ostavi na stolu 4 šibice, jer tada koliko god da šibica uzme njegov protivnik on uzima sve preostale i ne ostavlja ništa na stolu. Samim tim postaje pobednik.

Rešenje:

Na osnovu Analize zaključujemo da igrač koji počinje igru može da sebi obezbedi pobedu ako u prvom potezu uzme jednu šibicu, a u ostalim potezima uzima onoliko šibica koliko je potrebno da broj šibica koje ostaju na stolu bude deljiv sa 4. To znači da će broj šibica koje su na stolu biti na početku 25, pa zatim 24, pa kako oba igrača odigraju prvi ostavlja na stolu 20, u sledećem krugu ostavlja 16 i sve tako dok ne ostanu samo 4 šibice na stolu. Nakon toga drugi igrač ni na koji način ne može sprečiti prvog da uzme poslednju šibicu.

Dokaz:

Dokaz da je ovo rešenje korektno sledi direktno iz zaključka izvedenog u Analizi i očigledno zadovoljava uslove zadatka, tj. pravila igre.

Diskusija:

Ovakav način rešavanja bi bio primenljiv i u slučajevima kada je moguće uzeti od 1 do nekog n broja šibica, tako što bi prvi igrač ponovo vodio računa da uvek ostane na stolu broj šibica koji je deljiv sa $n + 1$.

Zadatak 4.

Dva igrača naizmenično pišu po tabli jednu do druge različite cifre sve dok je to moguće. U toj igri pobeđuje prvi igrač ukoliko uspe da tako dobijeni desetocifreni broj bude deljiv sa brojem 6, a u suprotnom pobeđuje drugi igrač. Koji od igrača može sigurno da pobedi u ovoj igri, ma kako igrao njegov protivnik, i na koji način on to može da postigne?

Analiza:

Da bi dobijeni desetocifreni broj bio deljiv sa brojem 6, on mora da bude deljiv sa brojevima 2 i 3. Kako je broj deljiv sa 3 ukoliko mu je zbir cifara deljiv sa 3, dobijamo da je ovaj desetocifreni broj sigurno deljiv sa 3. To se lako pokazuje jer kako god da poređamo cifre zbir cifara dobijenog desetocifrenog broja je zbir brojeva od 0 do 9 i on je jednak 45 što je deljivo sa 3, pa je i sam broj deljiv sa 3. Što se tiče deljivosti sa 2, dobijeni desetocifreni broj će biti deljiv sa 2 samo ukoliko je poslednja napisana cifra paran broj ($0, 2, 4, 6$ ili 8). Zaključujemo da će prvi igrač moći da pobedi ukoliko navede drugog igrača da poslednju napiše cifru koja je parna.

Rešenje:

Iz Analize vidimo šta je potrebno prvom igraču da bi pobedio. Samo još da otkrijemo kako da to postigne. Rešenje je veoma jednostavno. Ukoliko prvi igrač u svakom potezu bude pisao samo neparne cifre ($1, 3, 5, 7, 9$), dok god je moguće, na kraju drugom igraču neće preostati ništa drugo do da napiše parnu cifru. Time je prvi igrač pobednik. Samim tim zaključujemo da drugi igrač ne bi mogao da ima nikakvu taktiku za sigurnu pobedu, jer uz ovakvu igru prvog igrača on drži igru pod kontrolom.

Dokaz:

Dobijeno rešenje zadovoljava uslove zadatka, tj. pravila igre, jer igrači mogu da biraju cifre koje žele bez ograničenja, pa je i ovaj izbor prvog igrača mogući.

Diskusija:

Zadatak ima rešenje koje je jedinstveno u smislu da prvi igrač može da ima taktiku kojom dolazi do sigurne pobede. Ono što nije jedinstveno je način na koji će igrači birati cifre, odnosno može se dobiti više različitih brojeva koji zadovoljavaju tražene uslove. Međutim kako to nije bilo pitanje u zadatku nije neophodno proveravati. Da su cifre mogle da se ponavljaju (da igrači više puta koriste istu cifru), tada bi zadatak imao drugačije rešenje jer bi u tom slučaju bez obzira na prethodni tok igre u poslednjem koraku drugi igrač odlučivao o parnosti dobijenog broja i samim tim bi mogao da svaki put on bude pobednik. Međutim takva igra ne bi imala preteranog smisla, pa je ni ne razmatramo.

Zadatak 5.

Dva igrača igraju sledeću igru: prvi izgovara jedan prirodan broj koji nije

veći od 10, drugi mu dodaje bilo koji prirodan broj, ne veći od 10 i saopštava zbir. Tom zbiru prvi opet dodaje neki prirodan broj koji nije veći od 10 i saopštava zbir i tako dalje naizmenično, sve dok jedan od njih ne dobije zbir koji iznosi 100. Pobeđuje igrač koji prvi dobije zbir 100. Koji od igrača može igrati tako da sigurno pobedi?

Analiza:

Primetimo da gledajući od kraja igre onaj igrač koji u svom pretposlednjem potezu dobije broj 89 sa sigurnošću pobeđuje jer koji god broj da izabere njegov protivnik, on u sledećem potezu dobija zbir 100. Nakon nekoliko odigranih partija do ovog zaključka bi došli i sami rivali. Drugim rečima, prvi igrač otkriva strategiju ukoliko razmišlja 'unazad':

Ako dobijem 89, jednostavno dobijam 100;

Ako dobijem 78, jednostavno dobijam 89;

$\vdots$

Ako dobijem 12, jednostavno dobijam 23;

Ako dobijem 1, jednostavno dobijam 12.

Rešenje:

Igrač koji počinje partiju će svojim izborom brojeva moći da utiče na tok igre i da dovede do pobede ukoliko iskoristi pomenutu taktiku. Iz Analize zaključujemo da bi on u pretposlednjem koraku trebalo da dobije zbir 89. Na sličan način iz toga sledi da bi u koraku pre tog trebalo da dobije zbir 78 (kako bi osigurao da u sledećem koraku dođe do željenog zbira 89), pa pre toga 67 (da bi došao do 78) i sve tako do broja 12, što će biti lako da dobije u drugom koraku ukoliko u prvom izgovori broj 1. Dakle zaključak je da prvi igrač može sebi da obezbedi pobedu igrajući na gore opisan način, dok drugi igrač u tom slučaju neće moći da utiče na tok igre.

Dokaz:

Rešenje zadovoljava uslove zadatka, tj. pravila igre. To sledi očigledno iz izbora brojeva koji nisu veći od 10 i to je jedini uslov koji je trebalo ispuniti.

Diskusija:

Ovaj zadatak ima jedinstveno rešenje. Način na koji je rešen može se primeniti i na zadatke u kojima je zbir koji se traži za pobedu bilo koji drugi prirodan broj, recimo n, a brojevi koji se biraju ne veći od ponovo nekog prirodnog broja k, gde je $k < n$. Tada bi prvi igrač ponovo krenuo sa 1 i birao brojeve tako da dobija zbirove koji na kraju vode do zbira $n - k - 1$ u pretposlednjem koraku. Samim tim isti igrač bi u poslednjem koraku lako došao do traženog zbira n.

Zadatak 6.

Dve seljanke su na pijaci prodavale 100 jaja. Jedna je imala više od druge, ali su za prodata jaja dobile jednake sume novca. "Da sam ja prodavala tvoja jaja po ceni mojih" - počinje priču prva seljanka - "dobila bih za njih 15 novčića.". "A ja bih za tvoja jaja kada bi ih prodavala po mojim cenama" - nastavlja priču druga seljanka - "dobila $6\frac{2}{3}$ novčića.". Koliko jaja je imala na početku svaka seljanka?

Analiza:

Neka je prva seljanka imala manje jaja, a druga više. Da bi dobile za njih istu sumu novca zaključujemo da je prva prodavala jaja po skupljoj ceni. Pretpostavićemo da je druga seljanka imala n puta više jaja, pa zaključujemo da je prva prodavala jaja po n puta većoj ceni.

Rešenje:

Kako vidimo iz Analize, druga seljanka imala n puta više jaja, a prva je jaja prodavala po n puta većoj ceni. Da je prva seljanka prodavala jaja druge seljanke ona bi imala n puta više jaja koje bi prodavala po svojoj n puta većoj ceni, pa bi za njih dobila n^2 puta više novca od druge.

$$n^2 = 15 : 6\frac{2}{3} = \frac{9}{4}$$

Znači da je $n = \frac{3}{2}$. Kada 100 jaja koliko su ukupno imale na početku podelimo u razmeri $3 : 2$, izračunavamo da je prva seljanka prodala 40 jaja, a druga 60 jaja.

Dokaz:

Proverimo sada da li dobijeno rešenje zadovoljava uslove zadatka. Krećemo od toga da je prva seljanka prodala 40 jaja, a druga 60 jaja.

Prva je rekla da je ona prodala 60 jaja koje je prodavala druga da bi zaradila 15 novčića. Sto znači da bi svako jaje prodavala za $\frac{1}{4}$ novčića i to je cena po kojoj ona prodaje. Odatle vidimo da je ona svojih 40 jaja prodavala po toj ceni i zaradila 10 novčića. Sada još da vidimo po kojoj ceni je druga seljanka prodavala svoja jaja i ukoliko je zarada ista ispunjeni su uslovi zadatka. Kako je druga seljanka izjavila, ona bi za 40 jaja prve seljanke dobila $6\frac{2}{3}$ novčića. Što znači da bi ih prodavala po ceni od $\frac{1}{6}$ novčića i to je cena po kojoj je prodavala i svoja jaja. Dakle za svojih 60 prodatih jaja po ceni od $\frac{1}{6}$ novčića, druga seljanka bi dobila 10 novčića. Kako je toliko zaradila i prva seljanka vidimo da su uslovi dati u zadatku ispunjeni.

Diskusija:

Ovo rešenje je jedinstveno. Slično bi se rešavao svaki zadatak gde bi samo bile promenjene vrednosti. Opšti zadatak bi glasio:

Dve seljanke su prodavale na pijaci N jaja. Jedna je imala više od druge, ali su za prodata jaja dobile jednake sume novca. "Da sam ja prodavala tvoja jaja" - počinje priču prva seljanka - "dobila bih za njih x novčića.". "A ja bih za tvoja jaja" - nastavlja priču druga seljanka - "dobila y novčića.". Koliko je jaja imala svaka seljanka?

U tom opštem slučaju bismo zadatak rešavali na isti način i tražili bi n takvo da je $n^2 = \frac{x}{y}$. Pa bi polazni broj jaja N delili u dobijenoj razmeri na isti način kao i u našem rešenju.

Kosrisno je faze razmišljanja u navedenom rešenju povezati sa algebraskim zakonitostima koje koristimo prilikom rešavanja odgovarajućeg sistema od četiri jednačine sa četiri nepoznate:

- X broj jaja koja je imala prva seljanka i x cena po kojima ih je prodavala,
- Y broj jaja koja je imala druga seljanka i y cena po kojoj ih je prodavala.

Najavljeni sistem je:

$$X + Y = 100,\ Xx = Yy,\ Yx = 15,\ Xy = 6\frac{2}{3}.$$

Najjednostavniji način da se reši sistem jeste da se, na osnovu poslednje tri jednačine odredi razmera $\frac{Y}{X}$, *što je polazna ideja navedena u Analizi.* Uvodjenjem nove nepoznate n, $\frac{Y}{X} = n$, iz $Xx = Yy$ sledi da je $\frac{x}{y} = n$, što odgovara sledećem rezonu: *pošto su seljanke zaradile isto, ako je jedna imala n puta više jaja od druge, cena po kojoj je prodavala prva mora biti n puta manja od cene po kojoj je prodavala druga.* Najzad, iz poslednje dve sledi da je

$$15 : 6\frac{2}{3} = \frac{Yx}{Xy} = \frac{Y}{X} \cdot \frac{x}{y} = n^2.$$

Ove jednakosti kažu: *da je ona koja je imala n puta više jaja, prodavala po n puta većoj ceni, ona bi zaradila n^2 puta više novca.*

Zadatak 7.

Odrediti sve cifre x, y, z i t takve da važi

$$\overline{xyzt} + \overline{xyz} + \overline{xy} + x = 2014.$$

Analiza:

Najpre uočimo da je $1 \leq x \leq 9$ i $0 \leq y, z, t \leq 9$ jer prva cifra u zapisu višecifrenog broja ne sme da bude 0. Dalje ćemo koristiti da je data jednakost ekvivalentna sa jednakošću:

$$1000x + 100y + 10z + t + 100x + 10y + z + 10x + y + x = 2014$$

Sređivanjem ove jednakosti i koristeći poznate osobine brojeva lako ćemo doći do rešenja.

Rešenje:

Ekvivalentna jednakost polaznoj koju smo dobili u analizi je dalje ekvivalentna sa

$$1111x + 111y + 11z + t = 2014.$$

Kako su y, z i t nenegativni brojevi, zaključujemo da je $x = 1$, jer kada bi x bilo veće od 1 proizvod $1111x$ bi bio veći od 2014 i jednakost ne bi bila zadovoljena. Odavde je

$$111y + 11z + t = 903.$$

Kako su z i t nenegativni brojevi, zaključujemo na isti način kao i gore da je $y < 9$. Kako je još $11z \leq 99$ i $t \leq 9$, lako zaključujemo da je $y > 7$, što znači da je $y = 8$. Dalje je $11z + t = 15$, odakle lako zaključujemo da je $z = 1$ i $t = 4$. Dakle, $x = 1$, $y = 8$, $z = 1$ i $t = 4$.

Primetimo da je navedeno rešenje i jedino, što direktno sledi iz razmatranja navedenih u Rešenju.

Dokaz:

Polazimo od rešenja koje smo dobili da je $x = 1$, $y = 8$, $z = 1$ i $t = 4$. Ovde ćemo direktno proveriti da li ove vrednosti promenljivih x, y, z i t zadovoljavaju jednakost datu u zadatku.

$$\overline{xyzt} + \overline{xyz} + \overline{xy} + x = 1814 + 181 + 18 + 1 = 2014$$

Dobili smo da je vrednost izraza sa leve strane jednakosti jednaka 2014 za naše vrednosti promenljivih, a kako je toliko zadato u zadatku da bude i desna strana, dobijamo tačnu jednakost, što znači da rešenje zadovoljava uslove zadatka.

Diskusija:

Rešenje je jedinstveno. Međutim da je u zadatku bio drugi broj umesto 2014 zadatak bi mogao i da nema rešenja i da ima više od jednog tačnog rešenja. Do njih bi se došlo sličnim razmatranjem mogućnosti za svaku od promenljivih x, y, z i t posebno i u zavisnosti od ostalih, kao i u ovde prikazanom rešenju.

Zadatak 8.

Odrediti cifre koje su zamenjene slovima u sledećoj jednakosti:

$$(R + O + M + A)^4 = \overline{ROMA}.$$

Analiza:

Primetimo da je broj $\overline{ROMA}$ četvorocifren broj, dakle za njega važi:

$$999 < \overline{ROMA} < 10000$$

Odatle ćemo izvesti neke zaključke koji će nas dovesti do rešenja.

Rešenje:

Nastavimo dalje od ideje u Analizi. Odatle imamo da je sada:

$$999 < (R + O + M + A)^4 < 10000$$

$$5 < (R + O + M + A) < 10$$

Znači broj $\overline{ROMA}$ može biti samo jedan od brojeva 6^4, 7^4, 8^4 ili 9^4. Razmotrimo sada ta četiri slučaja:

$$6^4 = 1296, 7^4 = 2401, 8^4 = 4096, 9^4 = 6561$$

Vidimo da jedino za broj 2401 važi da je zbir cifara stepenovan sa četiri jednak samom tom broju, dakle to je traženi broj, a rešenje je:

$$(2 + 4 + 0 + 1)^4 = 2401$$

Dokaz:

Proverićemo da li je rešenje korektno direktnim računanjem:

$$(2 + 4 + 0 + 1)^4 = 7^4 = 2401$$

Dakle tačno je.

Diskusija:

Ovde smo imali priliku da vidimo još jednu drugačiju ideju koja može biti korisna za rešavanje šifrovanih zadataka. Ideja razmatranja mogućnosti na osnovu zaključaka koji proizilaze iz osobina brojeva je vrlo primenljiva, pa je zato jako važna.

Zadatak 9.

U jednakosti $3 \cdot \overline{MOJSIN} = 4 \cdot \overline{SINMOJ}$ treba zameniti slova odgovarajućim ciframa, kojim?

Analiza:

Najčešće se zadaci dešifrovanja rešavaju tako što broj koji je predstavljen slovima zapišemo kao zbir cifara pomnoženih sa odgovarfajućim dekadnim jedinicama. U ovom slučaju takvo rastavljanje bi dalo sledeće:

$$\overline{MOJSIN} = M \cdot 10^5 + O \cdot 10^4 + J \cdot 10^3 + S \cdot 10^2 + I \cdot 10 + N$$

Međutim ovo nam ne znači mnogo za rešenje jer u ovom slučaju možemo da primetimo sledeće da imamo grupe koje se ponavljaju u oba broja, a to su MOJ i SIN, pa ćemo uvesti smenu koja nam daje dve nepoznate $x = \overline{MOJ}$ i $y = \overline{SIN}$.

Rešenje:

Kada uvedemo smenu kao što je data ideja u Analizi dobijamo:

$$3 \cdot \overline{MOJSIN} = 4 \cdot \overline{SINMOJ}$$

$$3 \cdot (\overline{MOJ} \cdot 1000 + \overline{SIN}) = 4 \cdot (\overline{SIN} \cdot 1000 + \overline{MOJ})$$
$$3 \cdot (1000x + y) = 4 \cdot (1000y + x)$$

Odatle je kada se sredi:

$$y = \frac{428}{571}x$$

Odatle vidimo da x mora biti 571, a y je onda 428. Dakle rešenje je:

$$3 \cdot 571428 = 4 \cdot 428571.$$

Dokaz:

Proverimo da li rešenje koje smo pronašli zadovoljava uslove zadatka:

$$3 \cdot 571428 = 1714284 = 4 \cdot 428571$$

Računanjem smo proverili da je rešenje korektno.

Diskusija:

Kao što smo konstatovali u Analizi, najčešće se zadaci sa dešifrovanjem rešavaju rastavljanjem broja na zbir cifara pomnoženih sa odgovarajućom dekadnom jedinicom ili kao što je ovde bio slučaj broj smo podelili na deo manji od hiljadu kao jedan broj i broj hiljada kao drugi broj. Na sličan način se po potrebi mogu praviti i druge kombinacije. Nakon toga se razmatraju moguće vrednosti za nepoznate promenljive i dolazi do rešenja.

Zadatak 10.

Odrediti sa koliko nula se završava broj 562!.

Analiza:

Posmatrajmo prvo jednostavniji primer, neka je traženo sa koliko nula se završava broj 10!.

$$10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$$

Primećujemo da da bismo dobili nulu na kraju broja to znači da u ovom rastavljanju treba da imamo broj 10 i koliko takvih desetki se pojavi toliko nula ćemo imati. Međutim na ovom primeru je očigledno da to nije samo broj 10, već i proizvod $2 \cdot 5$ jer tako ponovo dobijamo još jednu desetku, pa taj slučaj ne smemo izostaviti. Dakle zaključujemo da se broj 10! završava sa dve nule. Šta je sa brojem 25!? U rastavljanju ovog broja na faktore imamo jednu desetku, jednu peticu i jednu dvojku, ali se tu pojavljuju i brojevi kao što su 15, 20 i 25 koji su takođe značajni za naše prebrojavanje, jer svaki od njih može da se rastavi na faktore od kojih je bar jedan broj 5. Dakle zaključujemo da moramo da vodimo računa i o takvim brojevima kod kojih se 5 pojavljuje kao faktor i posebno o onima kod kojih se 5 pojavljuje kao višestruki faktor.

Primetimo dakle da ustvari tražimo koliko puta će se broj 10 pojaviti kao faktor u rastavljanju broja 562!, to jest, potrebno je odrediti najveći mogući broj desetki u broju 562!. Kako je 10 složen broj koji se može zapisati kao $10 = 2 \cdot 5$, a 5 je veće od 2, to znači da je ustvari dovoljno pronaći koliko najviše puta će se prost broj 5 pojaviti u broju 562!. Kako se 5 ne nalazi samo kao prost činilac u 562!, primetimo da treba odrediti i koliko puta se pojavljuju njegovi proizvodi sa samim sobom 25 i 125. Jer kada je neki od brojeva u 562! deljiv sa recimo 25 on je deljiv i sa 5, ali nije dovoljno brojati ga jednom, zato se broji ponovo prvo kao broj deljiv sa 5, pa zatim kao broj deljiv sa 25. Slično je i sa 125, koji se broji tri puta, kao broj deljiv sa 5, zatim sa 25 i na kraju sa 125. Jedino takvim brojanjem dolazimo do tačnog broja petica u rastavljanju broja 562! na proste činioce, što nam je i bio cilj, a bez da izostavimo neki broj.

Rešenje:

U proizvodu 562! ima tačno $[\frac{562}{5}]$ brojeva koji su deljivi sa 5, zatim ima tačno $[\frac{562}{25}]$ brojeva koji su deljivi sa 25 (koji su dva puta deljivi sa 5) i tačno $[\frac{562}{125}]$ brojeva koji su deljivi sa 125 (tri puta deljivi sa 5).

Dakle zaključujemo da će ukupan broj pojavljivanja petica u faktorizaciji broja 562! na proste činioce biti:

$$\left[\frac{562}{5}\right] + \left[\frac{562}{25}\right] + \left[\frac{562}{125}\right] = 112 + 22 + 4 = 138$$

Znači broj 562! će se završavati sa 138 nula.

Dokaz:

Dokaz da naše rešenje zadovoljava uslove zadatka sastoji se u tome da pokažemo da nema drugih petica u faktorizaciji broja 562! koje nismo računali. To se lako pokazuje jer smo u Analizi već objasnili da ćemo deljenjem sa 5 odrediti koliko ima brojeva koji su deljivi sa 5 u proizvodu 562!, međutim kako se tu pojavljuju i brojevi koji su višestruki sadržaoci broja 5, taj problem smo rešili brojeći sada ponovo brojeve koji su sadržaoci broja 25 (oni koji dva puta sadrže broj 5 u svojoj faktorizaciji), a zatim još jednom brojeve u proizvodu koji su deljivi sa 125 (oni koji tri puta sadrže broj 5 u svojoj faktorizaciji, to jest sadrže 25 i 5). Ukoliko bismo išli dalje vidimo da bi sledeći broj koji proveravamo bio četvrti stepen broja 5, međutim to je broj 625 koji je veći od 562, pa sigurno neće postojati broj manji ili jednak od 562 koji je sadržalac broja 625. Dakle dalje nema potrebe proveravati i tu stajemo. Time su pokupljena sva pojavljivanja broja 5 u faktorizaciji ovog proizvoda na proste činioce. Pošto je 2 manji broj od 5, njega će svakako biti na još više mesta u faktorizaciji, pa će svaka petica zasigurno imati svog para sa kojim zajedno daje 10.

Diskusija:

Rešenje je jedinstveno, ali se može uopštiti i koristiti za pronalaženje broja nula sa kojima se završava faktorijel bilo kog prirodnog broja. To radimo na sledeći način:

Neka je n prirodan broj. Odrediti sa koliko nula se završava proizvod $n!$.

U proizvodu $n! = 1 \cdot 2 \cdot 3 \cdots n$ ima tačno $[\frac{n}{p}]$ faktora koji su sadržaoci broja p. Među njima je tačno $[\frac{n}{p^2}]$ onih koji su takođe sadržaoci prostog broja p^2 itd. Svaki faktor u proizvodu $n!$ koji je sadržalac broja p^m se broji tačno m puta:

kao sadržalac od p, p^2, $\cdots$, p^m. Dakle ukupan broj nula sa kojima se završava proizvod $n!$ je:

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots .$$

Primetimo da je prethodni zbir konačan jer je $\left[\frac{n}{p^k}\right] = 0$ za dovoljno veliko k.

4.2 Deljivost i prosti brojevi

Zadatak 11.

Dokazati da je broj $A = 8888\cdots88$ ($2012 \cdot 2013$ osmica) deljiv brojevima 2, 3, 7, 11, 13, 37. Proveriti da li je on deljiv i sa 4, 8, 16.

Analiza:

Koristićemo rastavljanje broja na činioce i na taj način ćemo pokušati da dođemo do rešenja. Primetimo još da se broj 888888 (6 osmica) može zapisati na sledeći način:

$$888888 = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$$

Što znači da je ovaj broj deljiv sa 2, 3, 7, 11, 13 i 37, kao i sa 4 i 8. To ćemo pokušati da iskoristimo u rastavljanju našeg broja.

Rešenje:

Broj A ima $2012 \cdot 2013 = 4050156 = 6 \cdot 675026$ cifara. Dakle, on se može zapisati u obliku:

$$A = 888888 + 10^6 \cdot 888888 + \cdots + 10^k \cdot 888888 =$$

$$= 888888 \cdot (1 + 10^6 + \cdots + 10^k) =$$

$$= 8 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot (1 + 10^6 + \cdots + 10^k).$$

Odavde je jasno da je broj A deljiv sa 2, 4, 8 kao i sa 3, 7, 11, 13, 37. Broj u zagradi u prethodnoj jednakosti je neparan pa broj A nije deljiv sa 16.

Dokaz:

Dokaz da dobijeno rešenje zadovoljava uslove zadatka direktno sledi iz računa prikazanog u Rešenju.

Diskusija:

Pokušajmo da uopštimo dobijene rezultate i iskoristimo ih za veći broj primera.

Videli smo u Analizi da je broj 888888 (6 osmica) deljiv sa brojevima 8, 3, 7, 11, 13 i 37. Ispostavlja se da je svaki šestocifren broj kod koga su sve cifre iste, dakle oblika $\overline{xxxxxx}$ deljiv sa brojevima 3, 7, 11, 13, 37 i sa brojem x. Sada ćemo to i dokazati:

$$\overline{xxxxxx} = 10^5 \cdot x + 10^4 \cdot x + 10^3 \cdot x + 10^2 \cdot x + 10 \cdot x + x =$$

$$= (10^5 + 10^2) \cdot x + (10^4 + 10^1) \cdot x + (10^3 + 1) \cdot x =$$

$$= 10^2 \cdot (10^3 + 1) \cdot x + 10^1 \cdot (10^3 + 1) \cdot x + (10^3 + 1) \cdot x =$$

$$= (10^3 + 1) \cdot (10^2 + 10 + 1) \cdot x =$$

$$= 1001 \cdot 111 \cdot x =$$

$$= 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot x$$

Iz poslednje jednakosti očigledno važi traženo.

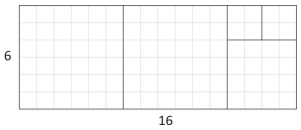
Dakle, možemo izvesti zaključak da će bilo koji broj sa svim istim ciframa kod koga je broj cifara deljiv sa 6 moći da se zapiše na sličan način kao i naš broj u zadatku i da će samim tim biti deljiv sa 3, 7, 11, 13, 37 i sa brojem koji predstavlja cifru koja se ponavlja u zapisu datog broja. Ovo uopštenje će biti veoma korisno u daljem rešavanju sličnih zadataka.

Zadatak 12.

Neka su m i n prirodni brojevi i $m < n$. Od pravougaonika čije su dimenzije $m \times n$ odsecani su kvadrati stranice m dok god nije ostao pravougaonik čija je jedna stranica kraća od m. Od dobijenog pravougaonika odsecani su kvadrati čije su stranice jednake dužini kraće stranice pravougaonika, dok god je to bilo moguće. Na novodobijeni pravougaonik je ponovo primenjen isti postupak. Postupak se zaustavlja kada se nakon odsecanja odgovarajućih kvadrata dobije kvadrat. Odrediti dimenzije poslednjeg kvadrata dobijenog rezanjem pravougaonika.

Analiza:

Pokušajmo prvo da rešimo neke od specijalnih slučajeva postavljenog zadatka za konkretne vrednosti m i n. Ako je na primer $m = 6$ i $n = 16$, direktno se možemo uveriti da je poslednji kvadrat dimenzija 2×2.



Prikazano rezanje zapravo ilustruje sledeći račun:

$$16 = 2 \cdot 6 + 4$$

(od pravougaonika 6×16 režemo dva kvadrata 6×6 i ostaje pravougaonik 4×6)

$$6 = 1 \cdot 4 + 2$$

(od pravougaonika 4×6 režemo jedan kvadrat 4×4 i ostaje pravougaonik 2×4)

$$4 = 2 \cdot 2$$

(od pravougaonika 2×4 režemo dva kvadrata 2×2 i ne ostaje ništa).
Dakle, stramica poslednjeg kvadrata je 2.

Za bilo koje m i n navedeni račun nas dovodi do odgovora bez direktnog crtanja. Na primer, ako je $m = 141$ i $n = 324$ imamo:

$$324 = 2 \cdot 141 + 42$$

(dva kvadrata stranice 141 i ostaje pravougaonik dimenzije 42×141)

$$141 = 3 \cdot 42 + 15$$

(tri kvadrata stranice 42 i ostaje pravougaonik dimenzije 15×42)

$$42 = 2 \cdot 15 + 12$$

(dva kvadrata stranice 15 i ostaje pravougaonik dimenzije 15×12)

$$15 = 1 \cdot 12 + 3$$

(jedan kvadrat stranice 12 i ostaje pravougaonik dimenzije 12×3)

$$12 = 4 \cdot 3$$

(četiri kvadrata stranice 3 i ne ostaje ništa)
Rezanjem pravougaonika 141×324 na kraju dolazimo do kvadrata stranice 3.

U opštem slučaju dobijamo:

$$n = q_1 \cdot m + r_1, 0 \leq r_1 < m,$$

$$m = q_2 \cdot r_1 + r_2, 0 \leq r_2 < r_1,$$

$$r_1 = q_3 \cdot r_2 + r_3, 0 \leq r_3 < r_2,$$

$\vdots$

Ukoliko za bilo koje m i n dolazimo do ostatka r_k (za neko k) koji je jednak nuli, rešenje zadatka će biti prethodni ostatak r_{k-1}.

Rešenje:

Na osnovu Analize i Euklidovog algoritma možemo zaključiti da za pravougaonik dimenzija $m \times n$, stranica poslednjeg kvadrata nakon rezanja jednaka je $NZD(m, n)$.

Dokaz:

Euklidov algoritam je iterativne prirode, što znači da se krajnji rezultat dobija u nizu koraka, dok se međurezultat proizvoljnog koraka koristi u prvom sledećem. Ukoliko je k ceo broj kojim su označeni koraci algoritma počevši od nule, prvom koraku odgovara jednakost $k = 0$, drugom $k = 1$, i tako dalje.

Svaki korak počinje sa dva nenegativna ostatka r_{k-1} i r_{k-2}. Kako algoritam osigurava da se ostaci svakim korakom neprekidno smanjuju, r_{k-1} je manje od svog prethodnika r_{k-2}. Cilj k-tog koraka je da se odrede količnik q_k i ostatak r_k takvi da važi jednakost:

$$r_{k-2} = q_k \cdot r_{k-1} + r_k$$

gde je $r_k < r_{k-1}$. Drugim rečima, umnošci manjeg broja r_{k-1} se oduzimaju od većeg broja r_{k-2} sve dok je dobijeni ostatak manji od r_{k-1}.

U prvom koraku ($k = 0$), ostaci r_{-2} i r_{-1} su jednaki a i b respektivno, a to su upravo brojevi za koje se traži NZD. U sledećem koraku ($k = 1$), ostaci postaju jednaki b i ostaku početnog koraka r_0... Na osnovu toga, algoritam se može predstaviti nizom jednakosti:

$$a = q_0 \cdot b + r_0$$

$$b = q_1 \cdot r_0 + r_1$$
$$r_0 = q_2 \cdot r_1 + r_2$$
$$r_1 = q_3 \cdot r_2 + r_3$$

$\vdots$

Kako se ostaci smanjuju u svakom koraku, i kako ne mogu biti negativni, ostatak r_N u nekom trenutku mora postati jednak nuli, pa se tada algoritam zaustavlja. Poslednji ostatak r_{N-1} koji je različit od nule je najveći zajednički delilac brojeva a i b. Broj N ne može biti beskonačan pošto između nule i prvog ostatka r_0 postoji konačan broj nenegativnih celih brojeva.

Dokaz validnosti Euklidovog algoritma:

Validnost Euklidovog algoritma se može dokazati u dva koraka. U prvom koraku pokazuje se da poslednji ostatak r_{N-1} različit od nule deli istovremeno i a i b. Kako je u pitanju zajednički delilac, on mora biti manji ili jednak najvećem zajedničkom deliocu g. U drugom koraku se pokazuje da proizvoljan zajednički delilac brojeva a i b, uključujući i g, mora da deli i r_{N-1}; odatle sledi da g mora biti manje ili jednako r_{N-1}. Dobijena dva zaključka su konzistentna samo u slučaju da je $r_{N-1} = g$.

Da bi se pokazao prvi korak, odnosno da r_{N-1} deli istovremeno i a i b, najpre treba primetiti da r_{N-1} deli svog prethodnika r_{N-2}.

$$r_{N-2} = q_N \cdot r_{N-1}$$

pošto je poslednji ostatak r_N jednak nuli, r_{N-1} deli i r_{N-3}.

$$r_{N-3} = q_{N-1} \cdot r_{N-2} + r_{N-1}$$

zato što istovremeno deli oba sabirka sa desne strane jednakosti. Razmatrajući redom ostale prethodnike, dobija se da ih r_{N-1} deli sve, ukljucujući a i b. Sa druge strane, nijedan od preostalih ostataka r_{N-2}, r_{N-3}, itd. ne deli istovremeno i a i b, pošto se u jednakostima uvek javlja ostatak. Kako je r_{N-1} zajednički delilac brojeva a i b, mora biti $r_{N-1} \leq g$.

U drugom koraku treba dobiti da proizvoljan prirodan broj c koji istovremeno deli i a i b (proizvoljan zajednički delilac brojeva a i b) mora da deli i ostatak r_k. Po definiciji, a i b mogu biti zapisani kao umnošci broja c: $a = mc$ i $b = nc$, pri čemu su m i n prirodni brojevi. Odatle sledi da c deli prvi ostatak r_0, jer važi sledeći niz jednakosti:

$$r_0 = a - q_0 b = mc - q_0 nc = (m - q_0 n)c.$$

Analogno se može dobiti da c deli i ostatke r_1, r_2, itd. Zaključak je da NZD g mora da deli r_{N-1}, odakle je $g \leq r_{N-1}$. Kako je prema prvom koraku $r_{N-1} \leq g$, mora biti $g = r_{N-1}$. Zato je g najveći zajednički delilac svih sledećih parova:

$$g = NZD(a, b) = NZD(b, r_0) = NZD(r_0, r_1) = \cdots = NZD(r_{N-2}, r_{N-1}) = r_{N-1}$$

Možemo primetiti da proces prikazan u Analizi ustvari jeste jedna primena Euklidovog algoritma, gde su polazni brojevi za koje trazimo NZD baš dimenzije pravougaonika $m \times n$, umnožak je broj kvadrata dimenzije n na koje možemo da isečemo pravougaonik, a ostatak je pravougaonik koji nam ostaje pri takvom sečenju. Ponavljajući postupak u poslednjem koraku ostatka neće biti, odnosno ostatak će biti nula, pa je traženo rešenje poslednji ostatak različit od nule. To je baš $NZD(m, n)$ i iz korektnosti Euklidovog algoritma imamo da rešenje zadovoljava uslove zadatka.

Diskusija:

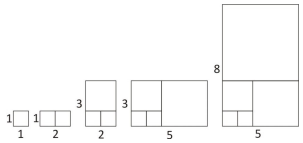
Euklidov algoritam je jedan od najstarijih algoritama koji se još uvek upotrebljava. On ima široku terijsku i praktičnu primenu. Predstavlja ključan element RSA algoritma, metode asimetrične kriptografije koja se u značajnoj meri primenjuje u elektronskom poslovanju. Koristi se pri rešavanju linearnih Diofantovih jednačina, na primer kod određivanja brojeva koji zadovoljavaju višestruke kongruencije (Kineska teorema o ostacima) ili pri određivanju multiplikativnog inverza konačnog polja. Može se upotrebiti za kostruisanje verižnih razlomaka, u Šturmovoj metodi za određivanje realnih nula polinoma, i još nekoliko savremenih algoritama za faktorizaciju prirodnih brojeva. Na kraju, Euklidov algoritam je osnovno sredstvo za dokazivanje teorema moderne teorije brojeva, kao što su Lagranžova teorema o četiri kvadrata i osnovna teorema aritmetike o jedinstvenoj faktorizaciji prirodnih brojeva.

Zadatak 13.

Naći prirodne brojeve m i n takve da se rezanjem pravougaonika $m \times n$ kao što je opisano u prethodnom zadatku dobijaju kvadrati tačno četiri različite dimenzije.

Analiza:

Razmišljajmo unazad, pod pretpostavkom da na kraju ostane jedinični kvadrat.



Vidimo sa slike da jedno rešenje možemo da nađemo direktno "slaganjem" kvadrata odgovarajućih dimenzija.

Rešenje:

Jedan traženi pravougaonik je 5×8, što je prikazano na slici.

Dokaz:

Proverimo rešenje primenom postupka iz prethodnog zadatka.

$8 = 1 \cdot 5 + 3$, (jedan kvadrat stranice 5 i ostaje pravougaonik dimenzije 5×3)
$5 = 1 \cdot 3 + 2$, (jedan kvadrat stranice 3 i ostaje pravougaonik dimenzije 3×2)
$3 = 1 \cdot 2 + 1$, (jedan kvadrat stranice 2 i ostaje pravougaonik dimenzije 2×1)
$2 = 2 \cdot 1$, (dva kvadrata stranice 1 i ne ostaje ništa)

Iz prikazanog vidimo da pravougaonik dimenzije 8×5 možemo rezanjem kao u prethodnom zadatku da podelimo na pet kvadrata od čega su četiri različitih dimenzija.

Diskusija:

Pokušajmo sada da uopštimo zadatak. Za svaki prirodan broj k mogu se naći prirodni brojevi m i n takvi da se rezanjem pravougaonika dimenzija $m \times n$ dobijaju kvadrati tačno k različitih dimenzija. Za m i n možemo uzeti članove F_{k+1} i F_k Fibonačijevog niza $F_1 = 1$, $F_2 = 2$, $F_{k+2} = F_{k+1} + F_k$, $k \geq 1$. Ako je $m = F_k$ i $n = F_{k+1}$, onda se može odseći samo jedan kvadrat stranice F_k i ostaje pravougaonik dimenzije $F_k \times F_{k-1}$. U navedenom rešenju zadatka uzeto je $F_4 = 5$ i $F_5 = 8$, pri čemu se rezanjem dobijaju kvadrati čije su stranice jednake sledećim članovima Fibonačijevog niza: 1, 2, 3, 5.

Zadatak 14.

Odrediti $NZD(1946, 848)$, primenom Euklidovog algoritma.

Analiza:

Koristićemo postupak Euklidovog algoritma kao što je prikazan u prethodnim zadacima.

Rešenje:

Polazni brojevi u Euklidovom algoritmu će biti 1946 i 848, a NZD ova dva broja će biti kao što je već pokazano poslednji ostatak u algoritmu koji je različit od nule.

$$1946 = 2 \cdot 848 + 250$$

$$848 = 3 \cdot 250 + 98$$

$$250 = 2 \cdot 98 + 54$$

$$98 = 1 \cdot 54 + 44$$

$$54 = 1 \cdot 44 + 10$$

$$44 = 4 \cdot 10 + 4$$

$$10 = 2 \cdot 4 + 2$$

$$4 = 2 \cdot 2$$

Dakle primenom Euklidovog algoritma smo dobili da je $NZD(1946, 848) = 2$.

Dokaz:

Kako su prosti delioci broja 848 samo 2 i 53, a broj 1946 ima samo jednom broj 2 u svojoj faktorizaciji i nema broj 53, direktno smo proverili da je 2 jedini zajednički delilac za ova dva broja različit od 1, pa je samim tim i najveći.

Diskusija:

Sada ćemo proširiti primenu Euklidovog algoritma na traženje najvećeg zajedničkog delioca za više od dva broja. Najveći zajednički delilac brojeva a_1, a_2, . . . , a_n može se dobiti višestrukom primenom Euklidovog algoritma, o čemu govori sledeća teorema.

Teorema:

Za prirodne brojeve a_1, a_2, . . . , a_n, $(n > 3)$ važi

$$NZD(a_1, a_2, ..., a_n) = NZD((a_1, a_2, ..., a_{n-1}), a_n).$$

Dokaz:

Neka je

$$d = NZD(a_1, a_2, ..., a_n) \text{ i } d' = NZD(NZD(a_1, a_2, ..., a_{n-1}), a_n).$$

Kako $d|a_i$ za $i = 1, 2, ..., n$, to $d|NZD(a_1, a_2, ..., a_{n-1})$ i $d|a_n$, pa prema tome $d|d'$. Slično, zbog $d'|NZD(a_1, a_2, ..., a_{n-1})$ i $d'|a_n$, važi $d'|a_i$ za $i = 1, 2, ..., n$, pa $d'|d$. Prema tome $d = d'$. □

Primer:

Odrediti $NZD(75, 625, 1050, 1400)$.

Primenom Euklidovog algoritma kao u teoremi rešavamo zadatak:

$$NZD(75, 625, 1050, 1400) = NZD(NZD(75, 625, 1050), 1400) =$$

$$= NZD(NZD(NZD(75, 625), 1050), 1400)$$

Prvo tražimo $NZD(75, 625)$:

$$625 = 8 \cdot 75 + 25$$

$$75 = 3 \cdot 25$$

Dakle $NZD(75, 625) = 25$, pa se tražena jednakost svodi na:

$$NZD(75, 625, 1050, 1400) = NZD(NZD(25, 1050), 1400)$$

Sada tražimo $NZD(25, 1050)$:

$$1050 = 42 \cdot 25$$

Dakle $NZD(25, 1050) = 25$, pa se polazna jednakost svodi sada na:

$$NZD(75, 625, 1050, 1400) = NZD(25, 1400)$$

$$1400 = 56 \cdot 25$$

$$NZD(75, 625, 1050, 1400) = 25.$$

Zadatak 15.

Dokazati da za svaki prirodan broj n važi $6|n^3 + 5n$.

Analiza:

Postoji više načina na koji bismo mogli da započnemo rešavanje postavljenog zadatka. Navodimo tri načina.

1. način: Oslanjajući se na osnovne osobine kongruencija, zaključujemo da je dovoljno ispitati ostatke pri deljenju sa 6 brojeva $r^3 + 5r$, kada $r \in \{0, 1, 2, 3, 4, 5\}$. Ako je $n \equiv r \pmod 6$, onda je $n^3 + 5n \equiv r^3 + 5r \pmod 6$. Dakle, treba dokazati da je $r^3 + 5r \equiv 0 \pmod 6$, za $r \in \{0, 1, 2, 3, 4, 5\}$, što se može jednostavno proveriti.

2. način: Budući da za svaki prirodan broj n važi $5n \equiv -n \pmod 6$, dovoljno je dokazati da za svako n važi $6 \mid n^3 - n$. U ovom slučaju od koristi će biti činjenica da se $n^3 - n$ može rastaviti na linearne činioce,

$$n^3 - n = (n - 1)n(n + 1),$$

za razliku od $n^3 + 5n = n(n^2 + 5)$.

3. način: Matematička indukcija.

Rešenje:

1. način: Na osnovu osnovnih osobina kongruencija, dovoljno je ispitati ostatke pri deljenju sa 6 brojeva $r^3 + 5r$, kada $r \in \{0, 1, 2, 3, 4, 5\}$.

r	$r^3 + 5r$	$r^3 + 5r \pmod 6$
0	0	0
1	6	0
2	18	0
3	32	0
4	84	0
5	150	0

2. način: Posmatrajmo odgovarajuće jednakosti:

$$n^3 + 5n = n^3 - n + 6n = (n - 1)n(n + 1) + 6n$$

kako su $(n-1)$, n i $(n+1)$ tri uzastopna broja to je makar jedan od njih deljiv

sa 2 i jedan od njih deljiv sa 3, pa je samim tim i proizvod $(n-1)n(n+1)$ deljiv i sa 2 i sa 3, a kako su 2 i 3 dva uzajamno prosta broja, znači da je deljiv sa 6. Očigledno je $6n$ takodje deljiv sa 6, pa je i ceo zbir sa desne strane jednakosti deljiv sa 6, a samim tim i $n^3 + 5n$.

3. način: Ako je $n = 1$, onda tvrdjenje očigledno važi: $6 \mid 1^3 + 5 \cdot 1$.
Pretpostavimo da za neko n važi $6 \mid n^3 + 5n$. Tada je:

$$(n+1)^3 + 5(n+1) = n^3 + 5n + 3n(n+1) + 6.$$

Imajući na umu induktivnu pretpostavku, jedino što treba ispitati jeste da li $6 \mid 3n(n+1)$. Da ovo poslednje važi zaključujemo oslanjajući se na iste argumente kao u prethodnom rešenju. Naravno, i ono se može dokazati indukcijom.

Dokaz:
Dokaz sledi iz pravila deljivosti i osobina brojeva.

Diskusija:
Na osnovu ovog primera možemo rešavati zadatke sa konkretnim vrednostima broja n. Recimo tako znamo za brojeve za koje je teško direktno ispitati deljivost ("velike" brojeve) da su deljivi sa 6. Primer $2017^3 + 5 \cdot 2017$ je deljiv sa 6 itd.

Zadatak 16.

Dokazati da proizvod dva cela pozitivna broja, od kojih je svaki manji od prostog broja p, nije deljiv sa p.

Analiza:
Ovo ćemo dokazati pretpostavljajući suprotno. Razmišljamo šta bi moralo da važi ako pretpostavimo da postoje neka dva cela pozitivna broja x i y koja su oba manja od prostog broja p, takva da $p|x \cdot y$. Razmatranjem ove pretpostavke u rešenju i koristeći pravilo da ako su dva izraza jednaka i važi da je jedan od njih deljiv nekim brojem, tada je i drugi izraz deljiv istim tim brojem.

Rešenje:
Pretpostavimo kao u Analizi da postoje dva cela pozitivna broja x i y koja su oba manja od prostog broja p, takva da $p|x \cdot y$. Dalje pretpostavimo da za njih važi da je njihov proizvod deljiv sa prostim brojem p. Ukoliko je to tačno dalje će postojati najmanji pozitivan broj $y_1 \leq y$, koji pri množenju sa x daje sadržalac broja p. Deljenjem y_1 sa p dobijamo:

$$y_1 = p \cdot m + n, n < y_1 < p$$

Odatle sledi:

$$n = y_1 - p \cdot m$$

Množenjem leve i desne strane sa x dobija se:

$$x \cdot n = y_1 \cdot x - p \cdot m \cdot x$$

Odatle se vidi da je $x \cdot n$ deljivo sa p, jer je proizvod $y_1 \cdot x$ deljiv sa p po pretpostavci da je y_1 najmanji broj za koji to važi, a $p \cdot m \cdot x$ je deljiv sa p jer je p jedan njegov činilac. Međutim $n < y_1$, pa y_1 neće biti najmanji pozitivan broj kojim treba pomnožiti x da se dobije sadržalac broja p, kao što je izrečeno u pretpostavci. Dakle dobijamo kontradikciju i otuda sledi da proizvod $x \cdot y$ nije deljiv sa p.

Dokaz:

Dokaz sledi direktno iz rešenja, jer smo na osnovu pretpostavke da važi suprotno dobili dva iskaza koja su protivrečna, samim tim sledi da je zaključak koji smo izveli jedino moguće tačno rešenje.

Diskusija:

Isti način rešavanja metodom suprotne pretpostavke bismo mogli da koristimo i za zadatak gde ne bismo posmatrali proizvod dva pozitivna cela broja manja od prostog broja p, već proizvoljan broj takvih brojeva. Dakle zaključujemo da će važiti i opštije da ako imamo n pozitivnih celih brojeva manjih od prostog broja p, tada njihov proizvod nije deljiv sa p.

Razmislimo sada kada će proizvod dva cela broja biti deljiv sa prostim brojem p. Nije teško zaključiti da će se to desiti ako i samo ako je bar jedan od ta dva broja deljiv brojem p. To ćemo lako i objasniti pretpostavljajući suprotno. Ukoliko ni jedan od dva broja koje množimo nije deljiv sa p, a njihov proizvod jeste deljiv, zaključujemo da u faktorizaciji ovih brojeva postoje neki činioci koji kada se pomnože daju broj koji je deljiv sa p. To je naravno nemoguće jer je p prost broj pa se ne može rastaviti na druge proste činioce.

Zadatak 17.

Odrediti proste brojeve p, q, r i s takve da je:

$$p \cdot q \cdot (r + s) = 2013.$$

Analiza:

Kako se traži da broj 2013 zapišemo kao proizvod neka tri broja, to ustvari znači da ga moramo rastaviti na činioce da bismo videli koji sve brojevi dolaze u obzir za izbor ova tri broja. Dalje ćemo koristiti i da je zbir parnog i neparnog broja neparan i razmatranje koji prost broj se može zapisati kao zbir dva prosta broja za deo $(r + s)$.

Rešenje:

Rastavljanjem broja 2013 na proste činioce dobijamo da je $2013 = 3 \cdot 11 \cdot 61$. Sva tri broja su prosta, pa sada razmatramo koji od njih mogu biti p i q, a koji može biti zbir prostih brojeva $(r + s)$. Najbitnije je prvo razmotriti $(r + s)$ jer vidimo da zbir dva prosta broja nikako ne može biti ni 3 ni 11, dakle preostaje nam samo da $r + s = 61$. Znači da će p i q biti iz skupa $\{3, 11\}$. Sada još da odredimo tačne vrednosti za r i s. Kako je 61 neparan broj dobijamo ga kao zbir jednog parnog i jednog neparnog broja (kada bi i r i s bili oba neparni, njihov zbir bi bio paran, što nam u ovom slučaju ne odgovara). Dakle kako je jedini prost paran broj 2 zaključujemo da jedan od brojeva r i s mora biti 2, a za drugi onda preostaje da bude 59, da bi u zbiru dali 61.

Skup rešenja je, dakle:

$$S(p, q, r, s) = \{(3, 11, 2, 59), (3, 11, 59, 2), (11, 3, 2, 59), (11, 3, 59, 2)\}.$$

Dokaz:

Dokaz da dobijena rešenja zadovoljavaju uslove zadatka izvešćemo direktnim zamenjivanjem dobijenih vrednosti na mesta odgovarajućih promenljivih p, q, r i s u polaznoj jednačini i proverom ispunjenosti jednakosti. Dakle za $(p, q, r, s) = (3, 11, 2, 59)$:

$$p \cdot q \cdot (r + s) = 3 \cdot 11 \cdot (2 + 59) = 3 \cdot 11 \cdot 61 = 2013.$$

Za $(p, q, r, s) = (3, 11, 59, 2)$:

$$p \cdot q \cdot (r + s) = 3 \cdot 11 \cdot (59 + 2) = 3 \cdot 11 \cdot 61 = 2013.$$

Za $(p, q, r, s) = (11, 3, 2, 59)$:

$$p \cdot q \cdot (r + s) = 11 \cdot 3 \cdot (2 + 59) = 11 \cdot 3 \cdot 61 = 2013.$$

Za $(p, q, r, s) = (11, 3, 59, 2)$:

$$p \cdot q \cdot (r + s) = 11 \cdot 3 \cdot (59 + 2) = 11 \cdot 3 \cdot 61 = 2013.$$

Time je dokazano da sva četiri rešenja zadovoljavaju polaznu jednakost i ona jesu rešenja ovog zadatka.

Diskusija:

Vidimo da zadatak ima četiri rešenja koja ispunjavaju uslove zadatka. Na sličan način smo mogli da rešimo svaki zadatak gde se traži da odredimo brojeve koji u proizvodu daju dati broj. Dakle, prvo rastavljamo na činioce, a zatim koristeći poznata pravila za brojeve dolazimo do zaključaka koji nas vode ka rešenju.

Zadatak 18.

Neka je n prirodan broj takav da broj $2n$ ima 28 pozitivnih delioca, a broj $3n$ ima 30 pozitivnih delioca. Koliko pozitivnih delioca ima broj $6n$?

Analiza:

Primetimo da $6 = 2 \cdot 3$, dakle kada pronađemo delioce broja $2n$ i broja $3n$, kombinacijom ta dva ćemo pronaći delioce broja $6n$. Kao što znamo svaki broj možemo da prikažemo kao proizvod svojih prostih delioca, pa ćemo to uraditi i za $2n$ i $3n$, pa na osnovu njih kasnije i za $6n$.

Rešenje:

Broj n prikažimo u obliku

$$n = 2^{e_1} \cdot 3^{e_2} \cdot p_3^{e_3} \cdots p_k^{e_k}.$$

Tada je

$$2n = 2^{1+e_1} \cdot 3^{e_2} \cdot p_3^{e_3} \cdots p_k^{e_k},$$
$$3n = 2^{e_1} \cdot 3^{1+e_2} \cdot p_3^{e_3} \cdots p_k^{e_k},$$
$$6n = 2^{1+e_1} \cdot 3^{1+e_2} \cdot p_3^{e_3} \cdots p_k^{e_k}.$$

Prema uslovu zadatka je

$$(2 + e_1)(e_2 + 1)(e_3 + 1) \cdots (e_k + 1) = 28,$$

$$(1 + e_1)(e_2 + 2)(e_3 + 1) \cdots (e_k + 1) = 30,$$

Stavimo $t = (e_3 + 1) \cdots (e_k + 1)$. Tada je

$$(2 + e_1)(e_2 + 1)t = 28,$$

$$(1 + e_1)(e_2 + 2)t = 30.$$

Dakle, t je zajednički delilac brojeva 28 i 30 pa je $t = 1$ ili $t = 2$ (jer su to jedini zajednički delioci za 28 i 30).

Ako je $t = 1$, onda je

$$(2 + e_1)(e_2 + 1) = 28,$$

$$(1 + e_1)(e_2 + 2) = 30.$$

Odavde, rešavajući sistem, nalazimo $e_1 = 5$ i $e_2 = 3$. Tada je:

$$\tau(6n) = (2 + e_1)(2 + e_2)t = 7 \cdot 5 \cdot 1 = 35.$$

Ako je $t = 2$, onda je

$$(2 + e_1)(e_2 + 1) = 14,$$

$$(1 + e_1)(e_2 + 2) = 15.$$

Jednostavno se proverava da ovaj sistem jednačina nema rešenja u skupu celih brojeva:

$$2e_2 + 2 + e_1e_2 + e_1 = 14$$

$$e_2 + 2 + e_1e_2 + 2e_1 = 15$$

Kada od druge jednačine oduzmemo prvu dobijamo:

$$-e_2 + e_1 = 1$$

$$e_1 = e_2 + 1$$

Zamenom ovoga u drugu jednačinu sistema dobijamo:

$$(e_2 + 2)^2 = 15$$

Odakle vidimo da ova jednačina nema celobrojnih rešenja. Dakle 35 je jedino rešenje.

Dokaz: Dokaz sledi direktno iz računa prikazanog u Rešenju, a može se proveriti za konkretne vrednosti prirodnog broja n. Koristili smo u Rešenju i poznato tvrđenje za rastavljanje prirodnih brojeva na proizvod njihovih prostih delilaca i broj delilaca tako rastavljenog broja:

Prirodan broj

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

ima tačno

$$\tau(n) = (e_1 + 1) \cdot (e_2 + 1) \cdots (e_k + 1)$$

pozitivnih delioca.

Diskusija:

Vidimo da dati zadatak ima jedinstveno rešenje i ovakav način rešavanja se može primeniti u mnogim konkretnim zadacima gde je umesto proizvoljnog prirodnog broja n zadat konkretan broj. Na sličan način mogu se rešavati i zadaci gde su dati brojevi pozitivnih delioca brojeva $p_1 \cdot n$ i $p_2 \cdot n$, a traži se broj pozitivnih delioca broja $p_1 \cdot p_2 \cdot n$.

Zadatak 19.

Neka su x i y prirodni brojevi i $xy = 2013^{2014}$. Dokazati da broj $x + y$ nije deljiv brojem 2012.

Analiza:

Iz jednakosti $xy = 2013^{2014}$ treba izvesti zaključke na osnovu kojih bismo mogli da izvedemo $2012 \nmid x + y$. Kako je $2012 = 4 \cdot 503$, željeni zaključak ćemo dobiti ako uspemo da dokažemo i jednostavnije činjenice poput $4 \nmid x + y$ ili $503 \nmid x + y$. Ako razmišljamo praktično, prirodno je očekivati da se verovatno može pokazati $4 \nmid x + y$, i da je malo verovatno da je sastavljač zadatka predvideo ispitivanje deljivosti sa 503, ili da je za rešenje baš neophodno razmatrati

broj 2012. Naravno, sve je moguće, ali uvek je dobra strategija najpre ispitati najjednostavnije mogućnosti. Ispostaviće se da iz $xy = 2013^{2014}$ zaista sledi da $4 \nmid x + y$, pa ostatak Analize navodimo kao Rešenje.

Rešenje:

Kako je $2013 \equiv 1 \pmod 4$, onda je i $2013^{2014} \equiv 1 \pmod 4$. Dakle, $xy \equiv 1 \pmod 4$, pa ostaje da ispitamo koji su mogući ostaci pri deljenju sa 4 brojeva x i y.

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	**1**	2	3
2	0	2	0	2
3	0	3	2	**1**

Na osnovu navedene tabele, jednostavno dolazimo do zaključka da mora važiti jedna od sledeće dve mogućnosti:

$$x \equiv 1 \pmod 4, y \equiv 1 \pmod 4 \text{ ili } x \equiv 3 \pmod 4, y \equiv 3 \pmod 4.$$

Medjutim, u oba slučaja $x + y$ ne može biti deljivo sa 4, jer je

$$x + y \equiv 2 \pmod 4.$$

Dakle, $4 \nmid x + y$, a samim tim i $2012 \nmid x + y$.

Dokaz:

Iz osnovnih osobina brojeva i deljivosti koje smo koristili direktno sledi dokaz, tako da nema potrebe dodatno proveravati ispunjenost uslova zadatka.

Diskusija:

Ideja prikazana u rešenju ovog zadatka je jako primenljiva na većinu zadataka u kojima se dokazuje da ne važi deljivost. Često se u takvim primerima može iskoristiti parnost brojeva i na taj način doći do suprotnosti i zaključka da deljivost ne važi. Potrebno je dobro razumeti ideju rešenja i tada će primena sličnog rešavanja biti prirodna ideja i u drugim zadacima.

Zadatak 20.

Dokazati da je broj $512^3 + 675^3 + 720^3$ složen.

Analiza:

Direktno izračunavanje vrednosti datog izraza svakako ne obećava mnogo:

$$512^3 = 134\,217\,728,\ 675^3 = 307\,546\,875,\ 720^3 = 373\,248\,000,$$

$$512^3 + 675^3 + 720^3 = 815\,012\,603.$$

Da li je broj 815 012 603 složen? Pokušajmo da otkrijemo neke pravilnosti koje će nas posredno dovesti do odgovora.

Sama postavka zadatka ukazuje na poznati identitet

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx).$$

Naravno ovaj identitet ne rastavlja zbir kubova na činioce, pa se ne može direktno upotrebiti. Pokušajmo zato da otkrijemo neku vezu izmedju brojeva 512, 675 i 720 koja bi mogla biti od koristi. Rastavljanjem datih brojeva na činioce:

$$512 = 2^9,\ 675 = 3^3 \cdot 5^2,\ 720 = 2^4 \cdot 3^2 \cdot 5,$$

(uz malo truda) uočavamo da je

$$2 \cdot 720^2 = 3 \cdot 512 \cdot 675.$$

Dakle, za $x = 512$, $y = 675$, $z = 720$ imamo da je $2z^2 = 3xy$, odakle sledi da je $2z^3 = 3xyz$, pa je

$$x^3 + y^3 + z^3 = x^3 + y^3 - z^3 + 2z^3 = x^3 + y^3 + (-z)^3 - 3xy(-z).$$

Rešenje:

Posmatrajmo opšti oblik iz Analize. Koristeći vezu između brojeva x, y i z, ukoliko dobijeni izraz razložimo na činioce strogo veće od 1 imamo željeni zaključa je $x^3 + y^3 + z^3$ složen broj. Jasno, ovaj rezon važi i za ma koje druge brojeve za koje pomenuta veza važi, a zaključak ostaje isti (naravno, ako su i činioci koje dobijamo u razlaganju veći od 1).

Rastavićemo izraz sa desne strane jednakosti na sledeći način:

$$x^3 + y^3 + (-z)^3 - 3xy(-z) = x^3 + y^3 - z^3 + 3xyz =$$

$$= x^2(x+y-z) - xy(x+y-z) + y^2(x+y-z) + xz(x+y-z) + yz(x+y-z) + z^2(x+y-z) =$$

$$= (x + y - z)(x^2 - xy + y^2 + xz + yz + z^2)$$

Da je zadati broj složen sledi iz dobijenog identiteta, veze koju smo koristili u njegovom dobijanju i koja za pomenute brojeve važi, kao i činjenice da su $x + y - z > 1$ i $x^2 - xy + y^2 + xz + yz + z^2 > 1$ za date brojeve. Primetimo da bi ovo moglo da važi i za druge brojeve pod uslovom da zadovoljavaju gore pomenute uslove.

Dokaz:

Dokaz sledi iz toga što smo dokazali opštije, da je $x^3 + y^3 - z^3$ složen, gde x, y i z zadovoljavaju uslove koje smo pomenuli. Odakle proizilazi da važi i za našu trojku brojeva koji zadovoljavaju iste uslove.

Diskusija:

U ovom primeru smo videli da je nekada lakše rešiti zadatak uopštavajući ga i dokazujući da važi za veću grupu brojeva, pa zatim dokazano iskoristiti u konkretnom slučaju.

Zadatak 21.

Odredi poslednje dve cifre broja 6^{2014}.

Analiza:

Ovakvi zadaci se mogu rešavati na više načina, ali najčešće se radi direktno izračunavanje poslednje dve cifre prvih nekoliko brojeva iz niza 6, 6^2, 6^3, 6^4 $\cdots$. Primetimo pre samog rešenja da će vrednost poslednje cifre u bilo kom proizvodu uvek zavisiti samo od poslednjih cifara brojeva koji se množe, poslednje dve cifre proizvoda će analogno zavisiti samo od poslednje dve cifre činilaca i tako dalje.

Rešenje:

Neposrednim izračunavanjem utvrđujemo da se brojevi 6^2, 6^3, 6^4, 6^5, 6^6, 6^7, $\cdots$ završavaju redom ciframa 36, 16, 96, 76, 56, 36, $\cdots$. Dakle, periodično se ponavljaju poslednje cifre sa periodom od 5 brojeva. Da je 5 zaista period kojim se ponavljaju dvocifreni završeci brojeva 6^m, $m \geq 2$, sledi iz činjenice da je za svako $m \geq 2$, $6^m \equiv 6^{m+5} \pmod{100}$:

$$6^{m+5} - 6^m = 6^m(6^5 - 1) = 2^m \cdot 3^m \cdot 7775 = 2^m \cdot 3^m \cdot 311 \cdot 25$$

.

Kako je $2014 = 4 + 5 \cdot 402$, to se 6^{2014} završava istim ciframa kao 6^4, dakle sa 96.

Dokaz:

Dokaz sledi direktno iz Rešenja i Analize, gde je objašnjena opravdanost ovakvog rešavanja i nema potrebe dodatno je proveravati.

Diskusija:

Rešenje je očigledno jedinstveno jer se broj može završavati samo na jedan način sa određene dve cifre i to se ne dovodi u pitanje. Pitanje je da li ovakav rezon možemo primeniti na druge zadatke. Odgovor je da možemo pa tako možemo izračunati koje su poslednje dve cifre broja 6 na bilo koji stepen. Dalje se rešenje može proširiti i na računanje poslednje dve cifre bilo kog prirodnog broja na bilo koji stepen, samo je potrebno da se utvrdi period ponavljanja dvocifrenog završetka kod prvih nekoliko stepena datog broja direktnim izračunavanjem. Očigledno da tako ne moramo gledati samo dvocifreni završetak, samo će se zadatak dodatno zakomplikovati što više poslednjih cifara se traži da odredimo. Lakše bi kod komplikovanijih primera bilo posmatrati ostatak pri deljenju datog broja sa odgovarajućom dekadnom jedinicom u zavisnosti koliko poslednjih cifara se traži da odredimo. Takav način je prikazan u Zadatku 33.

Zadatak 22.

Ako je

$$2A = 1 + \frac{1}{1+2} + \frac{1}{1+2+3} + \cdots + \frac{1}{1+2+\cdots+2014}$$

izračunati A.

Analiza:

Koristićemo formulu za zbir prvih n prirodnih brojeva:

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

i raščlanjivanje razlomka $\frac{1}{n(n+1)}$ na razliku dva razlomka na sledeći način:

$$\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$$

Rešenje:

Prvo ćemo primeniti formulu za zbir prvih n prirodnih brojeva na imenioce koji se pojavljuju u izrazu datom u zadatku. To možemo da uradimo jer su svi imenioci zbirovi prvih nekoliko prirodnih brojeva. Dakle dobijamo:

$$1 + 2 = \frac{2 \cdot 3}{2}$$

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

$$\vdots$$

$$1 + 2 + 3 + \cdots + 2014 = \frac{2014 \cdot 2015}{2}$$

Sada polaznu jednakost možemo zapisati u skraćenom obliku:

$$2A = 1 + \frac{1}{\frac{2 \cdot 3}{2}} + \frac{1}{\frac{3 \cdot 4}{2}} + \cdots + \frac{1}{\frac{2014 \cdot 2015}{2}}$$

Što je dalje kada se reše dvojni razlomci ekvivalentno sa:

$$2A = \frac{2}{1 \cdot 2} + \frac{2}{2 \cdot 3} + \frac{2}{3 \cdot 4} + \cdots + \frac{2}{2014 \cdot 2015}$$

Kada poslednju jednakost podelimo sa leve i desne strane sa 2 dobijamo:

$$A = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{2014 \cdot 2015}$$

Sada ostaje još da primenimo rastavljanje razlomaka koji se pojavljuju u ovom zbiru na razlike po dva razlomka kao što je navedeno u Analizi i dobićemo:

$$A = 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{2014} - \frac{1}{2015}$$

Oduzimanjem odgovarajućih istih razlomaka dobija se da je $A = 1 - \frac{1}{2015}$, to jest sređivanjem ovoga $A = \frac{2014}{2015}$.

Dokaz:

Dokaz sledi direktno iz računa.

Diskusija:

Posebnost ovog zadatka je u tome što nam je na relativno lakom primeru prikazana ideja koja je primenljiva i u bilo kom drugom izboru brojeva. Sada ćemo prikazati kako bi na sličan način rešili zadatak gde nisu dati konkretni brojevi već opšti slučaj koji će čitalac dalje moći da primenjuje.

Neka je n prirodan broj. Ako je

$$2A = 1 + \frac{1}{1+2} + \frac{1}{1+2+3} + \cdots + \frac{1}{1+2+\cdots+n}$$

izračunati A.

Koristeći istu formulu iz Analize kao i u gore prikazanom Rešenju imamo:

$$1 + 2 = \frac{2 \cdot 3}{2}$$

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

$$\vdots$$

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

Sada polaznu jednakost možemo zapisati u skraćenom obliku:

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

Što je dalje kada se reše dvojni razlomci ekvivalentno sa:

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

Kada poslednju jednakost podelimo sa leve i desne strane sa 2 dobijamo:

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

Sada ostaje još da primenimo rastavljanje razlomaka koji se pojavljuju u ovom zbiru na razlike po dva razlomka kao što je navedeno u Analizi i dobićemo:

$$A = 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{n} - \frac{1}{n+1}$$

Oduzimanjem odgovarajućih istih razlomaka dobija se da je $A = 1 - \frac{1}{n+1}$, to jest sređivanjem ovoga $A = \frac{n}{n+1}$.

Zadatak 23.

Zapisati broj $2014,201420142014\cdots$ u obliku $\frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$.

Analiza:

Da bi neki broj x bio racionalan moraju postojati brojevi p i q takvi da je $p \in \mathbb{Z}$, $q \in \mathbb{N}$, $(p,q) = 1$ i $x = \frac{p}{q}$. Kako je broj $2014,201420142014\cdots$ beskonačan periodičan decimalan broj pretpostavljamo da će on zaista i biti racionalan, ali je za dokaz potrebno pronaći odgovarajuće p i q opisane gore.

Rešenje:

Neka je $2014,201420142014\cdots = x$. Tada je

$$10000x = 20142014,20142014\cdots,$$

pa je

$$10000x - x = 9999x = 20142014,20142014\cdots - 2014,201420142014\cdots = 20140000.$$

Odavde je $x = \frac{20140000}{9999}$.

Dokaz:

Dokaz da je rešenje koje smo dobili u skladu sa uslovima zadatka dobijamo direktnim pretvaranjem dobijenog razlomka u decimalni broj:

$$\begin{array}{l} 20140000 : 9999 = 2014,2014\cdots \\ \underline{19998} \\ \quad 1420 \\ \quad\;\; 0 \\ \quad\underline{14200} \\ \quad\;\; 9999 \\ \quad\underline{42010} \\ \quad\;\; 39996 \\ \quad\underline{\;\;2014} \\ \vdots \end{array}$$

Dakle rešenje zadovoljava uslove zadatka.

Diskusija:

Na isti način se dokazuje za svaki beskonačan periodičan decimalni broj da je racionalan, samo što se x ne množi uvek sa 10000, već sa dekadnom jedinicom koja ima onoliko nula kolike je dužine perioda koja se ponavlja u decimalnom broju. Takođe decimalni broj koji je periodičan počevsi od neke decimale, ali ne od prve, možemo da dovedemo prvo do periodičnog, pa da onda taj broj pretvaramo u razlomak. Neka je dat beskonačan periodičan broj:

$$A = a_1a_2...a_n, b_1b_2...b_m(c_1c_2...c_k)$$

Perioda koja se ponavlja je $c_1c_2...c_k$. Prvo moramo da broj A dovedemo do oblika gde se u decimalnom zapisu na mestu decimala pojavljuje samo perioda.

$$10^m \cdot A = a_1a_2...a_nb_1b_2...b_m, (c_1c_2...c_k)$$

Sada bi broj A trebalo pomnožiti sa stepenom broja 10 tako da perioda ostane nepromenjena:

$$10^k \cdot 10^m \cdot A = a_1a_2...a_nb_1b_2...b_mc_1c_2...c_k, (c_1c_2...c_k)$$

Sada možemo da oduzmemo $10^{k+m} \cdot A$ i $10^m \cdot A$ i tako se oslobodimo decimalnog broja sa desne strane, sve decimale će nestati i ostaje:

$$10^{k+m} \cdot A - 10^m \cdot A = a_1a_2...a_nb_1b_2...b_mc_1c_2...c_k - a_1a_2...a_nb_1b_2...b_m$$

$$(10^{k+m} - 10^m) \cdot A = a_1a_2...a_nb_1b_2...b_mc_1c_2...c_k - a_1a_2...a_nb_1b_2...b_m$$

$$A = \frac{a_1a_2...a_nb_1b_2...b_mc_1c_2...c_k - a_1a_2...a_nb_1b_2...b_m}{10^{k+m} - 10^m}$$

Dakle svaki beskonačan periodičan broj je racionalan.

4.3 Kongruencije i Diofantove jednačine

Zadatak 24.

Naći ostatak pri djeljenju broja 1978^{20} sa 125.

Analiza:

Kada rešavamo zadatke ovakvog tipa koristimo kongruencije i pravila koja važe za njih. Prvo pokušavamo da pronađemo najbliži broj broju 1978 koji je deljiv sa 125, dakle kongruentan sa 0 po modulu 125. Ovde ćemo ukratko prikazati osnovne osobine kongruencije koje možemo da koristimo:

a) Ako je $a \equiv b \pmod{m}$, onda brojevi a i b imaju isti ostatak pri djeljenju sa m.

b) Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a + c \equiv b + d \pmod{m}$ i $a - c \equiv b - d \pmod{m}$.

c) Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $ac \equiv bd \pmod{m}$.

d) Ako je $a \equiv b \pmod{m}$, onda je $a^k \equiv b^k \pmod{m}$.

Rešenje:

Kako je $1978 = 2000 - 22$ i broj 2000 je deljiv sa 125, to je:

$$2000 \equiv 0 \pmod{125}$$

$$1978 \equiv -22 \pmod{125}$$

Tada je

$$1978^{20} \equiv (-22)^{20} \pmod{125}.$$

Nadalje, je

$$(-22)^{20} = 484^{10} \equiv (-16)^{10} \pmod{125} = 256^5 \equiv 6^5 \pmod{125} \equiv 26 \pmod{125}.$$

Dakle ostatak pri deljenju broja 1978^{20} sa 125 je 26.

Dokaz:

Dokaz da rešenje zadovoljava uslove zadatka sledi iz računa prikazanog u Rešenju i osobina kongruencija prikazanih u Analizi.

Diskusija:

Na sličan način možemo rešavati svaki zadatak u kome se traži da se odredi ostatak pri deljenju neka dva broja, kao što je u Analizi već i objašnjeno, tako da ovaj zadatak ima svoju primenu na mnogobrojne zadatke iz iste klase.

Zadatak 25.

Dokazati da ni za jedan ceo broj n broj $n^2 + 3n + 5$ nije deljiv sa 121.

Analiza:

Budući da je $121 = 11^2$, prvo nam pada na pamet da ispitamo da li postoji

neko n za koje $11 \mid n^2+3n+5$. Ako takvo n ne postoji, odmah će slediti rešenje zadatka. Ako pak pronađemo takvo n, onda nas očekuju dodatna istraživanja. Iako je predložena strategija pomalo 'pešačka', možda nas navede i na neko elegantnije rešenje.

$n \pmod{11}$	n^2+3n+5	$n^2+3n+5 \pmod{11}$
0	5	5
1	9	9
2	15	4
3	23	1
4	33	0
5	45	1
6	59	4
7	75	9
8	93	5
9	113	3
10	135	3

Zaključujemo da $11 \mid n^2+3n+5$, jedino ako je $n \equiv 4 \pmod{11}$, odn. $n = 11k+4$, za neko k. Do istog zaključka brže dolazimo ako primetimo da je

$$n^2+3n+5 \equiv n^2-8n+16 = (n-4)^2 \pmod{11},$$

odakle sledi

$$11 \mid n^2+3n+5 \;\Leftrightarrow\; 11 \mid (n-4)^2 \;\Leftrightarrow\; 11 \mid n-4.$$

Dakle, ostaje samo da ispitamo da li 121 deli n^2+3n+5, kada je $n = 11k+4$, za neko k. Iz jednakosti

$$n^2+3n+5 = (11k+4)^2+3(11k+4)+5 = 121k(k+1)+33,$$

sledi da $121 \nmid n^2+3n+5$.

U narednom rešenju izložićemo pristup zasnovan na jednakosti

$$n^2+3n+5 = (n+7)(n-4)+33.$$

Rešenje:

Primetimo da je:

$$n^2+3n+5 = (n+7)\cdot(n-4)+33$$

Ovo nam je važno jer za brojeve $n+7$ i $n-4$ važi da ukoliko je

$$n+7 \equiv 0 \pmod{11},$$

tada je i
$n-4 = (n+7)-11 \equiv 0 \pmod{11}$, kao razlika dva broja koja su deljiva sa 11.

Dakle brojevi $n+7$ i $n-4$ će ili oba biti deljiva sa 11 ili neće ni jedan od njih biti deljiv sa 11.

Ukoliko su oba broja deljiva sa 11, tada je njihov proizvod deljiv sa 121 jer

se u proizvodu dva puta pojavljuje činilac 11, međutim kako 33 nije deljivo sa 121 to ni zbir $(n+7)\cdot(n-4)+33$ neće biti deljiv sa 121.

Ukoliko sada brojevi $n+7$ i $n-4$ nisu deljivi sa 11, tada ni njihov proizvod nije deljiv sa 11, a kako 33 jeste deljivo sa 11, dobijamo da zbir $(n+7)\cdot(n-4)+33$ neće biti deljiv sa 11, pa samim tim ni sa 121.

Dakle zaključak je da kako god da izaberemo ceo broj n broj n^2+3n+5 neće biti deljiv sa 121, što je i trebalo dokazati.

Dokaz:

Dokaz da rešenje koje smo prikazali zadovoljava uslove zadatka sledi iz pravila deljivosti i kongruencija.

Diskusija:

Zaključak iz ovog zadatka važi za bilo koji ceo broj n, kako takvih brojeva ima beskonačno mnogo primena je moguća u svakom konkretnom primeru. Recimo zadatak "Dokazati da broj $20162016\cdots2016^2+3\cdot20162016\cdots2016+5$ nije deljiv sa 121" bi mogao da bude rešen primenom ovog zadatka. To bi bila jedna konkretizacija opšteg zadatka koja ne izgleda toliko jednostavno kao što je to bio slučaj sa opštim primerom.

Zadatak 26.

Tri data cela broja su potpuni kvadrati. Ako je zbir ta tri broja deljiv sa 9, onda se među njima mogu izabrati dva čija je razlika deljiva sa 9.Dokazati.

Analiza:

Ostaci pri deljenju nekog broja sa 9 mogu biti 0, 1, 2, 3, 4, 5, 6, 7 i 8. Kako su nam ovde potrebni ostaci pri deljenju kvadrata brojeva sa 9 posmatraćemo prvo kvadrate ovih devet prirodnih brojeva koji su mogući ostaci za proizvoljan broj i njihove ostatke pri deljenju sa 9 ne bismo li uočili neku pravilnost.

$$0^2 = 0 \equiv 0 \pmod 9$$

$$1^2 = 1 \equiv 1 \pmod 9$$

$$2^2 = 4 \equiv 4 \pmod 9$$

$$3^2 = 9 \equiv 0 \pmod 9$$

$$4^2 = 16 \equiv 7 \pmod 9$$

$$5^2 = 25 \equiv 7 \pmod 9$$

$$6^2 = 36 \equiv 0 \pmod 9$$

$$7^2 = 49 \equiv 4 \pmod 9$$

$$8^2 = 64 \equiv 1 \pmod 9$$

Dakle možemo da izvedemo zaključak da su jedini ostaci pri deljenju kvadrata celih brojeva sa 9 brojevi 0, 1, 4 i 7. Ovaj zaključak će nam biti od koristi za

rešavanje ovog zadatka.

Rešenje:

Kao što smo u Analizi utvrdili pri deljenju sa 9, kvadrati celih brojeva mogu davati ostatke 0, 1, 4 i 7. Posmatrajmo sada zbirove ta tri cela broja. U zadatku se traži da zbir kvadrata zadata tri cela broja bude deljiv sa 9. To znači da kada saberemo ostatke pri deljenju svakog od ta tri broja sa 9 treba da dobijemo ostatak koji je deljiv sa 9, to jest da zbir nema ostatak pri deljenju sa 9. Ako ne bi bilo ponavljanja ova četiri broja imali bismo četiri mogućnosti za zbirove:

$$0 + 1 + 4 = 5 \equiv 5 \pmod 9$$

$$0 + 1 + 7 = 8 \equiv 8 \pmod 9$$

$$0 + 4 + 7 = 11 \equiv 2 \pmod 9$$

$$1 + 4 + 7 = 12 \equiv 3 \pmod 9$$

Vidimo da ni u jednom od ova četiri slučaja ne dobijamo zbir deljiv sa 9, dakle mora biti ponavljanja nekih od ovih cifara.

Dokaz:

Dokaz sledi direktno iz pravila o kongruencijama prikazanim u nekom od prethodnih zadataka i iz računa prikazanog u Rešenju. Takođe možemo direktno proveriti ispitujući šta se desava u slučajevima kada se neke od cifara ponavljaju. Sa tri ponavljanja jedino 0 daje zbir deljiv sa 9:

$$0 + 0 + 0 = 0 \equiv 0 \pmod 9$$

Sa dva ponavljanja imamo još tri mogućnosti:

$$1 + 1 + 7 = 9 \equiv 0 \pmod 9$$

$$4 + 4 + 1 = 9 \equiv 0 \pmod 9$$

$$7 + 7 + 4 = 18 \equiv 0 \pmod 9$$

Kao što vidimo iz ovih zbirova u sva četiri slučaja se pojavljuju po dva broja koji imaju isti ostatak pri deljenju sa 9. To znači da će njihova razlika imati ostatak 0 pri deljenju sa 9 i samim tim će razlika biti deljiva sa 9, što je i trebalo dokazati.

Diskusija:

Rešenje ovog zadatka se svelo na traženje svih mogućnosti za ostatke pri deljenju sa 9 kvadrata celih brojeva. Ovakav način rešavanja se može primeniti i na druge brojeve, samo se za veće brojeve broj mogućnosti za ostatke povećava, pa će biti teže proveriti sve slučajeve.

Zadatak 27.

Rešiti jednačinu $96x + 68y = 48$.

Analiza:

Primećujemo da je ovo jedna linearna Diofantova jednačina, za čije rešavanje imamo postupak u Dodatku, pa ćemo ga ovde primeniti da bismo pronašli sva njena rešenja.

Rešenje:

Proverimo prvo da li data jednačina ima rešenja. Za to je potrebno ispitati da li $NZD(96, 68)|48$, pa pronađimo prvo $NZD(96, 68)$:

$$96 = 1 \cdot 68 + 28$$

$$68 = 2 \cdot 28 + 12$$

$$28 = 2 \cdot 12 + 4$$

$$12 = 3 \cdot 4$$

Dakle $NZD(96, 68) = 4$, kako $4|48$ zaključujemo da naša jednačina ima rešenja.

Sada nam je potrebno jedno rešenje jednačine $96x + 68y = 4$, koje ćemo naći uz pomoć Euklidovog algoritma:

$$4 = 28 - 2 \cdot 12$$

$$4 = 28 - 2 \cdot (68 - 2 \cdot 28)$$

$$4 = 5 \cdot 28 - 2 \cdot 68$$

$$4 = 5 \cdot (96 - 68) - 2 \cdot 68$$

$$4 = 5 \cdot 96 + (-7) \cdot 68$$

Dakle jedno rešenje jednačine $96x + 68y = 4$ je $(5, -7)$. Kako je $48 : 4 = 12$, pomnožimo poslednju relaciju sa 12. Dobijamo da je:

$$96 \cdot 60 + 68 \cdot (-84) = 48,$$

odakle imamo jedno rešenje polazne jednačine i to je $(60, -84)$.

Sada je samo ostalo da zapišemo opšti oblik rešenja ove jednačine:

$$x = 60 + \frac{68}{4}t,$$

$$y = -84 - \frac{96}{4}t,$$

odnosno

$$x = 60 + 17t,$$

$$z = -84 - 24t.$$

Dokaz:

Dokaz ćemo izvesti direktnom proverom. Zamenićemo vrednosti koje smo dobili za x i y u polaznoj jednačini i proveriti da li je ispunjena jednakost:

$$96x + 68y = 96 \cdot (60 + 17t) + 68 \cdot (-84 - 24t) =$$

$$= 5760 + 1632t - 5712 - 1632t = 48$$

Diskusija:

Znanje rešavanja Diofantovih jednačina nam je alat koji možemo koristiti pri rešavanju i mnogih tekstualnih zadataka čiju postavku uspemo da zapišemo kao jednu diofantovu jednačinu. Primer za to je:

U jednoj prostoriji se nalaze stolice sa 3 *i sa* 4 *noge. Kada na sve stolice sedne po jedna osoba, u sobi ima ukupno* 69 *nogu. Koliko u prostoriji ima stolica sa* 3 *a koliko sa* 4 *noge?*

Kada na stolicu sa 3 noge sedne jedna osoba, onda je tu ukupno 5 nogu, a kada na stolicu sa 4 noge sedne jedna osoba, onda je tu ukupno 6 nogu. Označimo sa x broj stolica sa 3 noge, a sa y broj stolica sa 4 noge. Sada se ovaj zadatak može preformulisati da glasi: *Reši jednačinu* $5x + 6y = 69$. Takav zadatak bismo rešili na gore prikazan način.

Vidimo da je primena Diofantovih jednačina široka.

Zadatak 28.

Da li postoji neki prirodan broj koji pri deljenju sa 1001 daje ostatak 23, a pri deljenju sa brojem 1170 ostatak 42?

Analiza:

Kada bi postojao prirodan broj n sa ovim svojstvom, onda bi moralo da važi:

$$n = 1001x + 23$$

$$n = 1170y + 42,$$

tj.

$$1001x - 1170y = 19.$$

Dakle problem smo sveli na rešavanje ove Diofantove jednačine. Ukoliko ona ima rešenja takav broj postoji i možemo naći kog su oblika ti brojevi, a ukoliko jednačina nema rešenja prirodan broj sa ovim svojstvima ne postoji.

Rešenje:

Proverimo da li ova Diofantova jednačina ima rešenja. Tražimo $NZD(1170, 1001)$:

$$1170 = 1001 \cdot 1 + 169$$

$$1001 = 169 \cdot 5 + 156$$
$$169 = 156 \cdot 1 + 13$$
$$156 = 13 \cdot 12$$

zaključujemo da je $NZD(1170, 1001) = 13$. Kako $13 \nmid 19$, sledi da jednačina nema rešenja, tj. da ne postoji prirodan broj n sa ovim svojstvima.

Dokaz:

Rešenje je korektno jer smo zadatak sveli na rešavanje Diofantove jednačine, a ona zaista nema rešenja ukoliko $NZD(1170, 1001) \nmid 19$.

Diskusija:

Ovaj primer pokazuje da, za razliku od uslova u Kineskoj teoremi o ostacima, u opštem slučaju sistem kongruencija ne mora da ima rešenje. Samim tim broj sa traženim osobinama ne postoji.

Zadatak 29.

Neka je d bilo koji pozitivan ceo broj različit od 2, 5 i 13. Dokazati da postoje različiti a i b iz skupa $\{2, 5, 13, d\}$ takvi da $ab - 1$ nije potpun kvadrat.

Analiza:

Jasno je da ako su a i b oba iz skupa $\{2, 5, 13\}$ izraz $ab - 1$ jeste potpun kvadrat (što je i provereno u Rešenju). Tako da ostaje zanimljiv slučaj kada je $a = d$ ili $b = d$. Taj slučaj ćemo rešavati tako što ćemo pretpostaviti da u svakoj kombinaciji za a i b iz ovog skupa, $ab - 1$ jeste potpun kvadrat. Ukoliko dobijemo kontradikciju znači da postoji neki izbor za a i b tako da $ab - 1$ ne bude potpun kvadrat.

Dakle da dokažemo tvrđenje pokazaćemo da $2d - 1$, $5d - 1$ i $13d - 1$ ne mogu istovremeno biti kvadrati prirodnih brojeva. Kvadrat neparnog broja daje ostatak 1 pri deljenju sa 4 i 8, to je svojstvo koje se često koristi, dok je razmatranje ostataka pri deljenju sa 5 motivisano uslovom da je $5d - 1$ potpun kvadrat. Dakle od koristi će nam biti da razmotrimo ostatke pri deljenju potpunih kvadrata sa 4, 5 i 8, koji su prikazani u narednim tabelama:

n	0	1	2	3
$n^2 \pmod 4$	0	1	0	1

n	0	1	2	3	4
$n^2 \pmod 5$	0	1	4	4	1

n	0	1	2	3	4	5	6	7
$n^2 \pmod 8$	0	1	4	1	0	1	4	1

Rešenje:

Kao što smo pomenuli u Analizi, proverimo prvo šta se dešava kada su $a, b \neq d$.
$2 \cdot 5 - 1 = 10 - 1 = 9$ ($a = 2$, $b = 5$ ili $a = 5$, $b = 2$)
$2 \cdot 13 - 1 = 26 - 1 = 25$ ($a = 2$, $b = 13$ ili $a = 13$, $b = 2$)
$5 \cdot 13 - 1 = 65 - 1 = 64$ ($a = 5$, $b = 13$ ili $a = 13$, $b = 5$)

Direktnom proverom smo utvrdili da u svim slučajevima kada su oba $a, b \neq d$, $ab - 1$ jeste potpun kvadrat.

Pretpostavimo sada da je $a = d$, b će tada biti iz skupa $\{2, 5, 13\}$. Dakle proveravamo da li može neki od $2d - 1$, $5d - 1$ i $13d - 1$ da ne bude potpun kvadrat. Da bismo to dokazali pretpostavićemo suprotno. Neka su sva tri potpuni kvadrati. Posmatrajmo ostatke pri deljenju sa 4.

$$13d - 1 = k^2 \quad (1)$$

$$5d - 1 = l^2 \quad (2)$$

$$2d - 1 = m^2 \quad (3)$$

$$(1) \Rightarrow 13d \equiv 1, 2 \pmod 4 \Rightarrow d \equiv 1, 2 \pmod 4$$

1. slučaj: $d \equiv 1 \pmod 4 \Rightarrow d = 4k + 1$, za neko $k \in \mathbb{Z}$

$$(2) \Rightarrow 20k + 4 = 4(5k + 2) = l^2 \Rightarrow (\frac{l}{2})^2 \equiv 2 \pmod 5$$

tu imamo kontradikciju sa rezultatima u drugoj tabeli prikazanoj u Analizi, gde vidimo da su mogući ostaci potpunih kvadrata pri deljenju sa 5 samo 0, 1 ili 4, ali ne i 2. Dakle preostaje slučaj kada je $d \equiv 2 \pmod 4$.
2. slučaj: $d \equiv 2 \pmod 4 \Rightarrow d = 4k + 2$, za neko $k \in \mathbb{Z}$

$$(3) \Rightarrow m^2 \equiv 3 \pmod 8$$

Sada i ovde imamo kontradikciju sa rezultatima u trećoj tabeli prikazanoj u Analizi, gde vidimo da su mogući ostaci potpunih kvadrata pri deljenju sa 8 samo 0, 1 ili 4, ali ne i 3. Zaključujemo da $2d - 1$, $5d - 1$ i $13d - 1$ ne mogu sva tri da budu potpuni kvadrati, pa znači da postoji bar jedan koji nije i time je zadatak završen.

Dokaz:

Ono što smo koristili u zadatku su ostaci po modulu 4, 5 i 8 kvadrata prirodnih brojeva. Svi parni brojevi su oblika $2k$, dakle parni broj na kvadrat će biti oblika $4k^2$, a to je $\equiv 0 \pmod 4$. Što se tiče neparnih brojeva, oni su oblika $2k + 1$, pa je svaki neparan broj na kvadrat oblika $4k^2 + 4k + 1$, a to je $\equiv 1 \pmod 4$. Dakle kvadrati svih prirodnih brojeva daju ostatke 0 ili 1 pri deljenju sa 4.

Ostaci pri deljenju sa 5 za prirodne brojeve su 0, 1, 2, 3 ili 4, pa su ostaci po modulu 5 za kvadrate ovih brojeva 0, 1 ili 4. Slično za 8, ostaci za prirodne brojeve su 0, 1, 2, 3, 4, 5, 6 ili 7, pa su mogućnosti za ostatke kvadrata 0, 1, 4.

Koristeći se ovim znanjima i pravilima kongruencija došli smo do rezultata.

Diskusija:

U zadacima sa kvadratima brojeva često se koriste kongruencije po modulu nekih odgovarajućih brojeva za koje uočavamo određene pravilnosti. Tako smo i ovde iskoristili kongruencije po modulu 4, 5 i 8 da bi dokazali da neki broj ne može biti potpun kvadrat jer ne zadovoljava uslove koje kvadrati zadovoljavaju pri deljenju sa ova tri broja.

Zadatak 30.

Pronađite sve mogućnosti za pozitivne cele brojeve x, y i z takve da je $x \leq y \leq z$ i

$$x^3(y^3 + z^3) = 2012(xyz + 2).$$

Analiza:

Primetimo da je $2012 = 2 \cdot 2 \cdot 503$, pa je desna strana deljiva sa ovim brojevima, dakle da bi jednakost bila ispunjena i leva strana mora da bude deljiva sa 503 i 2^2. To ćemo iskoristiti da ispitamo mogućnosti za x, y i z.

Rešenje:

Ako $503|x$ tada 503^3 deli levu stranu jednakosti dok najviše 503^1 deli desnu stranu. Odatle zaključujemo da $503 \not| x$. Kako x deli levu stranu jednakosti, jasno je da mora da deli i $2012 \cdot (xyz + 2)$. Ako $x \not| 2012$, tada $x|xyz + 2$, pa $x|2$ (jer $x|xyz$), što je suprotno pretpostavci da $x \not| 2012$. Kada $x|2012$ mora biti $x = 2^a$ gde je $a \in \{0, 1, 2\}$. Ako je $x = 2^2$ tada 2^6 deli levu stranu dok najviše 2^3 deli desnu stranu, dakle $x \in \{1, 2\}$.

Kako je 503 prost broj, na osnovu Male Fermaove teoreme imamo:

$$y^{502} \equiv z^{502} \pmod{503}$$

Iz toga da $503|x(y^3 + z^3)$ i $503 \not| x$ imamo da $503|(y^3 + z^3)$, odnoso:

$$y^3 + z^3 \equiv 0 \pmod{503}$$

$$y^3 \equiv -z^3 \pmod{503}$$

Dalje imamo:

$$y^{3 \cdot 167} \equiv -z^{3 \cdot 167} \pmod{503}$$

$$\implies y \equiv -z \pmod{503}$$

Tako da $503|y + z$, pa je $y + z = 503k$.

Slučaj 1: $x = 1$

Tada jednačina postaje:

$$\begin{aligned} y^3 + z^3 &= 2012(yz+2) \\ 503k(y^2 - yz + z^2) &= 2012(yz+2) \\ k(y^2 - yz + z^2) &= 4yz + 8 \\ k(y-z)^2 + yz(k-4) &= 8 \end{aligned}$$

Kako je $yz(k-4) \leq 8$, mora biti $k \leq 4$ jer je $yz + 1 \geq y + z = 503k \geq 503 \implies yz \geq 502$. Pošto je $y^3 + z^3 = 2012(yz+2)$, zaključujemo da $y^3 + z^3$ mora da bude paran broj, što dalje znači da će y i z biti iste parnosti, pa će samim tim i $y + z$ biti paran broj. Ali kako imamo da je $y + z = 503k$ zaključujemo da je k paran. Dakle, $k \in \{2, 4\}$.

Ako je $k = 4$ tada $(y-z)^2 = 2$ što je nemoguće. Ako je $k = 2$ tada $2(y-z)^2 - 2yz = 8 \implies (y+z)^2 - 5yz = 4 \implies 2^2 \cdot 503^2 - 4 = 5yz$ ali leva strana nije deljiva sa 5 tako da rešenja nema kada je $x = 1$.

Slučaj 2: $x = 2$
Jednačina tada postaje:

$$\begin{aligned} y^3 + z^3 &= 503(yz+1) \\ k(y^2 - yz + z^2) &= yz + 1 \end{aligned}$$

Ako je $|y - z| > 1$, tada $k(y^2 - yz + z^2) \geq y^2 - yz + z^2 > yz + 1$, što nije tačno, dakle $y = z$ ili $|y - z| = 1$. Odatle imamo $2y^3 = 503y^2 + 503$, dakle 503 deli desnu stranu, pa sigurno deli i levu. Znači da $503|y$ pa $503^3|2y^3$, ali kako 503^3 ne deli desnu stranu to je kontradikcija. Znači $k = 1$ i onda je rešenje $(x, y, z) = (2, 251, 252)$.

Dokaz:

Proverimo direktnim izračunavanjem da li naše rešenje zadovoljava uslove:

$$x^3(y^3 + z^3) = 2012(xyz + 2)$$

$$\begin{aligned} 2^3 \cdot (251^3 + 252^3) &= 8 \cdot (251 + 252) \cdot (251^2 - 251 \cdot 252 + 252^2) = \\ &= 8 \cdot 503 \cdot (251 \cdot 252 - 251 - 251 \cdot 252 + 251 \cdot 252 + 252) = \\ &= 8 \cdot 503 \cdot (251 \cdot 252 + 1) = 4 \cdot 503 \cdot (2 \cdot 251 \cdot 252 + 2). \end{aligned}$$

Diskusija:

Vidimo da je u ovom primeru rešenje jedinstveno, međutim da bi se došlo do takvog zaključka morali smo da ispitamo sve slučajeve i odbacimo sve druge mogućnosti. U ovakvim primerima važno je voditi računa da se ne ispusti neki slučaj i da se svaki do detalja razmotri da ne bi došlo do greške.

Zadatak 31.

Dokazati da se svaki ceo broj može zapisati u obliku $a^2 + b^2 - c^2$, gde su $a, b, c \in \mathbb{Z}$.

Analiza:

Razmotrimo identitet razlika kvadrata $a^2 - b^2 = (a + b)(a - b)$. U njemu su $a + b$ i $a - b$ iste parnosti, pa umemo da zapišemo u obliku $(a + b)(a - b)$ broj koji je deljiv sa 4 ili neparan. To je osnovna motivacija zašto ćemo u rešenju gledati posebno parne i neparne brojeve i stepen dvojke koji deli broj n.

Rešenje:

Ako je n neparan broj, onda se on može zapisati kao $n = 2k + 1$, za $k \in \mathbb{Z}$. Onda je:

$$n = 2k + 1 = (k + 1)^2 - k^2$$

tako da možemo uzeti da je $a = k + 1$, $b = 0$ i $c = k$. Time je slučaj neparnih brojeva rešen.

Za parne brojeve razlikujemo dva slučaja:
(1) $n = 2^{2k}(2l + 1)$
(2) $n = 2^{2k+1}(2l + 1)$, $k > 0$, $l \in \mathbb{Z}$.

U prvom slučaju je

$$n = 2^{2k}(2l + 1) = 2^{2k}((l + 1)^2 - l^2) = (2^k(l + 1))^2 - (2^k l)^2$$

tako da možemo uzeti da je $a = 2^k(l + 1)$, $b = 0$ i $c = 2^k l$. U drugom slučaju je

$$n = 2^{2k+1}(2l + 1) = 2^{2k} \cdot 2 \cdot (2l + 1) = 2^{2k}(4l + 2) =$$

$$= 2^{2k}(4l + 1 + 1) = 2^{2k}((2l + 1)^2 + 1^2 - (2l)^2) =$$

$$= (2^k(2l + 1))^2 + (2^k)^2 - (2^{k+1}l)^2$$

tako da možemo uzeti da je $a = 2^k(2l+1)$, $b = 2^k$ i $c = 2^{k+1}l$ i time je dokazano da za sve cele brojeve postoji traženi zapis.

Dokaz:

Rešenje smo dobili odgovarajućim transformacijama izraza do željenog oblika. Kako su ovim zaista obuhvaćeni svi celi brojevi imamo traženi rezultat.

Diskusija:

Primetimo u ovom zadatku da smo sve cele brojeve podelili u dve velike grupe, na parne i neparne brojeve. To je veoma čest slučaj da se u zadacima posebno posmatraju ove dve celine jer svaka za sebe ima osobine koje nam olakšavaju rad. Tako da nekada bude lakše dokazati da tvrđenje važi na dva manja skupa brojeva, pa odatle izvući opšti zaključak. Naglasimo ovde značaj primedbe da su brojevi koji učestvuju u razlaganju na činioce razlike kvadrata iste parnosti i motivacju za posmatranjem stepena dvojke koji deli n.

Zadatak 32.

Poslednja cifra broja $x^2 + xy + y^2$ je 0. Dokazati da su onda poslednje dve cifre ovog broja nule.

Analiza:

Da bismo dokazali da su poslednje dve cifre nekog broja nule možemo da koristimo kongruentnost po modulu 100. Ukoliko je $x^2+xy+y^2 \equiv 0 \pmod{100}$ onda se ovaj broj završava sa dve nule.

Rešenje:

Krenimo od toga da znamo da je poslednja cifra nula, dakle ovaj broj je deljiv sa 10. Ukoliko je broj deljiv sa 10, znači da je deljiv i sa 2 i sa 5. Dakle:

$$2|x^2 + xy + y^2,$$

$$5|x^2 + xy + y^2.$$

Da bi bilo ispunjeno da $2|x^2 + xy + y^2$ moraju i x i y biti deljivi sa 2. Ako su oba neparna ili jedan paran, a drugi neparan $x^2 + xy + y^2$ neće biti deljiv sa 2. A što se tiče deljivosti sa 5 imamo da ostati pri deljenju kvadrata prirodnog broja sa 5 motivišu na niz implikacija kojima od izraza x^2+xy+y^2 dolazimo do $x^2 + y^2 + (x + y)^2$ gde su sva tri sabirka zapisana kao kvadrati nekih prirodnih brojeva.

$$\begin{aligned} & 5|x^2 + xy + y^2 \\ \implies & 5|2(x^2 + xy + y^2) \\ \implies & 5|(x + y)^2 + x^2 + y^2 \end{aligned}$$

Mogući ostaci kvadrata pri deljenju sa 5 su 0, 1 i 4. Dakle mogućnosti su da $5|x$, $5|y$ i $5|x + y$ ili da je jedan od ova tri broja deljiv sa 5, a od druga dva jedan oblika $5k \pm 1$, a drugi oblika $5l \pm 2$, a kako je ovaj drugi slučaj nemoguć, ostaje da je tačan prvi i da su i x i y deljivi sa 5. Kako su oba deljiva i sa 2 i sa 5, sledi da su oba deljiva sa 10. Odatle zaključujemo da onda izraz $x^2 + xy + y^2$ mora biti deljiv sa 100, pa se ovaj broj zaista završava sa dve nule.

Dokaz:

Koristili smo pravila deljivosti i kongruencije, pa rezultat očigledno važi.

Diskusija:

Primetimo da ovaj rezultat možemo da koristimo i u konkretnim primerima kada se traži da se odrede poslednje dve cifre brojeva koji su oblika zadatog u primeru. Tada bi brojevi x i y morali da budu deljivi sa 10, pa bi na osnovu prethodnog imali da je ceo izraz deljiv sa 100 i da su poslednje dve cifre dve nule, mada za konkretne brojeve ovaj rezultat bi bio manje više očigledan i ne bi iziskivalo toliko razmatranja.

Zadatak 33.

Odrediti trocifreni završetak broja $2003^{2002^{2001}}$.

Analiza:

Grubo rečeno, strategija je da razmatranja svedemo na što manje brojeve. Osnovne osobine kongruencija nam omogućavaju da smanjimo osnovu stepena, Ojlerova teorema nam pomaže da smanjimo eksponent, a kineska teorema o ostacima može biti korisna da se razmatranje svede na kongruencije manjeg modula.

Rešenje:

Kao što smo primetili u Analizi, posmatrajmo kongruenciju po modulu 1000 datog broja:

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{1000}$$

Iz Ojlerove teoreme imamo da je $3^{400} \equiv 1 \pmod{1000}$, jer je $NZD(3, 1000) = 1$, a $\phi(1000) = 400$ pa će onda biti:

$$3^{2002^{2001}} \equiv 3^{2^{2001}} \pmod{1000}$$

Pronađimo sada ostatak pri deljenju 2^{2001} sa 400 da bismo ponovo primenili rezultat koji smo dobili iz Ojlerove teoreme. Kako $400 = 16 \cdot 25$, a 2^{2001} je deljivo sa 16, ostaje da odredimo ostatak pri deljenju sa 25. Kako je $\phi(25) = 20$ to je $2^{2001} \equiv 2 \pmod{25}$. Iz $2^{2001} \equiv 2 \pmod{25}$ i $2^{2001} \equiv 0 \pmod{16}$ imamo po Kineskoj teoremi o ostacima:

$$2^{2001} \equiv 352 \pmod{400}$$

Otuda je

$$3^{2^{2001}} \equiv 3^{352} \pmod{1000}$$

Kako je $1000 = 125 \cdot 8$, sada tražimo ostatke pri deljenju 3^{352} sa 8 i sa 125.

$$3^{352} = (3^2)^{176} \equiv 1 \pmod{8}$$

Kako je $\phi(125) = 100$ imamo da je $3^{352} \equiv 3^{52} \pmod{125}$. Koristićemo da je $3^6 \equiv 4 \pmod{125}$.

$$3^{52} = 3^4 \cdot 3^{48} = 3^4 \cdot (3^6)^8 \equiv 3^4 \cdot 4^8 \equiv 81 \cdot (2^7)^2 \cdot 4 \equiv$$

$$\equiv 81 \cdot 3^2 \cdot 4 \equiv 324 \cdot 9 \equiv 74 \cdot 9 \equiv 666 \equiv 41 \pmod{125}$$

Kako je $3^{52} \equiv 1 \pmod{8}$ i $3^{52} \equiv 41 \pmod{125}$ imamo da je

$$3^{52} \equiv 41 \pmod{1000}$$

Znači $2003^{2002^{2001}}$ se završava sa 041.

Dokaz:

U zadatku je korišćena Ojlerova teorema i Kineska teorema o ostacima, čija formulacija i dokaz se nalaze u Teorijskom dodatku.

Diskusija:

U ovom zadatku smo koristili Kinesku teoremu o ostacima za sistem od dve kongruencije, može se koristiti i za više kongruencija na sličan način i vrlo je primenljiva kada želimo da problem rešavanja kongruencije svedemo na više lakših.

5 Teorijski dodatak

5.1 Deljivost

Definicija 1.
Ceo broj a deljiv je celim brojem b, različitim od nule, ako postoji ceo broj q takav da je $a = bq$. Ako je broj a deljiv brojem b, pišemo $b|a$ ("b deli a").

Osobine relacije deljivosti:

1. Ako $b|a$, onda $b|ac$ za svako $c \in \mathbb{Z}$.
2. Ako $a|b$ i $b|c$, onda $a|c$.
3. Ako $a|b$ i $a|c$, onda $a|bx + cy$ za sve $x, y \in \mathbb{Z}$.
4. Ako $a|b$ i $b|a$, onda je $a = b$ ili $a = -b$.
5. Ako za pozitivne brojeve a i b važi $a|b$, onda je $a \leq b$.

Dokaz:

1. Ako $b|a$, onda postoji ceo broj m takav da je $a = mb$. No onda je $ac = mbc$, pa kako je mc ceo broj kao proizvod dva cela broja, sledi da $b|ac$.

2. Ako $a|b$ i $b|c$, onda postoje celi brojevi m i n takvi da je $b = ma$ i $c = nb$. No onda je $c = nma$, pa kako je nm ceo broj, sledi da $a|c$.

3. Ako $a|b$ i $a|c$, onda postoje celi brojevi m i n takvi da je $b = ma$ i $c = na$. No onda je

$$bx + cy = max + nay = (mx + ny)a.$$

Kako je $mx + ny$ ceo broj, to $a|(bx + cy)$.

4. Pretpostavimo da $a|b$ i $b|a$. Tada postoje $k, l \in \mathbb{Z}$ takvi da $a = kb$ i $b = la$, pa je $a = kb = kla$ odakle zaključujemo da je $kl = 1$. Kako su k i l celi brojevi i njihov proizvod jednak 1, oni su ili oba jednaka 1 ili -1. Dakle mora biti $a = b$ ili $a = -b$.

5. Ako $a|b$, tada po definiciji postoji nenegativan ceo broj m takav da je $b = ma$. Kako je $b > 0$, brojevi a i m su pozitivni, tj. $1 \leq a$ i $1 \leq m$, pa je $b = ma \geq a \cdot 1 = a > 0$. □

Kao posledica ovih osobina deljivosti važi sledeće svojstvo koje se često koristi u zadacima:

Ako se u jednakosti oblika

$$a_1 + a_2 + \cdots + a_k = 0$$

za sve sabirke osim jednog zna da su deljivi celim brojem p, onda je i taj sabirak deljiv sa p.

Teorema o deljenju sa ostatkom:
Za svaki ceo broj a i svaki prirodan broj b, postoje jedinstveni celi brojevi q i r takvi da važi jednakost:

$$a = bq + r, \quad 0 \leq r < b,$$

Pri tome q nazivamo količnikom, a r ostatkom pri deljenju broja a brojem b.

Dokaz:

Dokažimo najpre egzistenciju brojeva q i r. Razmotrimo najpre slučaj kada je $a \geq 0$. Označimo sa $S = \{m \in \mathbb{Z} : mb > a\}$. Kako je $a + 1 \in S$, to je S neprazan podskup skupa prirodnih brojeva $\mathbb{N}$, pa ima najmanji element. Neka je $s = \min S$ i $q = s-1$. Tada $q \notin S$, pa je stoga $qb \leq a$. Stoga je $r = a-qb \geq 0$. Sa druge strane je $sb > a$, jer je $s \in S$. Stoga je

$$b = sb - qb > a - qb = r,$$

čime smo dokazali da je $0 \leq r < b$. Iz jednakosti za r imamo da je $a = qb + r$. Neka je sada $a < 0$. Kako je $-a > 0$, prema dokazanom slučaju postoje $s', r' \in \mathbb{Z}$ takvi da je $-a = s'b + r'$ i $0 \leq r' < b$. Sada je $a = -s'b - r'$ i $-b < -r' \leq 0$. Ako je $r' = 0$, onda je za $q = -s'$ i $r' = 0$ tvrđenje zadovoljeno. Međutim, ako je $r' > 0$, onda $-r'$ ne zadovoljava tražene nejednakosti. Zbog toga radimo popravku:

$$a = -s'b - r' = -s'b - b + b - r' = (-s' - 1)b + (b - r').$$

Neka je $q = -s' - 1$, $r = b - r'$. Sada je $a = bq + r$. Proverimo nejednakosti za r. Kako je $0 < r' < b$, množenjem sa -1 dobijamo $-b < -r' < 0$. Dodavanjem b dobijamo $0 < b - r' < b$, tj. $0 < r < b$. Konačno imamo da je $a = bq + r$ i $0 < r < b$.
Ostaje da dokažemo jedinstvenost. Pretpostavimo da je $a = bq + r = bq_1 + r_1$, $0 \leq r, r_1 < b$. Ne umanjujući opštost dokaza možemo pretpostaviti da je $r \leq r_1$. Iz polazne jednakosti imamo da je $b(q - q_1) = r_1 - r$. Kako je $0 \leq r_1 - r < b$, to je $0 \leq b(q - q_1) < b$. Skraćivanjem sa b, dobijamo da je $0 \leq q - q_1 < 1$. Kako je $q - q_1$ nenegativan ceo broj, to je $q - q_1 = 0$. Otuda je $q = q_1$, pa je i $r = r_1$. □

Teorema
Ako $q|ab$ i pri tome su q i b uzajamno prosti brojevi onda $q|a$.

Dokaz:

Pretpostavićemo da je $a > 0$. Za $a < 0$ radili bi analogno. Prvo primetimo da $NZD(b, q) = 1$ povlači $NZD(ab, q) = NZD(a, q)$. Naime, broj $NZD(ab, q)$ deli brojeve ab i aq, pa deli i broj $NZD(ab, aq) = aNZD(b, q) = a$. Kako $NZD(ab, q)$ deli q sledi da $NZD(ab, q)$ deli $NZD(a, q)$. Međutim, broj $NZD(a, q)$ deli oba ab i q, pa $NZD(a, q)$ deli $NZD(ab, q)$, dakle $NZD(ab, q) = NZD(a, q)$. Kako iz pretpostavke $q|ab$ proizilazi $NZD(ab, q) = q$, to iz poslednje dokazane jednakosti izlazi $q|a$. □

Jedan od opštijih načina dobijanja kriterijuma deljivosti je tzv. Paskalov metod:

Teorema:
Da bi broj $a = \overline{a_n a_{n-1}...a_1 a_0} = \sum_{i=0}^{n} a_1 \cdot 10^i$ bio deljiv prirodnim brojem m, neophodno je i dovoljno da je sa m deljiv zbir

$$a_n r_n + a_{n-1} r_{n-1} + ... + a_1 r_1 + a_0 r_0,$$

gde su r_i proizvoljni celi brojevi za koje važi $10^i \equiv r_i \pmod{m}$ $(i = 0, 1, ..., n)$.

Dokaz:

Dokaz je očigledan jer je

$$a = \sum_{i=0}^{n} a_i \cdot 10^i \equiv \sum_{i=0}^{n} a_i r_i \pmod{m}$$

□

Posledica:
Neka je t takav broj da je $10^t \equiv 1 \pmod{m}$. Da bi broj a bio deljiv sa m, neophodno je i dovoljno da je sa m deljiv zbir brojeva koji se dobijaju podelom zdesna nalevo broja a na grupe od po t cifara.

Dokaz:

Uzeti u u Teoremi da je $r_i = 10^i$ $(i = 0, 1, ..., t-1)$ i $r_{tq+i} = 10^i$ $(q \in \mathbb{N})$, jer $10^{tq+i} \equiv 10^i \pmod{m}$. □

Posledica:
Neka je t takav broj da je $10^t \equiv -1 \pmod{m}$. Da bi broj a bio deljiv sa m, neophodno je i dovoljno da je sa m deljiv zbir brojeva koji se dobijaju podelom zdesna nalevo broja a na grupe od po t cifara, ali im se još naizmenično menjaju znaci.

Dokaz:

Uzeti u u Teoremi da je $r_i = 10^i$ $(i = 0, 1, ..., t-1)$ i $r_{tq+i} = (-1)^q \cdot 10^i$ $(i = 0, 1, ..., t-1)$, $q \in \mathbb{N}$. □

Birajući na odgovarajući način brojeve r_i, dobijamo razne kriterijume deljivosti. Najčešće se za brojeve r_i uzimaju ostaci pri deljenju brojeva 10^i sa m.

Sada ćemo dati neke od kriterijuma deljivosti prirodnih brojeva sa nekim od brojeva:

• 2: Broj n je deljiv sa 2 (ili drugačije rečeno, broj n je paran) akko se završava parnom cifrom, odnosno nekom od cifara 0, 2, 4, 6 ili 8.
Dokaz:
Dovoljno je u teoremi uzeti da je $r_0 = 10^0 = 1$ i $r_j = 0$ za $j \geq 1$. □

• 3: Broj n je deljiv sa 3 akko je zbir cifara broja n deljiv sa 3.
Dokaz:
Na osnovu Posledice imamo za $t = 1$ da je $10^1 \equiv 1 \pmod{3}$ pa kriterijum važi. □

• 4: Broj n je deljiv sa 4 akko se završava dvocifrenim brojem koji je deljiv sa 4.

Dokaz:

Dovoljno je u teoremi uzeti da je $r_i = 10^i = 1$ $(i = 0, 1)$ i $r_j = 0$ za $j \geq 2$. □

• 5: Broj n je deljiv sa 5 akko se završava nekom od cifara 0 ili 5.

Dokaz:

Dovoljno je u teoremi uzeti da je $r_0 = 10^0 = 1$ i $r_j = 0$ za $j \geq 1$. □

• 7: Broj $n = \overline{a_k a_{k-1} \cdots a_3 a_2 a_1}$ je deljiv sa 7 akko je i broj $m = \overline{a_3 a_2 a_1} - \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} - \cdots$ deljiv sa 7.

Dokaz:

Na osnovu Posledice imamo za $t = 3$ da je $10^3 \equiv -1 \pmod 7$ pa kriterijum važi.

• 8: Broj n je deljiv sa 8 akko se završava trocifrenim brojem koji je deljiv sa 8.

Dokaz:

Dovoljno je u teoremi uzeti da je $r_i = 10^i$ $(i = 0, 1, 2)$ i $r_j = 0$ za $j \geq 3$. □

• 9: Broj n je deljiv sa 9 akko je zbir cifara broja n deljiv sa 9.

Dokaz:

Na osnovu Posledice imamo za $t = 1$ da je $10^1 \equiv 1 \pmod 9$ pa kriterijum važi. □

• 10: Broj n je deljiv sa 10 akko se završava cifrom 0.

Dokaz:

Dovoljno je u teoremi uzeti da je $r_0 = 10^0 = 1$ i $r_j = 0$ za $j \geq 1$. □

• 11: Broj $n = \overline{a_k a_{k-1} \cdots a_3 a_2 a_1}$ je deljiv sa 11 akko je i broj $m = a_1 - a_2 + a_3 - a_4 + \cdots$ deljiv sa 11.

Dokaz:

Na osnovu Posledice imamo za $t = 2$ da je $10^2 \equiv 1 \pmod{11}$ pa kriterijum važi. □

• 13: Broj $n = \overline{a_k a_{k-1} \cdots a_3 a_2 a_1}$ je deljiv sa 13 akko je i broj $m = \overline{a_3 a_2 a_1} - \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} - \cdots$ deljiv sa 13.

Dokaz:

Na osnovu Posledice imamo za $t = 3$ da je $10^3 \equiv -1 \pmod{13}$ pa kriterijum važi. □

• 25: Broj n je deljiv sa 25 akko se završava dvocifrenim brojem koji je deljiv sa 25.

Dokaz:

Dovoljno je u teoremi uzeti da je $r_i = 10^i$ $(i = 0, 1)$ i $r_j = 0$ za $j \geq 2$. □

• 27: Broj $n = \overline{a_k a_{k-1} \cdots a_3 a_2 a_1}$ je deljiv sa 27 akko je i broj $m = \overline{a_3 a_2 a_1} + \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} + \cdots$ deljiv sa 27.

Dokaz:

Na osnovu Posledice imamo za $t = 3$ da je $10^3 \equiv 1 \pmod{27}$ pa kriterijum važi. □

• 37: Broj $n = \overline{a_k a_{k-1} \cdots a_3 a_2 a_1}$ je deljiv sa 37 akko je i broj $m = \overline{a_3 a_2 a_1} + \overline{a_6 a_5 a_4} + \overline{a_9 a_8 a_7} + \cdots$ deljiv sa 37.

Dokaz:

Na osnovu posledice imamo za $t = 3$ da je $10^3 \equiv 1 \pmod{37}$ pa kriterijum važi. □

• 100: Broj n je deljiv sa 100 akko se završava sa dve cifre 0 (tj. sa 00).

Dokaz:

Dovoljno je u teoremi uzeti da je $r_i = 10^i$ $(i = 0, 1)$ i $r_j = 0$ za $j \geq 2$. □

Zadaci za vežbanje:

1. Dokazati da je proizvod tri uzastopna cela broja deljiv sa 6 i da je proizvod četiri uzastopna cela broja deljiv sa 24.

2. Dokazati da razlomak $\frac{21n+4}{14n+3}$ ne može da se skrati ni za jedan prirodan broj n.

3. Ako prirodan broj n nije deljiv sa 7, dokazati da je jedan od brojeva $n^3 - 1$ i $n^3 + 1$ deljiv sa 7.

4. Petocifreni broj $\overline{a378b}$ je deljiv sa 72. Odrediti cifre a i b

5. Dokazati da $4n^2 + 4$ nije deljivo sa 19 ni za jedan prirodan broj n.

6. Ako se razlomak $\frac{an+b}{cn+d}$, $(n \in \mathbb{N})$ može skratiti sa k, onda je ceo broj $ad - bc$ deljiv sa k.

5.2 Prosti brojevi

Definicija 1.

Ceo broj $p > 1$ je prost ako p nema nijedan delilac d, $1 < d < p$. Ceo broj $m > 1$ koji nije prost je složen broj.

Teorema (Euklid):

Postoji beskonačno mnogo prostih brojeva. Drugim rečima, od svakog prostog broja postoji veći prost broj.

Dokaz:

Pretpostavimo suprotno tj. da ih ima konačno mnogo. Označimo ih sa $p_1, p_2, \cdots, p_n$ i posmatrajmo broj

$$P = p_1 \cdot p_2 \cdots p_n + 1$$

Tada P nije deljiv ni sa jednim prostim brojem p_i, a znamo da P mora biti ili prost ili ima prostog delioca (*Pomoćno tvrđenje*) koji je tada različit od svih p_i. To je u kontradikciji sa pretpostavkom te smo dokazali tvrđenje. □

Pomoćno tvrđenje:

Svaki prirodan broj $n \geq 2$ je ili prost ili je proizvod prostih brojeva.

Dokaz:

(1) Za $n = 2$ broj 2 je prost, pa tvrđenje važi.

(2) Neka je $n > 2$ prirodan broj. Pretpostavimo da tvrđenje važi za sve $k < n$. Broj n je prost, pa za njega tvrđenje važi, ili je složen pa se može napisati u obliku $n = k_1 \cdot k_2$, gde su k_1 i k_2 prirodni brojevi manji od n. Međutim za k_1 i k_2 važi indukcijska pretpostavka, pa su oni prosti ili proizvodi prostih brojeva. Dakle u tom slučaju je $n = k_1 \cdot k_2$ proizvod prostih brojeva. □

Teorema:

Ako je dat proizvoljan prirodan broj k, uvek se može naći k uzastopnih složenihi brojeva.

(Ova teorema govori o tome koliko su prosti brojevi retki u skupu prirodnih brojeva iako ih ima beskonačno mnogo)

Dokaz:

Primer ovakvih k uzastopnih složenih brojeva:

$$a_1 = (k+1) \cdot k \cdot (k-1) \cdots 3 \cdot 2 \cdot 1 + 2$$

$$a_2 = (k+1) \cdot k \cdot (k-1) \cdots 3 \cdot 2 \cdot 1 + 3$$

. . .

$$a_{k+1} = (k+1) \cdot k \cdot (k-1) \cdots 3 \cdot 2 \cdot 1 + k + 1$$

Teorema:

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$.

Dokaz:

Ova teorema je direktna posledica već dokazanog tvrđenja da ako $q|ab$ i q i a su uzajamno prosti, tada $q|b$.
Neka je p prost broj i neka $p|ab$. Pretpostavimo da p ne deli a, onda treba dokazati da $p|b$. Kako $p|ab$ i p i a su uzajamno prosti, na osnovu već dokazanog tvrđenja imamo da mora biti $p|b$. Slično se dokazuje ako pretpostavimo da p ne deli b. □

Teorema (Osnovni stav aritmetike):
Svaki prirodan broj a veći od 1 može se jednoznačno do na redosled faktora izraziti u obliku proizvoda prostih činioca.

Dokaz:

Egzistencija: Ako je a prost broj onda je dokaz gotov. Ako nije onda postoji najmanji prost broj q_1 takav da $q_1|a$, odakle imamo $a = q_1 \cdot a_1$ i $a > a_1$ jer je $q_1 \geq 2$. Sada analogno razmatranje primenimo na a_1. Dakle, ako je a_1 prost broj dokaz je gotov jer je $a = q_1 \cdot a_1$, ako a_1 nije prost onda postoji minimalni prost broj $q_2 \geq q_1$ (jer u suprotnom q_1 ne bi bio minimalan koji deli a) takav da $q_2|a_1$, odakle sada imamo $a_1 = q_2 \cdot a_2$ i $a_1 > a_2$ jer je $q_2 \geq 2$, itd. Tako dolazimo do niza prirodnih brojeva $a = a_0 > a_1 > a_2 \cdots > a_k > 1$ i algoritam staje kada je a_k prost. To se mora desiti jer između a i 1 ima konačno mnogo prostih brojeva. Ako sada među prostim brojevima $q_1 \leq q_2 \leq \cdots \leq q_k \leq a_k$ združimo one koji su jednaki u faktor na odgovarajući stepen, dobijamo traženu dekompoziciju.

Jedinstvenost: Pretpostavimo da imamo dva predstavljanja broja a kao proizvoda prostih brojeva, tj.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$
$$a = q_1^{\beta_1} g_2^{\beta_2} \cdots q_m^{\beta_m},$$

takvi da je $p_1 < p_2 \cdots < p_n$ i $q_1 < q_2 \cdots < q_m$. Sada pretpostavimo da postoji najmanji indeks i takav da je
$p_1 = q_1$, $\alpha_1 = \beta_1$; $p_2 = q_2$, $\alpha_2 = \beta_2$; $\cdots$ $p_{i-1} = q_{i-1}$, $\alpha_{i-1} = \beta_{i-1}$; i $p_i \neq q_i$ ili $p_i = q_i$, ali $\alpha_i \neq \beta_i$,
jer je u suprotnom dokaz gotov. Pretpostavimo da je npr. $p_i < q_i$ onda je i $p_i < q_j (j = i, \cdots, m)$, sada imamo sa jedne strane

$$p_i | a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

a sa druge

$$p_i \not| a = q_1^{\beta_1} g_2^{\beta_2} \cdots q_m^{\beta_m},$$

što je nemoguće. Slično dobijamo i u slučaju da je $p_i > q_i$.
Neka je sada $p_i = q_i$ ali je npr. $\alpha_i > \beta_i$ odakle
$a = p_i^{\alpha_i} \cdot a_1$, odakle $p_i^{\alpha_i} | a$ i $p_i \not| a_1$, $a = p_i^{\beta_i} \cdot a_2$, odatle dalje imamo $p_i^{\beta_i} | a$ i $p_i \not| a_2$,
tj. sa jedne strane $p_i^{\alpha_i} | a$, a sa druge strane $p_i^{\alpha_i} \not| a$, što je nemoguće. □

Kanonska faktorizacija:

Ako se u razlaganju broja n neki činioci ponavljaju, pa se p_1 javlja α_1 puta, p_2 javlja α_2 puta, $\cdots$, p_k javlja α_k puta, onda se oblik

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

zove se kanonski oblik prirodnog broja n.

Teorema:

Ako je proizvod dva uzajamno prosta prirodna broja kvadrat celog broja:

$$ab = c^2, \quad NZD(a, b) = 1,$$

tada su i a i b kvadrati celih brojeva:

$$a = a_1^2, \quad b = b_1^2.$$

Dokaz:

Neka je $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = q_1^{\beta_1} g_2^{\beta_2} \cdots q_m^{\beta_m}$. Kako je $NZD(a, b) = 1$, to je $p_i \neq q_j$ za svako $i \leq k$ i svako $j \leq m$. Otuda je

$$c^2 = a \cdot b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \cdot q_1^{\beta_1} g_2^{\beta_2} \cdots q_m^{\beta_m}.$$

Kako je izraz na desnoj strani, do na uređivanje po veličini osnova, prosta faktorizacija broja c^2, to je α_i paran broj za svako $i \leq k$, dok je β_j paran broj za svako $j \leq m$. To dokazuje da su a i b kvadrati prirodnih brojeva. $\square$

Teorema:

Neka je $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ kanonska faktorizacija broja a. Tada su svi pozitivni delioci broja a oblika:

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad 0 \leq \beta_1 \leq \alpha_1, 0 \leq \beta_2 \leq \alpha_2, \cdots, 0 \leq \beta_n \leq \alpha_n.$$

Ukupan broj pozitivnih delilaca broja a (uključujući i 1 i a) je

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1).$$

Definicija:

Ukupan broj pozitivnih delilaca prirodnog broja a označavamo sa $\tau(a)$.

U teoriji brojeva je veoma bitna i Ojlerova fi-funkcija, $\phi(n)$ koja predstavlja broj prirodnih brojeva manjih od n i uzajamno prostih sa n.

Osobine Ojlerove funkcije:

(1) $\phi(1) = 1$.

(2) Ako je p prost broj, tada je svaki prirodan broj j takav da je $j < p$ uzajamno prost sa p pa važi $\phi(p) = p - 1$.

Definicija:
Funkciju $f : \mathbb{N} \to \mathbb{C}$ za koju važi:
1. $f(1) = 1$,
2. $f(mn) = f(m)f(n)$ za sve m, n takve da je $NZD(m, n) = 1$,
zovemo multiplikativna funkcija.

Definicija:
Skup $\{x_1, ..., x_n\}$ zove se potpuni sistem ostataka modulo n ako za svaki $y \in \mathbb{Z}$ postoji tačno jedan x_j takav da je $y \equiv x_j \pmod{n}$.

Lema:
Ako je $ax \equiv ay \pmod{n}$ i $NZD(a, n) = 1$, onda je $x \equiv y \pmod{n}$.

Dokaz:

$ax \equiv ay \pmod{n}$ povlači da n deli $ax - ay$. Kako su a i n uzajamno prosti, n mora da deli $x - y$ i time je tvrđenje dokazano. □

Lema:
Ako je A potpun sistem ostataka modulo n, i m i c celi brojevi takvi da je $NZD(m, n) = 1$, tada je i skup $Am + c = \{am + c : a \in A\}$ potpun sistem ostataka.

Dokaz:

Neka je $am + c \equiv a_0m + c \pmod{n}$, gde su $a, a_0 \in A$. Oduzimanjem broja c i deljenjem sa m prema prethodnoj Lemi sledi da je $a \equiv a_0 \pmod{n}$ pa je $a = a_0$. Prema tome, svih n elemenata $am + c$ nalaze se u različitim klasama ekvivalencije pa zajedno čine potpun sistem ostataka modulo n. □

Teorema:
Ojlerova funkcija je multiplikativna funkcija.

Dokaz:

Neka su m, n prirodni brojevi takvi da $NZD(m, n) = 1$. Za $m = n = 1$ je $\phi(1) = 1$. Ako je $m = 1$ i $n > 1$, tvrđenje važi jer $\phi(1 \cdot m) = \phi(m) = 1 \cdot \phi(m) = \phi(1)\phi(m)$. Slično se proveri i za $n = 1$. Još preostaje da se proveri slučaj kada je $m, n > 1$. Sada složimo brojeve $1, 2, ..., mn$ u tablicu sa n redova i m kolona na sledeći način:

$$\begin{array}{cccccc} 1 & 2 & 3 & ... & m \\ m+1 & m+2 & m+3 & ... & 2m \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)m+1 & (n-1)m+2 & (n-1)m+3 & ... & nm \end{array}$$

Brojevi i iz tablice čine potpun sistem ostataka modulo mn pa postoji $\phi(mn)$ brojeva koji su uzajamno prosti sa mn, odnosno $NZD(i, m) = NZD(i, n) = 1$. Svi brojevi u datoj koloni su međusobno kongruentni po modulu m, tj. u istoj

koloni imamo brojeve koji pri deljenju sa m daju isti ostatak. Svim kolonama odgovara m klasa ekvivalencije modulo m. Dakle, brojevi u istoj koloni ili su svi uzajamno prosti sa m ili nijedan nije uzajamno prost sa m. Dakle, tačno $\phi(m)$ kolona sastoji se od brojeva uzajamno prostih sa m, dok ostale kolone sadrže brojeve i takve da je $NZD(i, m) > 1$.

Uzmimo sada jednu od tih $\phi(m)$ kolona. Neka je to k-ta kolona. Ta kolona je sastavljena od brojeva k, $m + k$, $2m + k$, ... , $(n - 1)m + k$. Prema Lemi brojevi iz te kolone čine potpun sistem ostataka modulo n, budući da svaki od tih brojeva daje različit ostatak pri deljenju sa n i $NZD(m, n) = 1$. Naime, kada bi dva broja $mx_1 + k$, $mx_2 + k$, $x_1, x_2 \in \{0, 1, ..., n - 1\}$, $(x_1 \neq x_2)$ davala isti ostatak pri deljenju sa n, imali bismo da je:

$$mx_1 + k \equiv mx_2 + k \pmod{n},$$

odnosno $mx_1 \equiv mx_2 \pmod{n}$. Kako je $NZD(m, n) = 1$ sledilo bi da je

$$x_1 \equiv x_2 \pmod{n}$$

što je nemoguće jer razlika dva različita broja iz skupa $\{0, 1, ..., n - 1\}$ ne može biti deljiva sa n. Dakle, svaka od kolona iz tablice sadrži $\phi(n)$ brojeva uzajamno prostih sa n pa tih $\phi(m)$ kolona daje $\phi(m)\phi(n)$ brojeva i uzajamno prostih i sa m i sa n. Znači, $\phi(mn) = \phi(m)\phi(n)$ i tvrđenje je dokazano. □

Propozicija:
Neka je p prost broj i $\alpha \in \mathbb{N}$. Tada važi

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Dokaz:

Neka je p prost broj i $\alpha \geq 1$. Pozitivni delioci broja p^α su $1, p, ..., p^\alpha$. Jedini brojevi i takvi da $1 \leq i \leq p^\alpha$ koji nisu uzajamno prosti sa p^α su sadržaoci broja p, a to su $1 \cdot p, 2 \cdot p, ..., p^{\alpha-1} \cdot p = p^\alpha$. Dakle, ima ih $p^{\alpha-1}$ pa je

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p - 1) = p^\alpha(1 - \frac{1}{p}).$$

□

Propozicija:
Za $n \in \mathbb{N}$ i $n > 1$

$$\phi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_n}).$$

Dokaz:

Prema Osnovnom stavu aritmetike znamo da se svaki prirodan broj $n > 1$ može zapisati u obliku $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, gde su $p_1 < ... < p_k$ prosti brojevi

i svaki $\alpha_i \geq 1$. Uzastopnom primenom svojstva multiplikativnosti funkcije ϕ i formule za $\phi(p^\alpha)$ dobijamo

$$\phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_k^{\alpha_k}) =$$

$$= p_1^{\alpha_1}(1 - \frac{1}{p_1})...p_k^{\alpha_k}(1 - \frac{1}{p_k}) =$$

$$= p_1^{\alpha_1}...p_k^{\alpha_k}(1 - \frac{1}{p_1})...(1 - \frac{1}{p_k}) =$$

$$= n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_n})$$

Zadaci za vežbanje:

1. Dokazati da brojevi $2^n - 1$ i $2^n + 1$, za $n > 2$, ne mogu istovremeno biti prosti.

2. Odrediti prost broj p ako se zna da su $p + 10$ i $p + 14$ prosti brojevi.

3. Ako su p i q prosti brojevi veći od 3, dokazati da $24|p^2 - q^2$.

4. Dokazati da zbir tri i više uzastopnih prirodnih brojeva nije nikada prost broj.

5. Dokazati da je zbir kvadrata bilo kojih pet uzastopnih celih brojeva deljiv sa 5, ali nije deljiv sa 25.

6. Naći sve parove prostih brojeva (p, q) takvih da je $2(p^6 - q^2) = (p - q)^2$.

5.3 Kongruencije

Definicija 1.

Za cele brojeve a i b koji pri deljenju sa $m \neq 0$ daju iste ostatke kaže se da su kongruentni po modulu m. Simbolički se to piše $a \equiv b(mod \quad m)$.

Osobine kongruencije:

1. $a \equiv b \pmod{m}$ ako i samo ako je $a = mt + b$ za neki ceo broj t.
2. $a \equiv b \pmod{m}$ ako i samo ako je razlika brojeva a i b deljiva sa m.

Teorema:

Neka su a, b, c, d, x i y proizvoljni celi brojevi, tada važi:

a) $a \equiv a \pmod{m}$. (osobina refleksivnosti)

b) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$ i $a - b \equiv 0 \pmod{m}$ su ekvivalentna tvrđenja. (osobina simetričnosti)

v) Ako je $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$ onda je i $a \equiv c \pmod{m}$. (osobina tranzitivnosti)

g) Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ onda je i $ax + cy \equiv bx + dy \pmod{m}$. (osobina linearnosti)

d) Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ onda je i $ac \equiv bd \pmod{m}$. (osobina multiplikativnosti)

đ) Ako je $a \equiv b \pmod{m}$ i $d|m$, onda je $a \equiv b \pmod{d}$.

Dokaz:

a) Važi jer $m|a - a$.

b) Ako je $a \equiv b \pmod{m}$, tada $m|a - b$, pa samim tim očigledno važi i $m|a - b - 0$, tako da je odatle $a - b \equiv 0 \pmod{m}$. Odavde sledi da $m| - (b - a)$ odnosno $m|b - a$, pa je $b \equiv a \pmod{m}$.

v) Zaista, ako je $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$, tada postoje celi brojevi s i t takvi da je $a = b + sm$ i $b = c + tm$. No onda je $a = c + (s + t)m$, što dokazuje da je $a \equiv c \pmod{m}$.

g) S obzirom na relacije $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ postoje celi brojevi s i t takvi da je $a = b + sm$ i $c = d + tm$. Odavde se dobija da je $ax + cy = bx + dy + (sx + ty)m$, pa relacija $ax + cy \equiv bx + dy \pmod{m}$ važi.

d) Ako je $a \equiv b \pmod{m}$, tada $m|a - b$, pa tim pre $m|(a - b)c$, odnosno $m|ac - bc$. Ali tada je $ac \equiv bc \pmod{m}$. Slično bi dobili i da je $bc \equiv bd \pmod{m}$. Kako je relacija kongruencije tranzitivna odatle imamo traženu relaciju da je $ac \equiv bd \pmod{m}$.

đ) Kako je $a \equiv b \pmod{m}$, to $m|a - b$. Pošto $d|m$, to zbog tranzitivnosti relacije $|$ sledi da $d|a - b$, pa je $a \equiv b \pmod{d}$. □

Teorema:

Neka su brojevi a i m uzajamno prosti. Ako je $ax \equiv ay \pmod{m}$, tada važi i $x \equiv y \pmod{m}$.

Dokaz:

Ako je $ax \equiv ay \pmod{m}$, onda je $a(x - y) = km$. Pošto je $NZD(a, m) = 1$, na osnovu jedne od prethodnih Teorema mora biti $x - y = \alpha m$, odnosno

$x \equiv y \pmod{m}$. □

Teorema:
Neka je $S = \{a_1, a_2, ..., a_n\}$ potpun sistem ostataka modulo n. Tada je i $\{b \cdot a_1, b \cdot a_2, ..., b \cdot a_n\}$ potpun sistem ostataka modulo n, za svaki ceo broj b za koji važi $NZD(b, n) = 1$.

Dokaz:

Brojeva ba_i ima isto koliko i brojeva a_i, dakle dovoljno je dokazati da su svaka dva elementa skupa $\{b \cdot a_1, b \cdot a_2, ..., b \cdot a_n\}$ međusobno nekongruentna modulo n (da pripadaju različitim klasama). Pretpostavimo da je $b \cdot a_i \equiv b \cdot a_j \pmod{n}$, za neke i, j. Kako su b i n uzajamno prosti, na osnovu prethodne Teorema imamo da je $a_i \equiv a_j \pmod{n}$. Iz činjenice da je S potpun sistem ostataka modulo n, zaključujemo da je $i = j$, čime je tvrđenje dokazano. □

Teorema (Mala Fermaova):
Ako je p prost broj i a ceo broj koji nije deljiv sa p, onda je

$$a^{p-1} \equiv 1 \pmod{p}.$$

Ova teorema se često zadaje i u obliku

$$a^p \equiv a \pmod{p},$$

gde je p prost broj, a a proizvoljan ceo broj.

Dokaz:

Oba skupa $\{1, 2, \cdots, p-1\}$ i $\{a, 2a, \cdots, (p-1)a\}$ čine potpune sisteme ostataka po modulu p. Prema tome, za svaki broj i postoji tačno jedan broj j, $1 \leq i, j \leq p-1$, takav da je $ai \equiv j \pmod{p}$. Ako pomnožimo sve kongruencije ovog oblika dobijamo da je $(p-1)! \equiv a^{p-1}(p-1)!$. Skraćivanjem $(p-1)!$ dobijamo traženo tvrđenje. □

Teorema (Ojler):
Ako je $(a, m) = 1$, onda je

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

U posebnom slučaju Ojlerova teorema, kada je $m = p$ prost broj (tada je $\phi(p) = p - 1$), je

$$a^{p-1} \equiv 1 \pmod{p}, \quad (a, p) = 1.$$

Dokaz:

Dokaz je analogan dokazu Fermaove teoreme. Ako je $\{r_1, r_2, \cdots, r_{\phi(m)}\}$ sveden sistem ostataka po modulu m, onda je to i $\{ar_1, ar_2, \cdots, ar_{\phi(m)}\}$. Prema tome, proizvodi elemenata u ova dva skupa su jednaki po modulu m:

$$r_1 r_2 \cdots r_{\phi(m)} \equiv a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Ostaje da se skrati $r_1 r_2 \cdots r_{\phi(m)}$. $\square$

Teorema (Vilson):
Neka je p prost broj, tada važi:

$$(p-1)! \equiv -1 \pmod{p}.$$

Dokaz:

Tvrđenje očigledno važi ako je $p = 2$ ili $p = 3$.
Neka je p prost broj veći od 3. Tada je $1 \equiv 1 \pmod{p}$ i $p - 1 \equiv -1 \pmod{p}$.
Da bismo dokazali teoremu, dovoljno je dokazati da za svaki broj x takav da je $2 \leq x \leq p-2$, postoji tačno jedan broj y takav da je:

$$x \cdot y \equiv 1 \pmod{p}, \quad 2 \leq y \leq p-2, x \neq y$$

Zaista, ako $x \in \{2, ..., p-2\}$, pošto je $NZD(x, p) = 1$, skup $\{0, x, 2x, ..., (p-1)x\}$ obrazuje potpuni sistem ostataka po modulu p, i tačno jedan element ovog skupa (koji je različit od nule) je kogruentan sa 1 po modulu p.
Ako bi bilo $y = 1$, imali bismo da je $x \equiv 1 \pmod{p}$, što je nemoguće.
Slično se dokazuje da ne može biti ni $y = p - 1$.
Najzad, ako bi bilo $x = y$, imali bismo da je $x^2 \equiv 1 \pmod{p}$, tj. da $p|x-1$ ili $p|x+1$, odnosno da je $x \equiv 1 \pmod{p}$ ili $x \equiv -1 \pmod{p}$, što je nemoguće. $\square$

Kineska teorema o ostacima:
Neka su $a_1, a_2, \cdots, a_r$ proizvoljni celi brojevi i neka su $m_1, m_2, \cdots, m_r$ po parovima uzajamno prosti prirodni brojevi, tj. $NZD(m_i, m_j) = 1$ za $i \neq j$. Tada postoji rešenje sistema kongruencija:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

Ako je x_0 jedno rešenje sistema jednačina, tada je x rešenje sistema ako i samo ako je oblika $x_0 + km$, gde je k proizvoljan ceo broj, a $m = m_1 m_2 \cdots m_r$.

Dokaz:

Pomoćna teorema:

Kongruencija $kx \equiv 1 \pmod{m}$ ima bar jedno rešenje (po x) ako i samo ako je broj k uzajamno prost sa m, i tada svaka od kongruencija $kx \equiv n \pmod{m}$ ima rešenje po x.

Dokaz:

Dokaz sledi iz činjenice da je $NZD(k,m) = 1$ ako i samo ako postoje $a, b \in \mathbb{Z}$ takvi da je $ak + bm = 1$.
□

Dokaz ćemo izvesti za sistem dve kongruencije:

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

pri čemu je $NZD(m_1, m_2) = 1$. Svako rešenje prve od ovih kongruencija je oblika $x = a_1 + ym_1$, $y \in \mathbb{Z}$. Ono je rešenje i druge od ovih kongruencija ako i samo ako je $m_1 y \equiv a_2 - a_1 \pmod{m_2}$. Pošto su m_1 i m_2 uzajamno prosti, na osnovu pomoćne teoreme sledi da poslednja kongruencija ima bar jedno rešenje y_0, pa je $x_0 = a_1 + m_1 y_0$ jedno zajedničko rešenje datog sistema kongruencija. Dalje, ako su x_0 i x_0' bilo koja zajednička rešenja datih kongruencija, iz $x_0 \equiv a_1 \pmod{m_1}$ i $x_0' \equiv a_1 \pmod{m_1}$ sledi da $m_1 | x_0 - x_0'$. Slično se dokazuje da $m_2 | x_0 - x_0'$, pa $NZS(m_1, m_2) | x_0 - x_0'$, tj. $x_0 \equiv x_0' \pmod{NZS(m_1, m_2)}$.
□

Zadaci za vežbanje:

1. Kojom cifrom se završava broj:
   a) 7^{2003}
   b) 777^{777}
   v) $((7^7)^7)^7$
   g) $7^{7^{7^7}}$?

2. Odrediti ostatak pri deljenju broja 317^{259} sa 15.

3. Dokazati da je za svaki prirodan broj n, broj $7^{2n} - 4^{2n}$ deljiv sa 33.

4. Koja je poslednja cifra broja $(9^9)^9$, a koja broja 9^{9^9}?

5. Dokazati da je $10! + 1$ deljiv sa 11.

5.4 Linearne Diofantove jednačine

Teorema:

Linearna Diofantova jednačina $ax + by = c$ ima rešenja ako i samo ako $NZD(a, b)|c$. U tom slučaju sva rešenja (ima ih beskonačno mnogo) date jednačine su:

$$x = \frac{c}{NZD(a,b)}x_0 + \frac{b}{NZD(a,b)}t,$$
$$y = \frac{c}{NZD(a,b)}y_0 - \frac{a}{NZD(a,b)}t, \quad (t \in \mathbb{Z})$$

gde je uređeni par (x_0, y_0) jedno rešenje jednačine $ax + by = NZD(a, b)$, koje se može odrediti, npr. Euklidovim algoritmom.

Dokaz:

Neka je $d = NZD(a, b)$. Ako $d \not| c$, onda je leva strana jednačine $ax + by = c$ deljiva sa d, a desna nije, pa jednačina nema rešenje.

Jednačina $ax + by = d$ uvek ima rešenje u skupu celih brojeva, koje se može dobiti npr. Euklidovim algoritmom.

Ako $d|c$, tada jednačina $ax + by = c$ ima rešenje

$$x_1 = \frac{c}{d}x_0, y_1 = \frac{c}{d}y_0,$$

gde je par (x_0, y_0) rešenje jednačine $ax + by = d$. Međutim, u tom slučaju jednačina ima beskonačno mnogo rešenja. Pretpostavimo da je (u, v) proizvoljno rešenje jednačine $ax + by = c$. Tada je:

$$ax_1 + by_1 = au + bv,$$

odakle je

$$\frac{a}{d}(u - x_1) = \frac{b}{d}(y_1 - v).$$

Kako je $d = NZD(a, b)$, to je $NZD(\frac{a}{d}, \frac{b}{d}) = 1$, pa $\frac{b}{d}|u - x_1$ i $\frac{a}{d}|y_1 - v$, odakle je $u = x_1 + \frac{b}{d}t$ i $v = y_1 - \frac{a}{d}t$, $t \in \mathbb{Z}$.
Neposrednom proverom vidimo da uređeni par (u, v) zadovoljava jednačinu $ax + by = c$ za sve $t \in \mathbb{Z}$.
□

6 Zadaci za samostalan rad

1. Da li je moguće umesto zvezdica u zapisu:

$$1 * 2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 = 30$$

staviti znake + i −, tako da se dobije tačna jednakost?

2. Dva igrača igraju sledeću igru: oni naizmenično pišu po tabli jednu do druge različite cifre sve dok je to moguće. U igri pobeđuje prvi igrač ukoliko uspe da tako dobijeni desetocifreni broj bude deljiv brojem 18, a u suprotnom pobednik je drugi igrač. Koji od igrača može sigurno da pobedi u ovoj igri bez obzira na to kako njegov protivnik igra, i na koji način će to postići?

3. Dat je niz brojeva 1234...9899100. Dva igrača na smenu upisuju između datih brojeva znakove +. − ili ·. Igra se odvija sve dok se ne popune sva slobodna mesta. Ako je konačan rezultat neparan broj, pobednik je prvi igrač, a kada je rezultat paran broj, pobedjuje drugi igrač. Može li jedan od igrača igrati tako da stalno pobeđuje?

4. Napisani su jedan za drugim prirodni brojevi: $123456789101112\cdots$. Koja je cifra na 1985. mestu?

5. Dečak ima 12 olovaka: zelenih isto koliko i žutih, a crvenih dva puta više nego plavih. Koliko olovaka svake boje ima dečak?

6. Napišite, jednu do druge, paran broj jedinica. Ako od tako nastalog broja oduzmete broj sa dva puta manje dvojki nego što je jedinica u prvom broju, onda će dobijena razlika biti potpun kvadrat nekog prirodnog broja. Dokazati.

7. Svi prirodni brojevi od 1 do 100 su podeljeni u dve grupe, na parne i neparne. Zatim su sabrane cifre kojima su zapisanni brojevi iz jedne, odnosno iz druge grupe. Koji od ta dva zbira je veći i za koliko?

8. Uzmimo sve cele brojeve od 1 do 1000000000. Podesnim grupisanjem ovih brojeva odrediti koliko iznosi zbir svih cifara koje su se morale upotrebiti da bi se napisali ovi brojevi.

9. Naći petocifreni broj $\overline{abcde}$ takav da su dvocifreni brojevi $\overline{ab}$, $\overline{bc}$, $\overline{cd}$ i $\overline{de}$ kvadrati celih brojeva.

10. Dokazati da postoji beskonačno mnogo prostih brojeva oblika $4n + 3$.

7 Deset mirakula

Pri računskim operacijama sa brojevima mogu se dobiti rezultati koji izazivaju i čuđenje i divljenje, poznati kao mirakuli. Evo nekoliko primera:

I

$$12345679 \cdot (1 \cdot 9) = 111111111$$
$$12345679 \cdot (2 \cdot 9) = 222222222$$
$$12345679 \cdot (3 \cdot 9) = 333333333$$
$$12345679 \cdot (4 \cdot 9) = 444444444$$
$$12345679 \cdot (5 \cdot 9) = 555555555$$
$$12345679 \cdot (6 \cdot 9) = 666666666$$
$$12345679 \cdot (7 \cdot 9) = 777777777$$
$$12345679 \cdot (8 \cdot 9) = 888888888$$
$$12345679 \cdot (9 \cdot 9) = 999999999$$

II

$$1 \cdot 8 + 1 = 9$$
$$12 \cdot 8 + 2 = 98$$
$$123 \cdot 8 + 3 = 987$$
$$1234 \cdot 8 + 4 = 9876$$
$$12345 \cdot 8 + 5 = 98765$$
$$123456 \cdot 8 + 6 = 987654$$
$$1234567 \cdot 8 + 7 = 9876543$$
$$12345678 \cdot 8 + 8 = 98765432$$
$$123456789 \cdot 8 + 9 = 987654321$$

III

$$0 \cdot 9 + 1 = 1$$
$$1 \cdot 9 + 2 = 11$$
$$12 \cdot 9 + 3 = 111$$
$$123 \cdot 9 + 4 = 1111$$
$$1234 \cdot 9 + 5 = 11111$$
$$12345 \cdot 9 + 6 = 111111$$

$$123456 \cdot 9 + 7 = 1111111$$
$$1234567 \cdot 9 + 8 = 11111111$$
$$12345678 \cdot 9 + 9 = 111111111$$
$$123456789 \cdot 9 + 10 = 1111111111$$

IV

$$9 \cdot 9 + 7 = 88$$
$$98 \cdot 9 + 6 = 888$$
$$987 \cdot 9 + 5 = 8888$$
$$9876 \cdot 9 + 4 = 88888$$
$$98765 \cdot 9 + 3 = 888888$$
$$987654 \cdot 9 + 2 = 8888888$$
$$9876543 \cdot 9 + 1 = 88888888$$
$$98765432 \cdot 9 + 0 = 888888888$$
$$987654321 \cdot 9 - 1 = 8888888888$$

V

$$11 \cdot 11 = 121$$
$$111 \cdot 111 = 12321$$
$$1111 \cdot 1111 = 1234321$$
$$11111 \cdot 11111 = 123454321$$
$$111111 \cdot 111111 = 12345654321$$
$$1111111 \cdot 1111111 = 1234567654321$$
$$11111111 \cdot 11111111 = 123456787654321$$
$$111111111 \cdot 111111111 = 12345678987654321$$

VI

$$143 \cdot 7 \cdot 111 = 111111$$
$$143 \cdot 7 \cdot 222 = 222222$$
$$143 \cdot 7 \cdot 333 = 333333$$
$$143 \cdot 7 \cdot 444 = 444444$$
$$143 \cdot 7 \cdot 555 = 555555$$

$$143 \cdot 7 \cdot 666 = 666666$$
$$143 \cdot 7 \cdot 777 = 777777$$
$$143 \cdot 7 \cdot 888 = 888888$$
$$143 \cdot 7 \cdot 999 = 999999$$

VII

$$1 + 2 + 1 = 2 \cdot 2$$
$$1 + 2 + 3 + 2 + 1 = 3 \cdot 3$$
$$1 + 2 + 3 + 4 + 3 + 2 + 1 = 4 \cdot 4$$
$$1 + 2 + 3 + 4 + 5 + 4 + 3 + 2 + 1 = 5 \cdot 5$$
$$1 + 2 + 3 + 4 + 5 + 6 + 5 + 4 + 3 + 2 + 1 = 6 \cdot 6$$
$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 6 + 5 + 4 + 3 + 2 + 1 = 7 \cdot 7$$
$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 = 8 \cdot 8$$
$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 = 9 \cdot 9$$

VIII

$$1 = \frac{1 \cdot 1}{1}$$
$$121 = \frac{22 \cdot 22}{1 + 2 + 1}$$
$$12321 = \frac{333 \cdot 333}{1 + 2 + 3 + 2 + 1}$$
$$1234321 = \frac{4444 \cdot 4444}{1 + 2 + 3 + 4 + 3 + 2 + 1}$$

IX

$$1 + 2 = 3 \quad i \quad 1^3 + 2^3 = 3^2$$
$$1 + 2 + 3 = 6 \quad i \quad 1^3 + 2^3 + 3^3 = 6^2$$
$$1 + 2 + 3 + 4 = 10 \quad i \quad 1^3 + 2^3 + 3^3 + 4^3 = 10^2$$
$$1 + 2 + 3 + 4 + 5 = 15 \quad i \quad 1^3 + 2^3 + 3^3 + 4^3 + 5^3 = 15^2$$

Uopšteno važi:

$$1^3 + 2^3 + ... + n^3 = (1 + 2 + ... + n)^2$$

Pokušajte da pronađete metod kako ovo dokazati.

X

$$11 \cdot 111 = 1221$$
$$111 \cdot 11111 = 1233321$$
$$1111 \cdot 1111111 = 1234444321$$

Literatura

[1] V. Baltić, *Teorija brojeva, Priprema za JMBO*, Beograd 2004.

[2] S. B. Branković, *Zbirka rešenih zadataka iz matematike za srednje škole, odabrana poglavlja*, Zavod za udžbenike, Beograd 2007.

[3] P. Vandendriessche, H. Lee, *Problems in Elementary Number Theory*, Jul 11, 2007. (http://www.artofproblemsolving.com/community/c146)

[4] H. Jamak, *Teorija brojeva, Okvirni program rada sa nadarenim učenicima osnovnih škola*, Prirodno-matematički fakultet, Sarajevo 2012.

[5] A. Jones (ed.), *Pappus of Alexandria Book 7 of the Collection*, Springer - Verlag, New York (1986).

[6] Z. Kadelburg, V. Mićić, S. Ognjanović, *Analiza sa algebrom 2*, Krug, Beograd 2005.

[7] V. Mićić, Z. Kadelburg, D. Đukić, *Uvod u teoriju brojeva, materijali za mlade matematičare, sveska 15*, DMS, Beograd 2004.

[8] B. Simić, *I to je matematika*, Zavod za udžbenike i nastavna sredstva, Beograd 1992.

[9] T. Tao, *Solving mathematical problems*, Department of Mathematics, UCLA, Los Angeles, CA 90095.

[10] $http://sh.wikipedia.org/wiki/Pap\_iz\_Aleksandrije$

[11] $http://en.wikipedia.org/wiki/Pappus\_of\_Alexandria$