Teorija brojeva u nastavi matematike

Obradović, Srđana

Master's thesis / Diplomski rad

2017

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:443360

SVEUČILIŠTE J. J. STROSSMAYERA U OSIJEKU

ODJEL ZA MATEMATIKU

Srđana Obradović

Teorija brojeva u nastavi matematike

Diplomski rad

Osijek, 21. travnja 2017.

SVEUČILIŠTE J. J. STROSSMAYERA U OSIJEKU

ODJEL ZA MATEMATIKU

SMJER: Sveučilišni nastavnički studij matematike i informatike

Srđana Obradović

Diplomski rad

Teorija brojeva u nastavi matematike

Voditelj diplomskog rada: doc. dr. sc. Ljerka Jukić Matić

Osijek, 2017.

Diplomski rad posvećujem svojoj obitelji, osobama koje su bezuvjetno vjerovale u mene. Također želim zahvaliti svojim krasnim cimericama i prijateljima koji su uvijek bili tu za mene i bez čije podrške ne bih bila sada ovdje gdje jesam. **Moji najdraži, hvala Vam svima!**

Sadržaj

Uvod

U ovom ću diplomskom radu govorit o osnovama teorije brojeva kojih bi učitelji u višim razredima osnovne škole i srednjim školama trebali biti svjesni. Ovo će gradivo biti poznato učiteljima koji su pohađali kolegije o teorijama brojeva, ali će uživati u važnim i elegantnim rezultatima koje čak i učenici srednjih škola mogu dokazati.

Teorija brojeva je grana matematike koja se uglavnom bavi cijelim brojevima. Već dugi niz godina njezina primjena u praktičnim situacija bila je ograničena, ali sa razvojem računala postaje važna za kriptografiju, generiranje slučajnog broja, i teorije kodiranja. Ove primjene izvan su dosega većine osnovnoškolskih učenika, ali postoje mnoge teme prikladne za istraživanje upravo i u osnovnoj školi.

Kroz rad također predstavljam razne zanimljive primjene koje se kreću od rekreacijskih područja poput numeričkih zanimljivosti i trikova do ozbiljne praktične primjene poput funkcioniranja računala i visoko razvijenih sigurnosnih sustava.

1 Parni i neparni brojevi

Razvrstavanje brojeva na parne i neparne jedna je od prvih tema teorije brojeva s kojom se djeca susreću. Počevši brojanjem po dva: $2, 4, 6, 8, 10 \ldots$ uče da je nešto posebno sa ovim brojevima. Ovo su parni brojevi, dok svi ostali, pozitivni cijeli brojevi neparni.

Učenici bi trebali razviti još jedan način utvrđivanja parnosti većih brojeva, a to je upravo primjena definicije parnih brojeva. Svi parni brojevi prilikom dijeljenja sa 2 nemaju ostatak, tj. on je 0, a neparni imaju ostatak 1.
Iako ovo izgleda kao poprilično laka ideja, samo 65% učenika četvrtog razreda može razvrstati dvoznamenkaste i troznamenkaste brojeve iz skupa prirodnih brojeva, na parne i neparne. Još manje učenika može primjeniti to znanje u problemskim zadacima.

Jedan od sličnih primjera je sljedeći zadatak.

Zadatak 1. *Pronađi pet neparnih brojeva čiji je zbroj* 100.

Nakon proučavanja zadatka, možda ćete se osjećati donekle frustrirano. Jeste li uspjeli pronaći bilo koju skupinu od pet brojeva koji daju zbroj 100? Možda čak pomislite da ne postoji takvih pet cijelih brojeva. Jeste li primijetili neke ponavljajuće obrasce u zbrojevima koje ste otkrili? Jesu li svi bili neparni? Možda ste pomislili, „Čekajte, zbroj pet neparnih brojeva mora biti neparan, tako da konačni zbroj ne može biti 100.“ Napokon!
Rješenje problema ovisi o shvaćanju da je zbroj dva neparna broja uvijek paran broj, a da je zbroj parnog i neparnog broja uvijek neparan broj. Ali kako znate da je zbroj dva neparna broja uvijek jednak broj? Ne mora značiti da je zbroj SVIH parova neparnih brojeva uvijek paran broj samo zato jer ste pokušali zbrajati neparne brojeve i uvijek dobili paran broj. Postoji li jednostavniji način da ovo dokažemo? Naravno! Sada ćemo vidjeti kako.

Postoji nekoliko načina da se ovaj problem riješi, ali posebno elegantan i jednostavan način je da shvatite da svaki paran broj može biti predstavljen kao neki drugi cijeli broj, ali dva puta veći. Na primjer, $2 = 2 \cdot 1$, $4 = 2 \cdot 2$, itd. To nas dovodi do

druge definicije parnog broja. Parni je broj bilo koji cijeli broj koji se može napisati kao dvostruki neki drugi cijeli broj. Broj n je paran u slučaju $n = 2k$ za neki cijeli broj k. Dakle, ako je paran broj broj u obliku $2k$, onda je neparan broj onaj koji je za jedan broj veći od parnog broja, također jednostavno definirati, tj. cijeli broj n je neparan u slučaju $n = 2k + 1$ za neki cijeli broj k.

Slijedeće pretpostavke su unutar dosega drugog i trećeg razreda osnovne škole. Ove pretpostavke možete učiniti prikladnijima za starije učenike pomoću slične izjave o produktima umjesto zbroja ili neka učenici sami dođi do njih.

Teorem 1. *(a) Zbroj dva neparna broja je paran.*

(b) Zbroj dva parna broja je paran.

(c) Zbroj tri neparna broja je neparan.

(d) Zbroj bilo kojeg broja parnih brojeva je paran.

(e) Zbroj neparnog broja neparnih brojeva je neparan.

(f) Zbroj dva neparna broja i jednog parnog je paran broj.

(g) Umnožak dva neparna broja je neparan broj.

(h) Ako pomnožimo paran broj s bilo kojim cijelim brojem, rezultat je paran broj.

Većina učenika dolazi do ovakvih zaključaka na temelju nekoliko primjera. Oni obično vjeruju da imaju dovoljno dokaza za prihvaćanje ovih odnosa kao činjeničnih. Učiteljeva je odgovornost da pouči učenike da promatranje tih primjera ne znači nužno da se ti zaključci mogu primijeniti u svim slučajevima. Ključan je viši stupanj shvaćanja koncepata i dokaza koji su temelj ovih odnosa. Čak i ako su dokazi previše komplicirani za učenike viših razreda osnovne škole i srednjih škola, učitelji ih mogu učiniti razumljivima učenicima na više neformalan način, ali samo ukoliko oni sami dobro shvaćaju te dokaze. Stoga, ovdje započinjemo proces vezan za prve teoreme potkrijepljene primjerima, trikovima i primjenama koji uključuju brojevne koncepte.

Dokaz. Nećemo ponuditi dokaze za sve ove slučajeve, ali ćemo dati dokaze za tvrdnje (b) i (g):

(b) Pretpostavimo da su M i N parni brojevi. Stoga, po definiciji parnog broja, svaki od ovih brojeva je dva puta veći od nekog drugog cijelog broja. Tako je $M = 2k$ i $N = 2l$ za neke cijele brojeve k i l. Trebamo pokazati da je zbroj ovih brojeva paran broj, što znači da zbroj također mora biti prikazan kao neki cijeli broj, ali dva puta veći. To radimo na sljedeći način:

$$M + N = 2k + 2l = 2(k + l)$$

I to je završetak postupka. Dokazali smo da je zbroj $M + N$ jednak duplo većem zbroju $k + l$.

(g) Pretpostavimo da su M i N neparni cijeli brojevi. U skladu sa definicijom neparnog broja, svaki od ovih je za jedan veći od parnog broja, tj. $M = 2k + 1$ i $N = 2l + 1$ za neke cijele brojeve k i l. Trebamo dokazati da je MN neparan broj, tj. da je u obliku $2m + 1$ za neki cijeli broj m. Ali,

$$MN = (2k + 1)(2l + 1) = 4kl + 2l + 2k + 1 = 2(2kl + l + k) + 1 = 2m + 1$$

gdje je $m = 2kl + l + k$. Stoga, umnožak dva neparna broja je neparan broj.

□

Možemo riješiti začuđujuće zahtjevne zadatke samo uz pomoć razmatranja jesu li brojevi u zadatku neparni ili parni. Dolje su navedeni neki zadaci za učenike srednjih škola. Prvi je sa natjecanja za srednje škole. Kalkulatori nisu bili dopušteni, a učenici su imali otprilike dvije minute za rješavanje zadataka.

Zadatak 2. *Od navedenih parova* (x, y)*, samo jedan od njih ne odgovara jednadžbi* $187x - 104y = 41$*. Koji je to par?*
Parovi: $(107, 192), (211, 379), (314, 565), (419, 753), (523, 940)$.

Rješenje.

Brzo rješenje bilo bi sljedeće: $104y$ je paran broj, dodajte 104y na obje strane jednadžbe $187x - 104y = 41$ kako biste dobili $187x = 104y + 41$. Desna strana jednadžbe je neparan broj, budući je to zbroj parnog i neparnog broja. Stoga, lijeva strana nove jednadžbe, $187x$, mora biti neparan broj. Ovaj postupak eliminira par čija je x koordinata 314, budući da je umnožak 187 i 314 neparan broj. Stoga, par $(314, 565)$ ne odgovara.

Sljedeći zadatak pokazuje kako se koncepti neparnih i parnih brojeva mogu koristiti za rješavanje trikova.

Zadatak 3. *Recite prijatelju da uzme kovanice od* 10 *lipa i* 5 *lipa i stavi jedan novčić u jednu ruku, a drugi u drugu. Možete se okrenuti prijatelju leđima dok on to radi. Recite mu da pomnoži vrijednost novčića u desnoj ruci s brojem* 8*, a vrijednost novčića u lijevoj ruci s brojem* 3*, nakon čega vam treba reći zbroj ta dva umnoška. Ako je zbroj paran broj, kovanica od* 10 *lipa je u njegovoj lijevoj ruci. Ako vam kaže da je rješenje neparan broj, kovanica od* 10 *lipa je u njegovoj desnoj ruci. Objasnite ovaj trik.*

Rješenje.

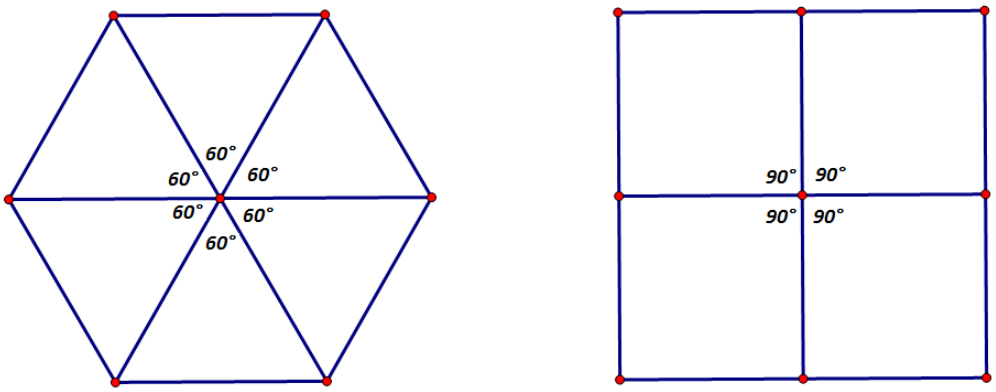
U ovom slučaju, trik je da shvatite da novčić od 10 lipa ima paranu vrijednos, a novčić od 5 lipa neparnu. Neka je d vrijednost novčića u lipama kojeg on drži u desnoj ruci, a l vrijednost novčića u lipama kojeg drži u lijevoj ruci. Vi tražite zbroj $8d+3l$. Sukladno tome, $8d$ je uvijek paran broj, a $3l$ će biti neparan ili paran broj, ovisno o tome je li l paran ili neparan. Ako je l paran broj, tj. ako je novčić od 10 lipa u njegovoj lijevoj ruci, zbroj $8d+3l$ biti će paran broj. Ako je l neparan broj, tj. ako je novčić od 5 lipa u njegovoj lijevoj ruci, zbroj će biti neparan broj.

Koncepti parnosti i neparnosti ovise o pitanju je li taj broj djeljiv s brojem 2. Ovaj koncept možemo primijeniti u svrhu proučavanja brojeva koji su djeljivi i s drugim brojevima osim s brojem 2. Na primjer, jedna od tema koji izdvajamo danas u školama je obrazac prepoznavanja. Stoga, npr. ako nabrojimo brojeve $3, 6, 9$, itd., uočavamo da je svaki broj višekratnik broja 3, ili, drugačije rečeno, svaki broj na popisu je djeljiv s 3. Što to znači da je broj djeljiv s 3? Vodimo se definicijom parnog broja. Broj N je djeljiv s 3, ako vrijedi da je $N = 3k$ za neki cijeli broj k. Broj N je djeljiv s 4, ako vrijedi da je $N = 4k$ za neki cijeli broj k, itd. Stoga, broj N je djeljiv s cijelim brojem a, ako vrijedi da je $N = ak$ za neki (jedinstveni) cijeli broj k.

Postoje i drugi načini na koje možemo pokazati da je broj N djeljiv s brojem a. Jedan od tih načina je naći rastav broja N na faktore, u kojemu je broj a . Drugi način je da je N višekratnik broja a ili da se broj N može podijeliti s brojem a ili da je broj a djelitelj broja N. Stoga, ako znamo da za cijeli broj vrijedi $N = 11k$ za neki cijeli broj k, odmah znamo da je N djeljiv s brojem 11.

Sljedeći zadatak povezan je i sa geometrijom.

Zadatak 4. *Prisjetimo se da pravilan mnogukut ima stranice jednake duljine i kutove jednake veličine. Stoga, jednakostranični trokut je pravilan mnogukut, kao i kvadrat. Ako uzmemo 4 kvadrata i postavimo ih oko središnje točke, možemo to napraviti na način da između njih ne ostane praznog prostora. Ako uzmemo 6 jednakostraničnih trokuta koji se podudaraju, možemo ih postaviti oko točke na isti način, tj. da između njih ne ostane praznog prostora kao na Slici 1.*



Slika 1

Dokaži da postoje samo tri pravilna mnogukuta koje na ovaj način možemo postaviti.

Rješenje. Trebamo se prisjetiti činjenice iz geometrije da, naime, za svaki unutarnji kut pravilnog mnogukuta vrijedi $\frac{180\cdot(n-2)}{n}$ gdje je n broj stranica. Ako se k ovih mnogokuta postave na način da nema prostora u centru, onda je zbroj kutova u središtu 360 stupnjeva, tj. $\frac{k\cdot 180\cdot(n-2)}{n} = 360$. Ako podijelimo to sa 180, dobijemo $\frac{k\cdot n - k\cdot 2}{n} = 2$. Kad pomnožimo obje strane s n, dobijemo $kn - 2k = 2n$, te kad oduzmemo $2n$ od obje strane i dodamo $2k$ na obje strane dobijemo $kn - 2n = 2k$. Naposljetku, izdvajamo n s lijeve strane i dijelimo s $k-2$ te dobijemo

$$n = \frac{2k}{k-2} = 2 + \frac{4}{k-2}$$

S obzirom da je lijeva strana jednakosti cijeli broj, cijeli broj je i desna strana. Stoga, $\frac{4}{k-2}$ je cijeli broj pa se $k-2$ dijeli s 4. Budući da $k-2$ dijeli 4, $k-2$ mora biti 1, 2 ili 4, stoga je $k = 3$, 4 ili 6. Kada uvrstimo ove vrijednosti, dobijemo da je $n = 6$, 4 ili 3. Zaključak je da su pravilni mnogukuti s kojima se može postići položaj naveden u zadatku samo šesterokut ($n = 6$), kvadrat ($n = 4$) i jednakostranični trokut ($n = 3$).

Teorem 2. *Ako su n i m djeljivi s a, onda su i $m+n$ i $m-n$ također djeljivi s a. Ili generalizirano: zbroj i/ili razlika skupa brojeva, od kojih je svaki djeljiv s a, je također djeljiva s a.*

Dokaz svake tvrdnje je identičan dokazu Teorema 1. (a).
Ilustrirat ćemo ovaj teorem jednostavnim primjerom.

Zadatak 5. *Dokaži da je jedini pozitivan cijeli broj n, koji dijeli cijele brojeve a i $a+1$, broj* 1.

Rješenje. Većina ljudi ne zna odakle bi počela u ovom zadatku. Ali, ako n djeli a i $a+1$, onda djeli i njihovu razliku $(a+1)-a$ ili 1. Ali jedini pozitivan cijeli broj koji djeli 1 je 1. Stoga, $n=1$.

Teorem 3. *Ako je m djeljiv s a, a n je bilo koji cijeli broj, onda je mn djeljiv s a.*

Dokaz. Moramo dokazati da je $mn = ak$ za neki cijeli broj k. Ali, m je djeljiv s a, stoga za neki cijeli broj m_1 vrijedi, $m = am_1$. To znači da je m djeljiv s a. Ako pomnožimo obje strane ove jednakosti s n, dobijemo da je $mn = am_1n$.
Stoga, $mn = ak$, gdje je k jednak m_1n pa je i mn djeljiv s a.
Jedna od zanimljivih igara za bolje upoznavanje sa parnim i neparnim brojevima je dobro poznati *Par-Nepar* u kojoj je cilj odrediti je li zbroj paran ili neparan broj, a može se igrati već u prvom razredu.
Ova igra vuče korijene iz antičkih vremena. Grci i Rimljani imali su svoje verzije ove igre, a ovo su njezina pravila:

- Jedan igrač odabire biti paran, a drugi neparan.
- Na "Tri, četiri, sad!" ili neki drugi dogovoreni uzvik igrači pokazuju $0, 1, 2, 3, 4$ ili 5 prstiju jedne ruke.
- Ako je zbroj pokazanih prstiju paran, "paran" igrač dobija bod. Analogno ako je zbroj neparan, "neparan" igrač dobija bod.
- Igra se dok jedan od igrača ne dostigne ciljani broj bodova (npr. 10).

Ovo je standardna i široko poznata verzija ove igre, ali postoje i varijacije kojima možete igru učiniti zanimljivijom, npr.:

- Igraju dva para kao dva tima. Jedan tim je "paran", a drugi "neparan". Zbrajaju se podignuti prsti sva četiri igrača, i pobjednički tim dobija bod istim prncipom kao i prije.
  Ova igra je ista kao i predhodna varijacija, ali u isto vrijeme omogućava vježbanje zbrajanja više brojeva.

- Igra sa n igrača, svatko za sebe. Igračima dodjelimo brojeve od 0 do $n-1$.
  Igra se na isti način kao i prije, ali zbroj se dijeli sa brojem n, tj. brojem igrača. Igrač kojemu je dodjeljen ostatak dobija bod.
  Npr. ako igraju 3 igrača dodjele im se brojevi $0, 1$ i 2. Svako podigne od 0 do 5 prstiju, te se suma svih prstiju dijeli sa 3. Ako je ostatak 0 igrač kojemu je dodjeljena 0 dobija poen, analogno i pri ostatku 1 i 2.
  Ova verzija igre može se koristiti i prilikom proučavanja modularne aritmetike koja će biti predstavljena kasnije u radu.

Nastavit ćemo s drugim zanimljivim i korisnim rezultatima koji uključuju koncept djeljivosti.

2 Djeljivost

Ovo poglavlje započet ću zadatkom.

Zadatak 6. *Koji je najmanji pozitivni cijeli broj koji ima samo parne znamenke, a djeljiv je s 9? Objasni svoj odgovor.*

Ako ne znate riješiti ovaj zadatak, nastavite čitati poglavlje i vratite se ovom zadatku poslije, nakon što otkrijete više „alata“ s kojima možete raditi na temu djeljivosti.

2.1 Osnovna pravila djeljivosti

Većina učenika viših razreda osnovne škole i učenika srednje škole znaju pravilo da, ako je broj djeljiv s 2, onda je njegova posljednja znamenka djeljiva s 2. Pravila djeljivosti za ostale brojeve su slabije poznata učenicima ali se uče već u petom razredu. Svaki učitelj bi trebao biti svjestan dokaza tih pravila i oni mu ne bi trebali predstavljati izazov da

ih možete pojasniti svojim učenicima, bez obzira na to što ih učenici ne moraju znati. Postoji nekoliko pravila djeljivosti koja su vrlo bitna i, iako ću ih dokazati za samo troznamenkaste brojeve, ona se odnose i na brojeve s bilo kojim brojem znamenaka.

2.1.1 Djeljivost s 2, 4, 5 i 8

Teorem 4. *Ako je posljednja znamenka broja n, djeljiva sa 2, onda je i n djeljiv s 2. Istovremeno, ako je broj n djeljiv s 2, onda je i njegova posljednja znamenka.*

Dokaz. Neka je n troznamenkasti broj te je pretpostavka da je njegova posljednja znamenka djeljiva s 2. Broj n možemo napisati u obliku $100s + 10d + j$. Očigledno, $100s + 10d$ je djeljivo s dva budući da ih možemo podijeliti s 2. Stoga, imamo

$$n = \underbrace{100s + 10d}_{\text{djeljivo s 2}} + \underbrace{j}_{\text{pretpostavka da je djeljiv s 2}}$$

Sada je n zbroj ova dva broja, koji je djeljiv s 2. Stoga, n mora biti djeljiv s 2 po Teoremu 1.
Da bismo dokazali obratan slučaj, preoblikovat ćemo $n = 100s + 10d + j$ na sljedeći način: $n - (100S + 10d) = j$. Sada pretpostavljamo da je n djeljiv s 2 i, budući da je $100s + 10d$ također djeljivo s 2, njihova razlika je djeljiva s 2 također po Teoremu 1.

Teorem 5. *Ako je dvoznamenkasti završetak broja n djeljiv sa 4, onda je i n djeljiv s 4. Istovremeno, ako je broj n djeljiv s 4, onda je i njegov dvoznamenkasti završetak.*

Dokaz. Dokazujemo da je, ako je broj kojeg tvore posljednje dvije znamenke broja djeljiv s 4, onda i sam broj djeljiv s 4. Ovu tvrdnju dokazujemo za četveroznamenkasti broj čija je tisućica a, stotica b, desetica c i jedinica d. Stoga vrijedi,

$$n = 1000a + 100b + 10c + d = \underbrace{1000a + 100b}_{\text{djeljivo s 4}} + \underbrace{10c + d}_{\text{pretpostavka da je djeljivo s 4}}$$

Prvi dio je automatski djeljiv s 4 budući da cijeli izraz možemo podijeliti s 4, a drugi je broj kojeg tvore posljednje dvije znamenke broja n, za koji pretpostavljamo da je djeljiv s 4. Napisali smo n kao zbroj dva izraza u zagradama, a svaka od njih je djeljiva s 4. Prema Teoremu 1, onda je i broj n djeljiv s 4.
Obrnuti postupak analogan je sa dosadašnjim dokazima, te ga ovdje neću iznjeti.

Teorem 6. *Broj n je djeljiv s 5, ako je njegova posljednja znamenka djeljiva s 5 i obrnuto.*

Dokaz je vrlo sličan dokazu djeljivosti brojem 2.

Teorem 7. *Ako je troznamenkasti završetak broja n djeljiv sa* 8*, onda je i n djeljiv s* 8 *i obrnuto.*

Dokaz je sličan dokazu djeljivosti brojem 4. Ovako što možemo ostaviti učenicima da to sami pokušaju. Kao primjer, 1234567 nije djeljiv s 8 zato jer broj kojeg tvore posljednje tri znamenke broja, tj. broj 567, nije djeljiv s 8.

2.1.2 Djeljivost s brojevima 3 i 9

Teorem 8. *Ako je zbroj znamenki broja n djeljiv s* 3*, onda je i broj n također djeljiv s* 3*. Obrnuto, ako je broj djeljiv s* 3*, onda je također i zbroj njegovih znamenaka.*

Kako bismo to ilustrirali, istražiti ćemo svojstva uz pomoć broja 231. Zbrajamo znamenke, $2+3+1=6$. S obzirom da je 6 djeljiv s 3, znamo da je i broj 231 djeljiv s 3. To možemo potvrditi na sljedeći način: $231:3=77$. Obrnuto, ako uzmemo broj 69, za koji znamo da je djeljiv s 3, uočavamo da je zbroj znamenki $6+9=15$ također djeljiv s 3. Ako želimo utvrditi je li neki veliki broj poput 1235492 djeljiv s tri, potrebno je zbrojiti njegove znamenke, $1+2+3+5+4+9+2=26$. S obzirom da broj 26 nije djeljiv s 3, ni prvotni broj nije djeljiv s 3.

Dokaz. Neka je broj $n=100s+10d+j$. Pokazat ćemo da, ako je zbroj znamenki $s+d+j$ djeljiv s 3, onda je i broj n. Preoblikujte n u obliku $n=99s+s+9d+d+j$ ili kao

$$n=\underbrace{99s+9d}_{\text{djeljivo s 3}}+\underbrace{s+d+j}_{\text{pretpostavka da je djeljiv s 3}}$$

Izraz u prvoj zagradi djeljiv je s 3, budući da ga možemo napisati kao $3(33s+3d)$. Nadalje, pretpostavljamo da je izraz u drugoj zagradi, zbroj znamenki, također djeljiv s 3. Stoga je n, budući da je on zbroj dva izraza u zagradama koji su djeljivi s 3, također djeljiv s 3 (Teorem 1). Da bi dokazali obrnuti slučaj, dovoljno je preoblikovati $n=(99s+9d)+(s+d+j)$ kao

$$\underbrace{n}_{\text{pretpostavka da je djeljiv s 3}}-\underbrace{99s+9d}_{\text{djeljivo s 3}}=s+d+j$$

i onda tvrditi da je, s obzirom da pretpostavljamo da je n djeljiv s 3, kao i $99s + 9d$, razlika $s + d + j$ također djeljiva s 3. Naravno, $s + d + j$ predstavlja zbroj znamenki. Stoga, ako je n djeljiv s 3, onda je i zbroj znamenki.

Teorem 9. *Broj je djeljiv s brojem* 9 *ako je zbroj njegovih znamenki djeljiv s* 9 *i obrnuto.*

Dokaz je praktički identičan dokazu djeljivosti s brojem 3 i učenici će vjerojatno htjeti znati zašto je to tako, stoga i ovo može biti prikladan zadatak za njih.

2.1.3 Djeljivost s brojem 11

Teorem 10. *Broj n je djeljiv s* 11 *ako od zbroja znamenki na neparnim pozicijama oduzmemo zbroj znamenki na parnim pozicijama i dobijemo broj koji je djeljiv s* 11*.*

Dokaz. pretpostavimo da se radi o troznamenkastom broju abc. Njega možemo zapisati i kao $100a + 10b + c$.
Ovo možemo transformirati u $99a+a+11b-b+c$, što je jednako $11(9a+b)+(a-2+c)$. Budući je prvi pribrojnik $11(9a + b)$ uvijek dijeljiv sa 11, trebamo provjeriti samo je li drugi pribrojnik $(a - 2 + c)$ dijeljiv sa 11, što je upravo i kriterij djeljivosti brojem 11. Postupak dokazivanja je analogan i za brojeve sa više znamenki, npr. za šesteroznamenkast:

$$100000a + 10000b + 1000c + 100d + 10e + f$$

$$100001a - a + 9999b + b + 1001c - c + 99d + d + 11e - e + f$$

$$11(9091a + 1111b + 91c + 9d + e) - (a - b + c - d + e - f)$$

iz čega je vidljvo da nam preostaje provjeriti je li $(a - b + c - d + e - f)$ djeljivo sa 11.

2.1.4 Djeljivost s brojem 6

Teorem 11. *Broj n je djeljiv s* 6*, ako je djeljiv s brojevima* 2 *i* 3*.*

Dokaz. Ako je broj djeljiv s 2, kada ga rastavimo na faktore, jedan od faktora bit će 2. Slično tome, ako je djeljiv s 3, kada ga rastavimo na faktore, imat će faktor 3. Stoga ako je dijeljiv i sa 2 i sa 3, kada ga podijelimo, imat će faktore 2 i 3. Stoga vrijedi da je $n = 2 \cdot 3 \cdot k$. To nam govori da je $n = 6k$ i da je djeljiv sa 6.

2.2 Primjena djeljivosti

Iako se ovi rezultati čine samo teoretskima, to zaista nije slučaj. Sada ćemo vidjeti praktičnu primjenu nekih od stvari koje smo ranije predstavili.
Kada idete u trgovinu, primijetit ćete da svaki proizvod koji kupujete ima crtični kod, tj. barkod. Primjer tipičnog crtičnog koda možete vidjeti na Slici 2.

Slika 2: Barkod

Uz pomoć ove etikete, obavlja se identifikacija proizvoda. Prvih šest znamenki koda predstavljaju proizvođača, a idućih šest opisuju proizvod. Svaki proizvođač ima svoj kod. Crtični kod očitava skener, koji onda identificira proizvođača i proizvod, nakon čega pronalazi cijenu proizvoda. Etiketa koju smo ovdje prikazali je etiketa male kutije grožđica. Tipična etiketa ima 12 znamenki, kao što to možete vidjeti na slici, uključujući i broj 0 na početku i broj 9 na kraju.
Zamislite sada da je skener na blagajni pogrešno skenirao etiketu i navodi da ste kupili kutiju deterdženta umjesto kutije grožđica pa vam je, umjesto nekoliko kuna za kutiju grožđica, naplaćen neki veći iznos. Ovo svakako nije dobra situacija. Stoga, svaki crtični kod ima nešto što se naziva „znamenkom provjere“ koja nas upozorava ako je došlo do pogreške te navodi prodavača da ponovi skeniranje. Znamenka provjere je uvijek posljednja znamenka crtičnog koda. U ovom slučaju, to je broj 9.
Skener zbraja sve znamenke na neparnim pozicijama kako bi dobio $0+5+0+0+2+4 = 11$ i množi ovaj zbroj brojem 3 da bi dobio broj 33. Ovome dodaje sve brojeve na parnim pozicijama, ali ignorira znamenku provjere, tj. ovome zbraja $7+7+0+3+1 = 18$. Za sada, ukupni zbroj je $33 + 18 = 51$. Znamenka provjere se uvijek bira na način da, kada se dodaje ukupnom zbroju, rezultat bude broj koji je djeljiv s 10. Naravno, $51 + 9 = 60$, što je djeljivo s 10. Ako se dogodi da, kada stroj pridoda znamenku provjere ukupnom zbroju, konačan rezultat nije djeljiv s 10, stroj obavještava blagajnika da je proizvod potrebno ponovo skenirati.
Ponekad stroj ne može skenirati etiketu pa blagajnik mora ručno unositi sve znamenke crtičnog koda. Naravno, može pogriješiti. Najčešće su pogreške unos pogrešne znamenke ili pogrešno upisan redoslijed znamenki (npr. umjesto 57 upiše 75). Sustav

prepoznaje pogrešku ako je makar jedna znamenka unesena pogrešno te će, u većini slučajeva, pronaći grešku ukoliko je došlo do slučajne zamjene znamenaka.

Već nakon naučene tablice množenja, u drugom razredu osnovne škole, djeca mogu riješavati neke zadatke vezane uz dijeljivost. Takav je i sljedeći zadatak.

Zadatak 7. *Morate podijeliti* 12 *bombona sa prijateljima. Svi moraju dobiti jednak broj bombona. Sa koliko sve prijatelja možete podjeliti bombone na taj način? Nacrtajte slike koje pokazuju na koje sve načine dijelite bombone.*

Rješenje.

- 12 prijatelja, svatko dobije po 1 bombon.
  Dvanaest grupa po jedan bombon

$$12 = 12 \cdot 1$$

- $11, 10, 9, 8, 7$ prijatelja ne mogu podijeliti pravedno.
- 6 prijatelja

12 je šest grupa po dva bombona

$$12 = 6 \cdot 2$$

- 5 prijatelja- Ne može!
- 4

Četiri grupe po tri bombona

$$12 = 4 \cdot 3$$

- 3

Tri grupe po četiri bombona

$$12 = 3 \cdot 4$$

- 2

Dvije grupe po šest bombona

$$12 = 2 \cdot 6$$

- 1

  To sam samo ja! Dobijam svih dvanaest bombona!

$$12 = 1 \cdot 12$$

3 Prosti i složeni brojevi

Zadatak 8. *Broj* $n = 49725$ *predstavlja umnožak godina skupine tinejdžera. O koliko tinejdžera je riječ i koja je njihova dob? Objasnite kako ste došli do rješenja.*

Pokušavajući riješiti prethodni zadatak može se naučiti puno toga o rastavljanju cijelih brojeva na faktore i o prostim brojevima. Istražit ćemo neka njihova svojstva u ovom dijelu poglavlja. Za ovu temu, ključan je koncept prostog broja.

Definicija 1. *Prost broj n je prirodan broj veći od 1, djelji bez ostatka samo s brojem* 1 *i samim sa sobom* 1.

Broj 2 bez ostatka djeljiv je samo s 2 i 1 tj. broj 2 možemo prikazati kao produkt $1 \cdot 2$, pa je broj 2 prost broj. Slično tome, broj 3 je također prost broj. Primijetite da

su prosti brojevi veći od broja 1.

Broj veći od 1 koji nije prost nazivamo složen broj. To znači da se on može prikazati kao produkt dva ili više manjih prostih brojeva. Broj 9 je složen broj jer se može napisati kao $3 \cdot 3$. Slično, broj 14 je složen broj jer se može napisati kao $2 \cdot 7$. Na primjer, $36 = 4 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3$.

Iako je očito da se svaki složen broj može rastaviti na proste faktore, moramo provjeriti je li to zaista tako. Idući teorem nam pokazuje da je to istina.

Teorem 12. *Svaki složeni broj n se može rastaviti na proste brojeve.*

Dokaz. Ako je n složen broj, može se rastaviti na dva manja faktora, a i b. Ako su a i b prosti brojevi, onda smo završili s postupkom. Ako nisu, onda se svaki od složenih faktora može opet rastaviti na manje brojeve. Ako su ti manji brojevi prosti, završili smo s postupkom. Ako nisu, svaki složeni faktor se može dalje rastaviti na manje brojeve. Ključna riječ ovog dokaza je „manji“. Ne možemo unedogled nastaviti rastavljati na faktore jer svaki puta dobijemo manje faktore, a postoji točno određen broj manjih cijelih brojeva koji su manji od n. To znači da postupak mora završiti, a završava u trenutku kada ne možemo pronaći manje faktore. U tom trenutku, svi preostali faktori su prosti brojevi.

Teorem 13. *Svaki cijeli broj $n > 1$ je ili prost broj ili se može rastaviti na proste faktore.*

Dokaz. Broj je ili prost ili složen. Ako je prost, postupak je završen. Ako je složen, može se rastaviti na proste brojeve uz pomoć predhodnog teorema.

Ovaj teorem se može činiti vrlo jednostavnim. Činjenica je da se svaki broj može rastaviti na proste faktore, ali je taj postupak dosta težak kada je u pitanju velik broj. Štoviše, ovaj postupak je temelj naše nacionalne sigurnosti. Mnoge tajne naše zemlje su šifrirane (kao i broj vaše kreditne kartice kada naručujete proizvode putem interneta) i koriste šifriranje koje se može dešifrirati samo ako otkrijete proste faktore određenih velikih brojeva. Problem leži u činjenici da su ovi brojevi jako veliki (sastoje se od nekoliko stotina znamenki) te bi otkrivanje prostih faktora, čak i uz pomoć računala, moglo trajati desetljećima. Stoga smo, za sada, dok netko ne otkrije brzi način rastavljanja brojeva na proste faktore, sigurni. Shema šifriranja je zanimljiva primjena prostih brojeva i više ćemo je predstaviti kasnije u poglavlju.

Također ćemo koristiti i sljedeći teorem.

Teorem 14. *Ako prost broj p dijeli umnožak ab, onda taj prost broj dijeli a ili b.*

Možete pomisliti da je rezultat očigledan. Potrebno je samo rastaviti a i b na proste brojeve, a ako p dijeli produkt tih prostih brojeva, on mora biti jedan od njih. Obratite pozornost na riječ „prost broj“ u teoremu. Rezultat je netočan ako izostavimo riječ „prost“. Na primjer, broj 18 možemo rastaviti na faktore u obliku $2 \cdot 9$, rezultat možemo podijeliti složenim brojem 6, ali broj 6 ne dijeli 2 niti 9.
Ovaj teorem se često koristi za dokazivanje različitih zadataka. Na primjer, ako znamo da broj 3 dijeli broj $(p^2 + 1)(q - 2)$ i znamo da ne dijeli prvi broj $p^2 + 1$, onda mora djeliti drugi broj, $q - 2$, s obzirom da je prost broj.

Ako po redu krenemo nabrajati proste brojeve, imamo $2, 3, 5, 7, 11, 13, 17, 19$, itd., čini se da ne postoje veći razmaci između uzastopnih prostih brojeva. Na primjer, 2 i 3 se razlikuju za $1, 5$ i 7 se razlikuju za $2, 7$ i 11 za 4, itd. Logično je postaviti pitanje – koliko veliki razmaci između uzastopnih prostih brojeva mogu biti? **Može li postojati razmak od najmanje** 10000 **između uzastopnih prostih brojeva?** Drugim riječima, možemo li pronaći 10000 uzastopnih cijelih brojeva ili se mora prost broj pojaviti negdje na tom popisu ?
Iznenađujuće, odgovor je da MOŽEMO pronaći 10000 uzastopnih, složenih brojeva. Štoviše, to ćemo i dokazati.

To su $(10001)! + 2, (10001)! + 3, (10001)! + 4, \ldots, (10001)! + 10001$ ($10001!$ je produkt svih cijelih brojeva od 1 do 10001). Ključ dokazivanja da su svi ovi brojevi složeni je da je broj $10001!$ djeljiv sa svim brojevima $2, 3, 4, \ldots$ do 10001. Stoga, prvi broj, $(10001)! + 2$ je zbroj dvaju brojeva od kojih je svaki djeljiv s 2 pa je i zbroj djeljiv s 2. Idući broj u nizu, $(10001)! + 3$ je zbroj dvaju brojeva od kojih je svaki djeljiv s 3 pa je i on djeljiv s 3. Slično tome, idući broj u nizu je zbroj dvaju brojeva od kojih je svaki djeljiv sa 4 pa je i on djeljiv sa 4. Ako nastavimo na ovaj način, vidjet ćemo da je svaki od 10000 brojeva u ovom nizu složeni broj.

Teorem 15. *Ako je n pozitivan cijeli broj, možemo pronaći niz uzastopnih složenih*

brojeva n.

Dokaz. Razmotrite n brojeva, $(n+1)!+2, (n+1)!+3, \ldots (n+1)!+(n+1)$. Kada shvatimo da je $(n+1)!$ djeljiv sa svim cijelim brojevima od 2 do $n+1$, uključujući $n+1$, i ako primijenimo isti argument kao što je to gore navedeno, shvatit ćemo da je svaki od tih brojeva složen broj, tj. prvi je složeni jer je zbroj dvaju brojeva koji su djeljivi s 2. Idući je složeni jer je zbroj dvaju brojeva djeljivih s 3, itd.

Stoga, možemo pronaći milijun, bilijun ili čak trilijun uzastopnih brojeva u nizu bez prostih brojeva. Ovo upućuje na činjenicu da prosti brojevi postaju rjeđi i rjeđi i na mogućnost da postoji konačan broj prostih brojeva. Čak i da je njihov broj beskonačan, kako bismo to uopće uspjeli dokazati?
Prosti su brojevi beskonačni, koliko znamo, a Euklid je to dokazao na sljedeći način. Ovaj dokaz se dan danas smatra jednim od najučinkovitijih, najingenioznijih i najelegantnijih dokaza u matematici. Promotrimo.

Teorem 16. *Prostih brojeva ima beskonačno mnogo.*

Dokaz. Koristeći dokaz kontradikcijom, pretpostavimo da broj prostih brojeva nije beskonačan. Onda bi imali konačan broj prostih brojeva koje možemo nazvati $p_1, p_2, p_3 \ldots p_L$, gdje p_L predstavlja posljednji prosti broj.
Sada ćemo oblikovati sljedeći broj:

$$n = p_1 \cdot p_2 \cdots p_L + 1$$

Sukladno Teoremu 3, ovaj broj n je ili prosti broj ili se može rastaviti na proste faktore, te bi u posljednjem slučaju imao prost faktor p.No, n ne može biti prost broj jer je veći od p_L, a p_L je najveći prost broj. Stoga, n moramo moći rastaviti na proste brojeve među kojima je i prost faktor p. Ali p mora biti jedan od prostih brojeva koji se pojavljuje u produktu $p_1 \cdot p_2 \cdots p_L$ s obzirom da je ovo navodno lista *svih* prostih brojeva. Stoga je umnožak $p_1 \cdot p_2 \cdots p_L$ je djeljiv s p.
Sada, s obzirom da je n djeljiv s p i s obzirom da je $p_1 \cdot p_2 \cdots p_L$ također djeljiv s p, njihova razlika, $n \breve{} p_1 \cdot p_2 \cdots p_L$ je djeljiva s p. Budući da je njihova razlika 1 slijedi da je 1 djeljiv s p.
Naša je pretpostavka da postoji konačan broj prostih brojeva nas je dovela do kontra-

dikcije da p mora djeliti 1. Stoga je naša prvotna pretpostavka da postoji konačan broj prostih brojeva netočna te postoji beskonačno mnogo prostih brojeva.

□

Sada se vraćamo dokazu Teorema 5 kojeg smo ranije naveli. Prvo moramo dokazati nešto povezano s tim teoremom, a to je „strukturalni teorem“. Naš cilj je pokazati da je, prilikom rastavljanja broja na proste faktore, ta faktorizacija jedinstvena do na poredak prostih brojeva.

Lema 1. *Neka je broj n najmanji broj koji se može rastaviti na faktore na dva različita načina. Tada se brojevi koji se pojavljuju u jednoj faktorizaciji broja n neće pojaviti u drugoj faktorizaciji broja n.*

Dokaz. Dokazat ćemo to uz pomoć kontradikcije. Sjetite se da broj n predstavlja najmanji broj koji se može rastaviti na faktore na dva različita načina. Pretpostavimo da su dva načina na koji to možemo napraviti $n = p_1 \cdot p_2 \cdots p_n$ i $n = q_1 \cdot q_2 \cdots q_k$ i pretpostavimo da ove dvije faktorizacije broja n imaju zajednički prost faktor p_1. Onda možemo presložiti proste brojeve faktorizacije broja n na način da p_1 dolazi na prvo mjesto, tj. možemo pretpostaviti da vrijedi $p_1 = q_1$. Stoga, vrijedi sljedeće, $n = p_1 \cdot p_2 \cdots p_n$ i $n = p_1 \cdot q_2 \cdots q_k$. Podijelimo li svaku od ovih jednakosti p_1. Dobijemo sljedeće, $\frac{n}{p_1} = p_2 \cdots p_n$ i $\frac{n}{p_1} = q_2 \cdots q_n$. Ovdje dvije jednakosti sugeriraju da se broj $\frac{n}{p_1}$ može rastaviti na faktore na dva različita načina, $p_2 \cdots p_n$ i $q_2 \cdots q_k$. Ali, ovaj razlomak je broj manji od n te se to suprotstavlja činjenici da je n najmanji broj koji se može rastaviti na faktore na različite načine.
Ova kontradikcija, koja proizlazi iz pretpostavke da postoje dva različita načina za faktorizaciju broja n sa zajedničkim prostim faktorom, pokazuje da, ako postoji najmanji broj koji se može rastaviti na proste faktore na dva različita načina, oni ne mogu imati zajednički faktor.

Teorem 17. *Rastav na proste faktore svakog prirodnog broja većeg od jedan je jedinstven.*[1]

Dokaz. Opet, koristeći kontradikciju, pretpostavimo da to nije istina. Onda postoji neki prirodni broj koji se može rastaviti na faktore na više načina. Stoga, mora postojati

[1] Jedinstvenost se ovdje promatra do na poredak prostih faktora

najmanji prirodni broj koji se može rastaviti na faktore na više načina. Nazovimo ga n. Prema prethodnoj lemi, n ima dvije različite faktorizacije: $n = p_1 \cdot p_1 \cdots p_n$ i $n = q_1 \cdot q_2 \cdots q_k$ i svi brojevi p ili q su različiti. Stoga vrijedi $p_1 \neq q_1$. Pretpostavimo da je $p_1 < q_1$ (Ako je obrnuto istina, imali bismo sličan argument). Naš plan je konstruirati broj p koji je manji od broja n s dvije različite faktorizacije i to ćemo suprotstaviti činjenici da je n najmanji takav broj. Ovo je naš kandidat za broj p:

$$p = (q_1 - p_1) \cdot q_2 \cdots q_k$$

Prvo vidimo da je $(q_1 - p_1) < q_1$. Sada obje strane nejednakosti pomnožimo s $q_2 \cdots q_k$ kako bismo dobili

$$(q_1 - p_1) \cdot q_2 \cdots q_k < q1 \cdot q_2 \cdots q_k$$

Lijeva strana izraza je p, a desna strana je n. Stoga vrijedi,

$$p < n$$

Dokazali smo da vrijedi $p < n$. Sada ćemo pokazati da p ima dvije različite faktorizacije. Prva faktorizacija broja p preuzeta iz jednakosti $(q_1 - p_1) \cdot q_2 \cdots q_k$. Brojevi q su svi prosti brojevi i nijedan od njih nije p_1, ali $q_1 - p_1$ ne mora biti prosti broj i može imati p_1 kao faktor. Provjerit ćemo što se dogodi ako $q_1 - p_1$ ima faktor p_1. Tada vrijedi,

$$q_1 - p_1 = k \cdot p_1$$

za neki broj k, a kada to riješimo po broju q_1 dobijemo

$$q_1 = k \cdot p_1 + p_1 = p_1 \cdot (k + 1)$$

To nam govori da je broj q_1 višekratnik prostog broja p_1. To nije moguće jer je q_1 prosti broj i nema pozitivnih faktora osim broja 1 i samog sebe. Stoga, faktorizacija broja p koja je predstavljena u ranijoj jednaksoti ne sadrži p_1. Sada ćemo pokušati pronaći još jednu faktorizaciju broja p koja sadrži faktor p_1. Skupa s prethodnom tvrdnjom, to će nam osigurati dvije faktorizacije broja p, kao i kontradikciju koju tražimo. Započinjemo s jednakosti

$$p = (q_1 - p_1) \cdot q_2 \cdots q_k$$

$$= q_1 \cdot q_2 \cdots q_k - p_1 \cdot q_2 \cdots q_k$$

$$= n - p_1 \cdot q_2 \cdots q_k$$

(s obzirom da je $q_1 \cdot q_2 \cdots q_k$ jedan od načina faktorizacije broja n)

$$= p_1 \cdot p_2 \cdots p_n - q_1 \cdot q_2 \cdots q_k$$

(s obzirom da je $p_1 \cdot p_2 \cdots p_n$ jedan od načina faktorizacije broja n)

$$= p_1 \cdot (p_2 \cdots p_n - q_2 \cdots q_k)$$

(Dijelimo s p_1).
Posljednja faktorizacija nam pruža drugu faktorizaciju broja p koja sadrži faktor p_1.

Stoga, ova pretpostavka je netočna, što nam govori da svi prirodni brojevi veći od 1 imaju jedinstvenu faktorizaciju na proste brojeve.
Još jedan koristan rezultat koji ćemo trebati je:

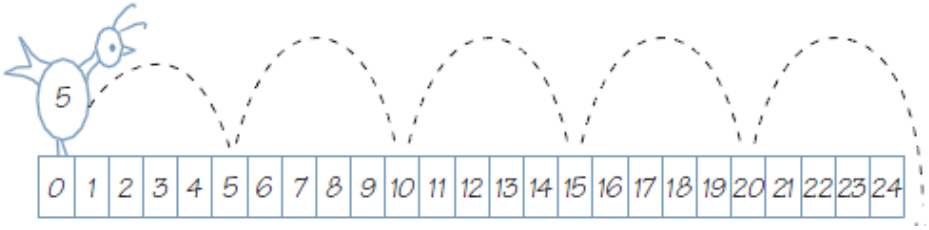
Teorem 18. *Ako su a i b relativno prosti brojevi te ako a djeli kb za neki cijeli broj k, onda a mora dijeliti i k.*

Dokaz. Ako a dijeli kb, onda svi prosti faktori broja a djele kb. Ali budući da a i b nemaju zajedničkih prostih faktora, jer su relativno prosti, svi prosti faktori broja a moraju djeliti broj k. Također, ako svi prosti faktori broja a djele broj k, onda k sadrži sve proste faktore broja a te je višekratnik broja a, tj. a dijeli k.

□

Prosti i složeni brojevi su tema koja se kod nas uvodi u 5. razerdu osnovne škole. Jedan model za određivanje koji brojevi su prosti je aktivnost *Skakanje na brojevnoj crti*. Cilj ovoga zadatka je pronaći proste brojeve, a primjeren je za učenike od petog razreda osnovne škole.

Zadatak 9. *Skakanje na brojevnoj crti*

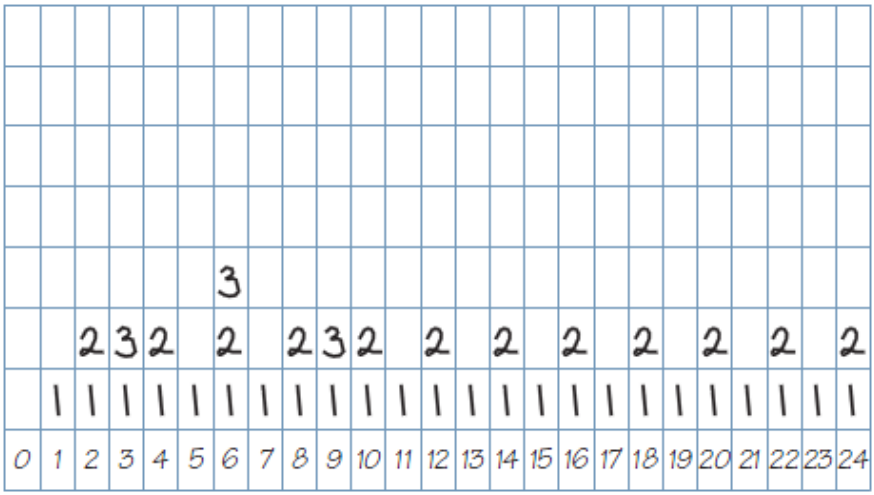


Slika 3: Skakač-5

Skakači su čudni likovi koji mogu skakati samo za određene udaljenosti. Na primjer, Skakač-5 skače za pet mjesta svaki puta. Svi skakači počinju od 0.

Gdje će doskočiti svaki Skakač?

*Na Slici 4 su riješeni Skakač-*1 *i Skakač-*2*. Vi budite Skakač-*3*, te svaki puta kada doskočite na neki broj, napišite broj* 3 *iznad njega. Nastavite rješavati zadatak na slici ispod.*



Slika 4: Skakači

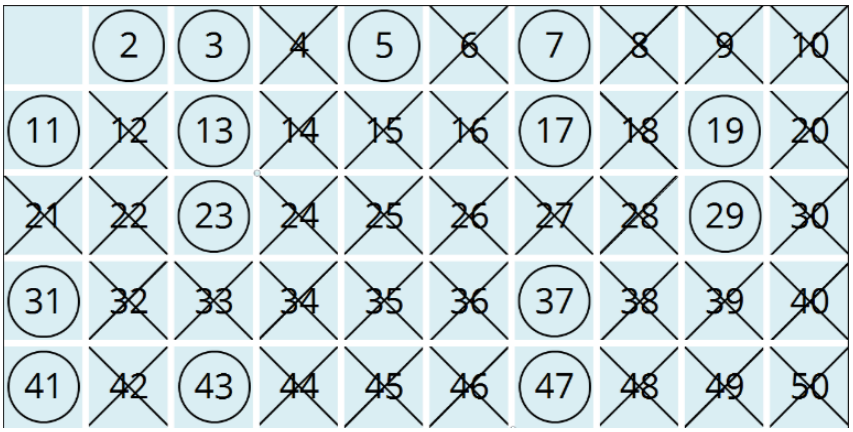
*Napravite isto i za Skakača-*4*, Skakača-*5*, . . . , sve do Skakača-*24*.*

Odgovori na sljedeća pitanja:

1. *Koji brojevi imaju samo* 2 *doskoka skakača?*
2. *Kako nazivamo takve brojeve?*
3. *Koji brojevi imaju više od* 2 *doskoka skakača?*
4. *Kako nazivamo takve brojeve?*
5. *Što je sa brojem* 1*?*

Drugi način da pronađemo proste brojeve je koristiti **Eratostenovo sito** na sljedeći način.

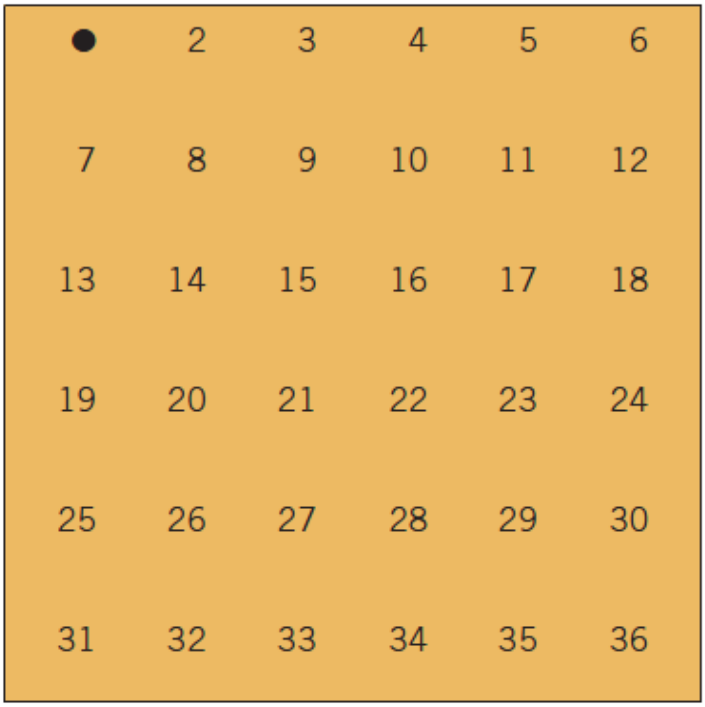
Brojevi su raspoređeni u redovima po 10. Zaokružujemo 2, prvi prost broj, i precrtavamo sve višekratnike broja 2. Nastavljamo sa sljedećim prostim brojem (prvi broj koji nije precratn) i zakružimo ga, a zatim precrtamo sve njegove višekratnike. Ako nastavite ovaj proces, samo prosti brojevi neće pasti kroz sito, tj. ostat će zaokruženi.



Slika 5: Eratostenovo sito

Da bi učenicima što više približili faktoriziranje prostih i složenih brojeva, možemo koristiti i sljedeću igru.

Zadatak 10. *Izaberite partnera i nacrtajte tablicu kao na Slici 6.*



Slika 6: Tablica

Pravila su sljedeća:

- *Napravite tablicu za praćenje bodovanja.*
- *Igrač 1 bira jedan broj iz tablice. Taj igrač dobiva toliki broj bodova. Protivnik dobija bodove jednake zbroju njegovih dijelitelja.*

- *Označite brojeve i dijelitelje koje ste iskoristili. Oni se ne mogu više koristiti.*
- *Ponovite tako da Igrač 2 prvi bira broj.*
- *Izmjenjujte se dok se ne prođete sve brojeve. Igrač koji ima najviše bodova pobjeđuje!*

4 Algoritam dijeljenja

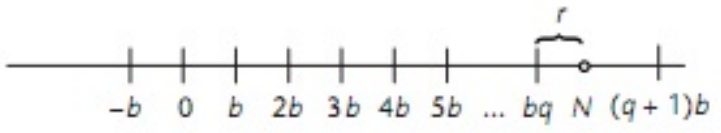
Zadatak 11. *Čarobnjak ima papir na kojem je zapisan jedan cijeli broj. On vam kaže da je taj cijeli broj podijeljen s brojem 23 te ćete, ako pogodite njegov ostatak, osvojiti put u Las Vegas! Dopušta vam 10 pokušaja da otkrijete ostatak. Imate li šanse osvojiti put? Objasnite.*

Velike su šanse da ćete, kada prvi puta pročitate zadatak, misliti da dio informacija nedostaje. Nadamo se da, nakon proučavanja dijeljenja cijelih brojeva, imate određeno znanje o odnosima između djelitelja i ostataka u slučaju dijeljenja. Istražit ćemo ovo pitanje u raspravi o algoritmu dijeljenja.

Pretpostavimo da podijelimo broj $n = 28$ s 4. Rješenje će biti 7, a ostatak 0. Kada dijelimo broj 29 sa 4, rezultat je opet 7, ali je ostatak 1. Kada 30 podijelimo s 4, rezultat je opet 7, a ostatak je 2. Kada 31 podijelimo s 4, rješenje je opet 7, ali je ostatak 3. Zatim se sve ponavlja. Kada podijelimo broj 32 sa 4, dobijemo 8 i ostatak 0, itd. Svaki puta kada povećamo broj n za 1, rezultat se povećava, a ostatak se ponavlja u ciklusu od $0, 1, 2, 3, 0, 1, 2, 3$. Kada dijelimo cijeli broj sa 4, moguća su samo 4 ostatka, a to su $0, 1, 2$ i 3. Na sličan način, kada podijelimo broj s 5, moguće je imati samo 5 različitih ostataka, $0, 1, 2, 3$ i 4. Općenito govoreći, ako podijelimo neki broj s pozitivnim cijelim brojem b, može postojati samo b broj ostataka, a to su $0, 1, 2, \ldots, b-1$. To smo naučili u osnovnoj školi:

Kada pozitivan broj n podijelimo s pozitivnim brojem b, dobijemo količnik q i ostatak r. Nadalje, ako pomnožimo količnik s djeliteljem i zbrojimo taj rezultat s ostatkom, dobijemo broj n, tj. $n = bq + r$. Ovo je vrlo jednostavno shvatiti na pravoj brojevnoj crti. Tamo imamo $b, 2b, 3b$, itd. Možemo shvatiti razmak između 0 i b kao segment duljine b, a razmak između b i $2b$ segment duljine b, itd. (svaki segment uključuje lijevu krajnju točnu, ali ne i desnu). Stoga, svaki broj n je ili krajnja točka jednog od ovih segmenata ili leži unutar njih. Drugačije rečeno, svaki broj n je ili višekratnik broja

b ili se nalazi između dva višekratnika broja b. Ako je lijevi dio tog segmenta najveći višekratnik broja b koji je manji ili jednak broju n, to znači da je razlika između n i bq neki ne-negativni cijeli broj, r, koji je manji od b. Pogledajte Sliku 6 ispod.



Slika 7

Iz te slike, vidljivo je da vrijedi $n = bq + r$. Naravno, sam dijagram nije dokaz ove činjenice, ali je vjerojatno uvjerljiv većini učenika srednjih škola. Sam dokaz se ne razlikuje previše od ovog intuitivnog objašnjenja. Zapravo, slika koju smo predstavili i naša opažanja ukazuju na dokaz u kojem razmatramo razlike između n i višekratnika broja b. Evo pravog teorema i dokaza:

Teorem 19. *Ako podijelimo cijeli broj n pozitivnim cijelim brojem b, onda mora postojati neki cijeli broj q_0 i neki ostatak r, $0 \leq r < b$ tako da je $n = bq_0 + r$. Štoviše, q_0 i r su jedinstveni.*

Dokaz. Dajemo dokaz slučaja kada su n i b pozitivni brojevi, budući da to malo pojednostavljuje stvari. Teorem vrijedi i u slučaju kada je n negativan broj, a b pozitivan.

Stoga, pretpostavimo da su n i b pozitivni. Razmotrite skup brojeva, S, koji formiraju $n-bq$, gdje je $q = 0, 1, 2, \ldots$ Ovaj skup očigledno ima nenegativne cijele brojeve budući da je, na primjer, broj n dio njega. Svaki skup nenegativnih cijelih brojeva ima najmanji element. Neka je najmanji element ovog skupa pojavljuje za $q = q_0$ i nazovimo ga r. Slijedi, $n - bq_0 = r$

Budući da je r najmanji nenegativni cijeli broj u ovom skupu kojeg smo odabrali, vrijedi $r \geq 0$. Pokazat ćemo da r mora biti manji od b. To ćemo postići tako što ćemo pokazati da, ako vrijedi $r \geq 0$, onda možemo pronaći nenegativni član skupa S koji je manji od člana prikazanog ranijom jendkosti, što nam pruža potrebnu kontradikciju. Pretpostavimo da je $r \geq b$ i $r - b \geq 0$. Razmotrimo $n - (q_0 + 1)b$, koji je manji od $n - bq_0$. Evo dokaza da je $n - (q_0 + 1)b$ nenegativan,

$$n - (q_0 + 1)b$$

$$= (n - q_0 b) - b$$

$$= r - b \geq 0$$

(budući da pretpostavljamo da vrijedi $r \geq b$)

Budući da je $n - (q_0 + 1)b$ nenegativan, a budući da je član skupa S i budući da je ovaj broj manji od najmanjeg elementa, $(n - q_0 b)$ skupa S, kao što smo i pokazali, imamo kontradikciju koju smo tražili. S obzirom da je ona proizašla iz pretpostavke da vrijedi $r \geq b$, slijedi da je $r < b$. Da bi dokazali jedinstvenost q i r, pretpostavimo da vrijedi

$$nN = bq_0 + r_1$$

$$n = bq_0 + r_2$$

Naš cilj je pokazati da vrijedi $q_0 + q_1$ i $r_1 = r_2$. Ako oduzmemo raniju jednakost, dobijemo $0 = b(q_1 - q_0) + r_2 - r_1$, što sugerira sljedeće

$$-b(q_1 - q_0) = r_2 - r - 1$$

Uzimajući apsolutne vrijednosti obje strane izraza, dobijemo

$$b|q_1 - q_0| = |r_2 - r_1|$$

Lijeva strana izraza je višekratnik broja b i razlikuje se od 0, ako je $q_0 \neq q_1$ i mora biti veći ili jednak b. Budući da se r_1 i r_2 nalaze između 0 i b, slijedi da je $|r_2 - r_1|$ manje od b jer je ova apsolutna vrijednost udaljenost između točaka (Pogledati Sliku 7 ispod).

Slika 8

Slijedi da je lijeva strana jednakosti veća ili jednaka b, ako je $q_0 \neq q_1$ na desnoj strani jednakosti manji od b. Ovo je nemoguće, pa vrijedi da je $q_0 = q_1$. Kada to uvrstimo u jednakost, dobijemo da je $|r_2 - r_1| = 0$ ili da je $r_1 = r_2$.

Primjećujete da ovaj postupak uključuje puno posla za postupak koji se, geometrijski gledano, čini očigledan.

U osnovnoj školi, prije nego li učenici uče o racionalnim brojevima, sva rješenja zadataka dijeljenja iznose u obliku količnika i ostatka. Stoga, kada broj 16 dijelimo s 3, količnik je 5, a ostatak 1. Kada napreduju do proučavanja racionalnih brojeva, rasprava o ostacima nestaje te rješenja zadataka dijeljenja poprimaju drugačiji oblik, npr.

$16 : 3 = 5\frac{1}{3}$. U smislu algoritma dijeljenja, to znači da, umjesto oblika $n = bq + r$, koriste oblik $\frac{n}{b} = q + \frac{r}{b}$

Važno je da ste, kao učitelj, svjesni odmaka od cijelih brojeva i prelaska na racionalne. Teorem 11 je temeljni rezultat dijeljenja cijelih brojeva i ima veliku primjenu unutar matematike i izvan nje. Primjer tome je slučaj kada računala obrađuju podatke, svaki djelić informacije se preoblikuje u nizove znamenki koje se sastoje od nula i jedinica. Brojevi se pohranjuju uz pomoć binarnog prikaza, o čemu ćemo više razgovarati kasnije. Međutim, da bi uopće došli do binarnog prikaza brojeva, moramo koristiti algoritam dijeljenja. Stoga, numeričko računanje na računalima koristi algoritam dijeljenja na impliciran način.

Ilustrirat ćemo ovaj teorem.

Zadatak 12. *Pretpostavimo da podijelimo svaki od brojeva $n = 32$ i $m = -32$ brojem $b = 6$. Pronađite q i r za svaki od ovih slučajeva.*

Rješenje.. Ako podijelimo broj $n = 32$ brojem $b = 6$, dobijmo količnik $q = 5$ i ostatak $r = 2$. Primjećujete da je $n = bq+r$ i da se r nalazi između 0 i 6, kao što teorem i nalaže. Kada podijelimo $m = -32$ sa 6, pomislit ćete da je količnik $q = -5$. Ali, da je q zapravo -5, jedini način da vrijedi $n = bq + r$ je da je $r = -2$, što se suprotstavlja činjenici da je ostatak broj između 0 i 6. Umjesto toga, uzmemo da je količnik -6 pa bi r bio 4 te vrijedi $m = -32 = 6(-6) + 4 = bq + r$, gdje je r broj između 0 i 6. Ovo je u skladu s dokazom kojeg smo ponudili. Uvijek pronalazimo najveći višekratnik broja b koji je manji ili jednak broju n kada koristimo formulu $n = bq + r$, a u slučaju kada je $n = -32$, najveći višekratnik broja 6 manji ili jednak broju -32 je $6(-6)$. To će biti začuđujuće učenicima i, na prvi pogled, čini se zaista neobično.

Zadatak 13. *Pretpostavimo da je $n = 4q + 1$. Možemo li reći da je, kada podijelimo n sa 4, ostatak 1?*

Rješenje. Možemo. Prema teoremu, postoji samo jedan b i jedan r koji je manji od 4 da vrijedi $n = bq+r$. Budući da $n = 4k+1$ sugerira da je $b = 4$ i $r = 1$, u pitanju mora biti naš jedinstveni par brojeva. Stoga, kada podijelimo n sa 4, ostatak mora biti 1.

5 Najveći zajednički djelitelj (NZD) i Euklidov algoritam

Zadatak 14. *Pronađite najveći zajednički djelitelj brojeva* 20 *i* 35. *Pronađite najveći zajednički djelitelj brojeva* 16807 *i* 14406.

Postoje različite metode pronalaska najvećeg zajedničkog djelitelja.

Teže je odgonetnuti najveći zajednički djelitelj većih brojeva iz prethodnog zadatka. Svrha ovog dijela rada je predstaviti algoritam koji će pomoći lako odgonetnuti najveći zajednički djelitelj te će otkriti druge koriste informacije o brojevima i njihovim najvećim zajedničkim djeliteljima.

Jedna od osnovnih tema koja se naglašava u kurikulu matematike u višim razredima osnovne škole i u srednjoj školi je najveći zajednički djelitelj ili najveći zajednički faktor dva broja a i b. Označit ćemo ga kao $nzd(a, b)$. To je najveći broj s kojim možemo podijeliti i a i b. Na primjer, $nzd(6, 8)$ je broj 2, a $nzd(10, 15)$ je broj 5.
Najveći zajednički djelitelj nije samo koristan u matematici. Koristi se i za razvijanje sigurnosnih kodova koje čak ni agencije nacionalne sigurnosti ne mogu probiti, zbog čega se i koristi. Koristi se i za razvijanje određenih glazbenih ritmova, neutronskih akceleratora, računalnom dizajnu, itd. U knjizi pod nazivom Teorija brojeva u znanosti i komunikaciji, M. R. Shroedera (1988), nalazimo sljedeću tvrdnju: *„Zanimljiva i najviše iznenađujuća primjena najvećeg zajedničkog djelitelja događa se u ljudskoj percepciji visokih tonova: mozak, kada dolazi u kontakt s frekvencijama koje su harmonijski povezane, percipira NZD (najveći zajednički djelitelj) ovih frekvencija kao visoki ton.“* (stranica 5).
Kada je najveći zajednički djelitelj dva broja a i b broj 1, onda a i b nemaju zajedničke proste faktore i oni su relativno prosti. Drugačiji način zapisa je $nzd(a, b) = 1$. Stoga, 8 i 15 su relativno prosti budući da je $nzd(8, 15) = 1$, kao i u slučaju brojeva 14 i 17, gdje također vrijedi $nzd(14, 17) = 1$.
Naravno, vrijedi i $nzd(a, b) = nzd(b, a)$. Također primjećujemo da, ako je a pozitivan,

$$nzd(a, a) = a$$

$$nzd(a, 1) = 1$$

$$nzd(a, 0) = a$$

Pojašnjenje ovih izraza prilično je jednostavno, ali svakako ih je potrebno iznjeti učenicima.

Otkrivanje najvećeg zajedničkog djelitelja dva broja, kada ih rastavimo na proste faktore, je jednostavan postupak. Za svaki zajednički prosti broj u postupku faktorizacije, uzimamo najnižu potenciju prostog broja i jednostavno množimo rezultate. Stoga, ako bi htjeli otkriti najveći zajednički djelitelj brojeva $n = 2^6 \cdot 3^9 \cdot 7$ i $m = 2^8 \cdot 3^4 \cdot 11$, primjećujemo da su zajednički prosti brojevi u faktorizaciji brojevi 2 i 3, a da je najmanja potencija broja 2 broj 2^6, dok je najmanja potencija broja 3 broj 3^4. Stoga, $nzd(m, n) = 2^6 \cdot 3^4$. Dakle, ako trebamo izraz $3a^3b^2 + 6ab^3$ rastaviti na faktore, izdvajamo $3ab^2$ i dobijemo $3ab^2(a^2 + 2b)$. Na sličan način, ako želimo izraz $x^4 - 9x^2$ rastaviti na faktore, izdvajamo prvo nzd, a on je x^2 i dobijemo $x^2(x^2 - 9) = (x - 3)(x + 3)$.

Otkrivanje nzd-a brojeva uz pomoć rastavljanja na proste faktore je jednostavno kada su brojevi mali ili već u rastavljenom obliku. Na primjer, ako želimo otkriti $nzd(24, 18)$, vrlo brzo ćemo doći do rješenja 6. Zamislite da pokušavate doći do nzd-a brojeva 4562 i 2460 ili brojeva koji su puno veći od ovih. Postupak rastavljanja na faktore bi bio zamarajući i dugotrajan. U praksi, to se ne radi na ovaj način jer su praktične primjene brojeva obično velike, zbog čega je neučinkovito i teško doći do faktora čak i uz pomoć računala. Umjesto toga, koristi se bolja metoda pod nazivom Euklidov algoritam kako bismo došli do nzd-a dva broja. Ona nam pokazuje kako da preoblikujemo nzd dva broja u nzd dva broja koja su, u najboljem slučaju, manja.

Teorem 20. ***(Verzija 1 Euklidovog algoritma)***
Ako su a i b cijeli brojevi, onda je $nzd(a, b) = nzd(b, a - b)$.

Dokaz. Pokazat ćemo da se skup djelitelja a i b podudara sa skupom djelitelja b i $a - b$. Stoga, najveći broj s kojim možemo podijeliti i a i b je ujedno i najveći broj s kojim možemo podijeliti b i $a - b$, tj. $nzd(a, b) = nzd(b, a - b)$. Na primjer, $nzd(15, 6) = nzd(6, 9) = 3$.

Neka je h bilo koji djelitelj a i b. Budući da je h djelitelj brojeva a i b, s njime možemo podijeliti i $a - b$, prema Teoremu 2. **Stoga, bilo koji djelitelj brojeva a i b je isto tako djelitelj $a - b$.**

Sada ćemo okrenuti postupak. Neka je h bilo koji djelitelj brojeva b i $a - b$. Prema

Teoremu 2, s h možemo podijeliti i zbroj $(a-b)+b$ ili samo a, tj. s bilo kojim djeliteljem brojeva b i $a-b$ možemo podijeliti i a i b. Stoga je h djelitelj i a i b.
Podebljanim tvrdnjama pokazali smo da je svaki djelitelj h brojeva a ili b ujedno i djelitelj broja b i $a-b$ i obrnuto. Slijedi da su djelitelji brojeva $a, b, a+b$ i $a-b$ jednaki, tj. najveći zajednički djelitelj a i b je ujedno i najveći zajednički djelitelj b i $a-b$.

Ovaj algoritam je vrlo jednostavno za programirati na računalu te je vrlo brz i učinkovit. Navodimo algebarski primjer kako se ovaj teorem treba koristiti.

Zadatak 15. *Pokažite da, za bilo koji cijeli broj n, vrijedi da je $nzd(n+1, n) = 1$.*

Rješenje.

$$nzd(n+1, n) = nzd(n, n+1-n) = nzd(n, 1) = 1$$

Uočite da je metoda faktorizacije u ovom slučaju beskorisna. Na sličan način možemo pokazati da vrijedi $nzd(2n+1, n) = 1$ za bilo koji cijeli broj n.

Dolje navodim još jednu verziju Euklidovog algoritma s kojom ćete se možda češće susresti.

Teorem 21. *(**Verzija 2 Euklidovog algoritma**). Pretpostavimo da je $a > b$ i da, kada a podijelimo s b, dobijemo ostatak r. Onda vrijedi da je $nzd(a, b) = nzd(b, r)$.*

Dokaz. Ovaj dokaz je gotovo identičan dokazu Teorema 12.
Znamo da je $a = bq + r$ za neki broj q. Ako pogledamo desnu stranu jednakosti, vidimo da bilo koji djelitelj brojeva b i r mora dijeliti i lijevu stranu, a (Teorem 12). Stoga, **djelitelji brojeva b i r su i djelitelji broja a (i b)**. Iz odnosa $a - bq = r$ uočavamo da, ako pogledamo lijevu stranu jednakosti, bilo koji djelitelj brojeva a i b dijeli i desnu stranu, broj r i, naravno, broj b (opet po Teoremu 2). Stoga, **djelitelji brojeva a i b su djelitelji brojeva r i b.**
Dvije podebljane izjave nam pokazuju da su djelitelji brojeva a i b isti kao i djelitelji brojeva b i r.
Slijedi, $nzd(a, b) = nzd(b, r)$.

Možete smatrati Teorem 13 boljom i naprednijom verzijom Teorema 12. Novi algoritam je vrlo učinkovit te ga uzastopno primjenjuju računala u potrazi za $nzd(a, b)$.

Zapravo, ono što knjige predstavljaju kao Euklidov algoritam je zapravo uzastopna primjena verzije 2 Euklidova algoritma.
Ovaj postupak ponavljamo dok konačno ne dođemo do $nzd(g, 0)$, a u tom slučaju znamo da je g najveći zajednički djelitelj broja a i b. To možemo izreći i matematički način da označimo ostatke u svakom koraku kao r_1, r_2, itd.:

$$nzd(a, b) = nzd(b, r_1) = nzd(r_1, r_2) = \ldots nzd(g, 0) = g$$

Kako bismo bolje pojasnili uporabu ove verzije Euklidovog algoritma, vratit ćemo se na ranije spomenute primjere.

Zadatak 16. *Pronađite:*

(a) $nzd(24, 18)$,

(b) $nzd(4562, 2460)$.

Rješenje.

(a) 24 i 18 se jednostavno mogu rastaviti na faktore. $24 = 2^3 \cdot 3$ i $18 = 2 \cdot 3^2$, pa dobijemo $nzd(24, 18) = 2 \cdot 3 = 6$. Da smo u ovom postupku primijenili verziju 2 Euklidovog algoritma, koraci bi bili,

$$nzd(24, 18) = nzd(18, 6) \text{ i } nzd(18, 6) = nzd(6, 0)$$

budući da smo dobili ostatak 0 kada smo podijelili 18 sa 6. Postupak je sada završen i znamo da je $nzd(6, 0) = 6$.
Za početak, dijelimo veći broj, 24 manjim brojem 18. Gledamo samo ostatak, a to je 6. To nam postaje novi djelitelj pa dijelimo prethodnog djelitelja, 18, s ostatkom 6. Metoda uvijek nalaže da dijelimo prethodnog djelitelja ostatkom dok ne dođemo do ostatka 0, a u tom slučaju nam je onda posljednji djelitelj nzd.

(b) Ovo je teže dokazati uz pomoć metode rastavljanja na faktore. Riješit ćemo ovaj zadatak uz pomoć verzije 2 Euklidovog algoritma:

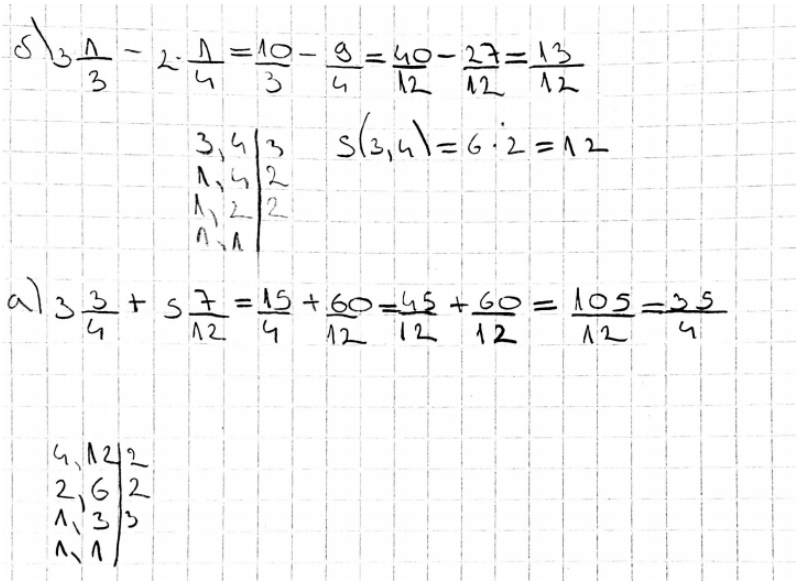
$nzd(4562, 2460) = nzd(2460, 2102) = nzd(2102, 358) = nzd(358, 312) = nzd(312, 46) =$

$= nzd(46, 36) = nzd(36, 10) = nzd(10, 6) = nzd(6, 4) = nzd(4, 2) = nzd(2, 0) = 2.$

Postoji još korisnih rezultata koji proizlaze iz Teorema 2, koji nisu očigledni, a jedan od njih ćemo koristiti kasnije kada budemo proučavali diofantske jednadžbe. Ovo je vrlo važno u proučavanju teorije brojeva.

5.1 Najmanji zajednički višekratnik

Osim najvećeg zajedničkog djelitelja, u algebri i drugdje jednako je koristan i najmanji zajednički višekratnik (nzv). Učenici se susreću s ovim konceptom u petom razredu osnovne škole, a koriste ga i kasnije u šestom, kada počinju zbrajati razlomke s različitim nazivnicima, kao na slici ispod.



Slika 9: Primjer traženja nzv nazivnika

Pod najmanjim zajedničkim višekratnikom dva pozitivna broja n_1 i n_2 smatramo najmanji pozitivni cijeli broj koji je višekratnik n_1 i n_2. Stoga, najmanji zajednički višekratnik broja 2 i 3 je broj 6 jer je to najmanji pozitivni cijeli broj koji je djeljiv i s 2 i s 3.

Kada n_1 i n_2 rastavimo na proste faktore, postaje vrlo lako pronaći najmanji zajednički višekratnik tih brojeva. Promatramo sve proste brojeve koji se pojavljuju u prostoj faktorizaciji ovih brojeva i uzimamo najveću potenciju svakog od ovih faktora koje vidimo. Zatim ih pomnožimo. Ako je $n_1 = 2^3 \cdot 3 \cdot 7$ i $n_2 = 3^2 \cdot 5 \cdot 11$, najmanji zajednički višekratnik brojeva n_1 i n_2 je $2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.

Najmanji zajednički višekratnik brojeva n_1 i n_2 označavamo s $nzv(n_1, n_2)$. Slično tome, u algebri, ako želimo pronaći najmanji zajednički višekratnik dva algebarska izraza, prvo ih u potpunosti rastavljamo na faktore i, razmatrajući svaki faktor kao prosti broj, uzimamo najveću potenciju tih prostih brojeva koje vidimo. Dakle, da bi pronašli nzv brojeva $3a^3b^2$ i $4ab^3$, dobijemo $12a^3b^3$.

U algebri koristimo najmanji zajednički višekratnik kada pokušavamo pronaći najmanji zajednički nazivnik. Dakle, ako želimo zbrojiti,

$$\frac{4}{3x3^5y^2} + \frac{7}{6xy^3}$$

prvo ćemo tražiti najmanji zajednički nazivnik, a to je $18x^5y^3z$, koji je $nzv(3x^5y^2z, 6xy^3)$. Zatim ćemo preoblikovati svaki razlomak ekvivalentu razlomka s tim nazivnikom tako da ćemo pomnožiti brojnik i nazivnik svakog razlomka kako bi dobili nazivnik nzv. Slično tome, ako želimo zbrojiti,

$$\frac{2x}{3(x-1)^3(x+2)} + \frac{4x-3}{4(x-1)^2(x+2)^4}$$

zajednički bi nazivnik bio $12(x-1)^3(x+2)^4$, koji je nzv $3(x-1)^3(x+2)$ i $4(x-1)^2(x+2)^4$. Kao što smo to već spomenuli, rastavljanje većih brojeva na faktore je teško pa je logično očekivati da otkrivanje nzv dva broja zahtijeva algoritam koji se razlikuje od Euklidovog algoritma. To nije istina. Kada otkrijemo nzd dva broja, lako je pronaći nzv ta dva broja. Koristimo sljedeći rezultat:

Teorem 22. *Ako su n_1 i n_2 dva prirodna broja, onda je $nzv(n_1, n_2) \cdot nzd(n_1, n_2) = n_1 n_2$.*

Da bismo pronašli $nzv(n_1, n_2)$, jednostavno pomnožimo $n_1 n_2$ i podijelimo s $nzd(n_1, n_2)$, kojeg možemo otkriti uz pomoć Euklidovog algoritma.
Ilustrirat ćemo to primjerom.

Zadatak 17. *Potvrdite Teorem 14 za*

(a) $n_1 = 24$ i $n_2 = 45$

(b) za algebarski izraz $n_1 = 3ab^3$ i $n_2 = 4a^2b^2c$.

Rješenje.

(a) $n_1 = 2^3 \cdot 3$ i $n_2 = 3^2 \cdot 5$. Sada su $nzd(n_1, n_2) = 3$, a $nzv(n_1, n_2) = 2^3 \cdot 3^2 \cdot 5$. Iz ovoga slijedi,

$$nzd(n_1, n_2) \cdot nzv(n_1, n_2) = 2^3 \cdot 3^3 \cdot 5 = n_1 \cdot n_2.$$

(b)

$$nzd(n_1, n_2) = a \cdot b^2$$

i

$$nzv(n_1, n_2) = 12 \cdot a^2 \cdot b^3 \cdot c$$

$$\Rightarrow nzd(n_1, n_2) \cdot nzv(n_1, n_2) = (a \cdot b^2)(12 \cdot a^2 \cdot b^3 \cdot c) = 12 \cdot a^3 \cdot b^5 \cdot c = n_1 \cdot n_2$$

.

6 Temeljni sustavi brojeva

Zadatak 18. *Tanja, vrlo bistra učenica, tvrdi da vam može pokazati da može napisati broj* 35 *samo uz pomoć brojeva* 1 *i* 0 *i da je taj broj zapravo jednak broju* 100011*. Objasnite o čemu ona priča?*
(Pomoć: Znate da se broj 35 može napisati i kao $3 \cdot 10 + 5 \cdot 1$ *ili* $3 \cdot 10^1 + 5 * 10^0$ *s bazom* 10*.)*

Ovaj zadatak učenike treba navesti na razmišljanje o tome kako brojeve možemo zapisati na različite načine uz pomoć različitih baza. Ono što možda nije očigledno je da se ova mogućnost nalazi u temelju nekih od najvažnijih napredaka u tehnologiji. U ovom poglavlju je prikazana jedna od najrevolucionarnijih primjena algoritma dijeljenja: prikaz brojeva uz pomoć različitih baza. Razvitak računala ovisio je o mogućnosti prikaza brojeva uz pomoć jedinica i nula. To je uspješno postignuto uz pomoć prikaza brojeva s bazom 2. Također, prikaz brojeva s bazom 8 i 16 od ključne je važnosti za dizajniranje i funkcioniranje bilo kojeg računala. Zapisivanje broja s bazom 2 dio je razloga zbog kojeg se aritmetika može tako brzo odraditi na računalu. Kada su brojevi prikazani s bazom 2, zbrajanje brojeva postaje trivijalno i odrađuje se nevjerojatnom brzinom. Primjene prikaza brojeva s različitom bazom su mnogobrojne pa će broj primjera primjene ovog sustava zadovoljiti i najznatiželjnije. Međutim, u zbrajanju, jednako je važno zaista shvaćati koncepte baze 10 koje koristimo u svakodnevnom životu, ali je također bitno informativno proučiti kako možemo prikazati brojeve uz pomoć drugih baza. Kao što je važno učiti gramatiku stranog jezika kako bi bolje shvatili vlastiti, tako i pomaže proučavanje brojevnih sustava s različitom bazom kako bi bolje shvatili bazu 10, tj. svakodnevni brojevni sustav.
Broj 3245 je skraćeni prikaz broja $3 \cdot 1000 + 2 \cdot 100 + 4 \cdot 10 + 5$. Kada isto zapisujemo uz pomoć eksponenata, dobijemo da je $3245 = 3 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10 + 5 \cdot 10^0$. To nazivamo prikazom broja 3245 uz pomoć baze 10.

Naravno, svaki broj u prikazu tog broja je manji od 10. Broj $3\cdot5^3+2\cdot5^2+4\cdot5+5\cdot5^0$ je zapravo broj 450. Ovakav prikaz se također naziva prikaz broja 450 s bazom 5, budući da je korištena baza broj 5. Ova baza 5 se označava na sljedeći način $(450)_5$.
Općenito govoreći, kada je pozitivan cijeli broj napisan u obliku zbroja potencija pozitivnog broja b, čiji su koeficijenti svake potencije b manji od b, kažemo da smo zapisali taj broj s bazom b. Stoga, broj $a_n(b)^n + a_{n-1}(b)^{n-1} + \dots a_0$, gdje su svi brojevi a manji od b, je prikaz nekog broja n s bazom b. Često ćemo to napisati u skraćenom obliku $(a_n a_{n-1} \dots a_0)_b$. Primijetit ćete da je eksponent broja b na početku, tj. b^n, za jedan manji od broja znamenki u prikazu broja. Kako bi to bolje shvatili, dat ćemo nekoliko primjera.

Zadatak 19. *Koja je vrijednost svakih od sljedećih brojeva?*

(a) $(1222)_3$,

(b) $(345)_6$,

(c) $(43216)_8$.

Rješenje.

(a) Baza za prikaz broja je 3. Sam broj ima 4 znamenke, stoga započinjemo s potencijom 3 za jedan manju od broja znamenki, tj. s 3^3. Naš je broj zapravo broj $1 \cdot 3^3 + 2 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3^0$ ili jednostavno, 53. Možemo ga napisati i kao $53 = (1222)_3$.

(b) Bazu za prikaz broja je 6. Budući da zadani prikaz broja ima 3 znamenke, naš broj izgleda $(345)_6 = 3\cdot6^2+4\cdot6^1+5\cdot6^0$ ili jednostavno, 137. Stoga, $137 = (345)_6$.

(c) U posljednjem primjeru zadana je baza 8 za prikaz broja. Broj ima 5 znamenki, stoga započinjemo s 8^4. Naš broj, $(43216)_8 = 4\cdot8^4+3\cdot8^3+2\cdot8^2+1\cdot8^1+6\cdot8^0 = 18062$.

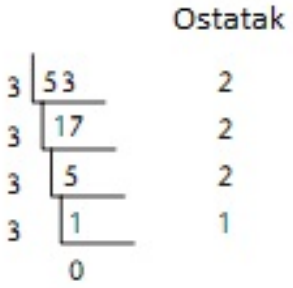
Kako preoblikovati broj iz dekadskog sustava, koji koristimo svakodnevno, na bazu b. Na primjer, želimo broj n preoblikovati na bazu 3. Onda znamo da će to izgledati na sljedeći način nakon preoblikovanja: $a_n(3)^n + a_{n-1}(3)^{n-1} + \dots + a_1(3)^1 + a_0$. Kako ćemo pronaći a_0? Moguće je broj $a_n(3)^n + a_{n-1}(3)^{n-1} + \dots + a_1(3)^1 + a_0$ napisati kao

$$3p + a_0 \text{ gdje je } 0 \leq a_0 < 3$$

Jednostavnije rečeno, kada podijelimo broj n brojem 3, dobijemo količnik p i ostatak a_0. Stoga, da bi pronašli a_0, dijelimo prvotni broj s 3 te je a_0 ostatak.
Pogledajmo sada količnik p. Budući da je $p = a_n(3)^{n-1} + a_{n-1}(3)^{n-2} + \cdots + a_2(3)^1 + a_1$, kada podijelimo s brojem 3 cijeli izraz osim posljednjeg, da je on u obliku $3q + a_1$. Jednostavnije rečeno, kada podijelimo p s 3, dobijemo količnik q i ostatak a_1. Stoga, kako bi pronašli a_1, dijelimo prvotni količnik p brojem 3. Ostatak je a_1. Sada možemo vidjeti kako ova metoda funkcionira. Kako bi pronašli a_2, dijelimo q, naš posljednji količnik, s brojem 3 te je naš ostatak a_1, itd.
Zapravo, algoritam (pravilo) koji nam dopušta da pronađemo prikaz broja n u bazi b je ustvari podijeliti n s b. Uzmite količnik i opet ga podijelite s b. Posljednji količnik opet dijelimo s b. U svakoj fazi, izdvajajte ostatak sa strane. Ostaci koje dobijemo bit će znamenke baze b prikaza broja, ali od posljednje prema prvoj. Zato je potrebno samo obrnuti redoslijed navedenih ostataka. Postupak je vidljiv u sljedećem primjeru.

Zadatak 20. *Pronađite prikaz broja* 53 *u bazi* 3.

Rješenje. Koraci su sljedeći: podijelimo 53 s 3. Dobijemo 17 i ostatak 2. Broj 2 zapišite sa strane. Sada dijelimo 17 s 3. Dobijemo 5 i ostatak 2. Ostatak opet zapisujemo sa strane. Zatim, dijelimo prethodni količnik, 5, s brojem 3. Dobijemo 1 i ostatak 2. Na kraju dijelimo 1 sa 3 i dobijemo 0 i ostatak 1. Kada dođemo do 0, postupak je završen. Na dolje navedenoj Slici 10 možete vidjeti cijeli postupak.



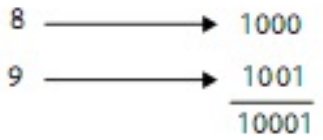
Slika 10

Ostatke je potrebno zapisati od dolje prema gore. Dobijemo broj 1222, koji je prikaz broja 53 s bazom 3, što nam govori da je $53 = 1(3)^3 + 2(3)^2 + 2(3)^1 + 2(3)^0$.

Kao što je već spomenuto, jedna od važnijih primjena prikaza broja s različitim bazama, posebno baza 2, jeste upravo u računalnoj tehnologiji, koja ih koristi u svrhu brzog aritmetičkog funkcioniranja. Takav se prikaz još naziva i binarni prikaz i koristi jedino znamenke manje od 2, tj. 0 i 1. Zašto je baza 2 bitna? Odgovor je jednosta-

van. Memorija računala se sastoji od velikog broja električnih prekidača, a oni mogu imati samo dvije pozicije – uključeno i isključeno. Stoga, ako želimo da ovi uključen-isključen prekidači predstavljaju neki broj, nemamo izbora nego da koristimo bazu 2. U ovom prikazu, broj jedan znači „uključen prekidač“, a broj nula znači „isključen prekidač“. Broj 8, koji je s bazom 2 oblika: $(1000)_2$, mogu predstavljati 4 prekidača, koji se nazivaju bitovima, od kojih je prvi uključen, a preostala tri su isključena. Ovo je pojednostavljeni prikaz onoga što se zapravo događa u računalu, ali ključno za shvaćanje funkcioniranja računala. „Prekidači“ za uključivanje i isključivanje jednostavno au dijelovi memorije magnetizirani u pozitivan ili negativan naboj.

Zbrajanje u bazi 2 vrlo je brzo, a to se događa zbog toga što su uključene jedino znamenke 0 i 1. Jedina pravila za zbrajanje su da vrijedi $0 + 0 = 0$, $0 + 1 = 1$ i $1 + 1 = 0$, ali u zadnjem slučaju, moramo prenijeti jedinicu u sljedeću kolonu. Kako bismo ponudili vrlo jednostavnu primjenu, ako želimo zbrojiti $8 + 9$, moramo ih prvo napisati u binarnom obliku, $8 = (1000)_2$, $9 = (1001)_2$. Postupak zbrajanja je vidljiv na Slici 11 ispod. Počevši od desne prema lijevoj strani, zbrajamo $0 + 1 = 1$, $0 + 0 = 0$, $0 + 0 = 0$, a zatim $1 + 1 = 0$ i prenosimo 1 u iduću kolonu te kada tu jedinicu zbrojimo s onime što nalazimo tamo, a to je ništa (0), dobijemo opet 1.

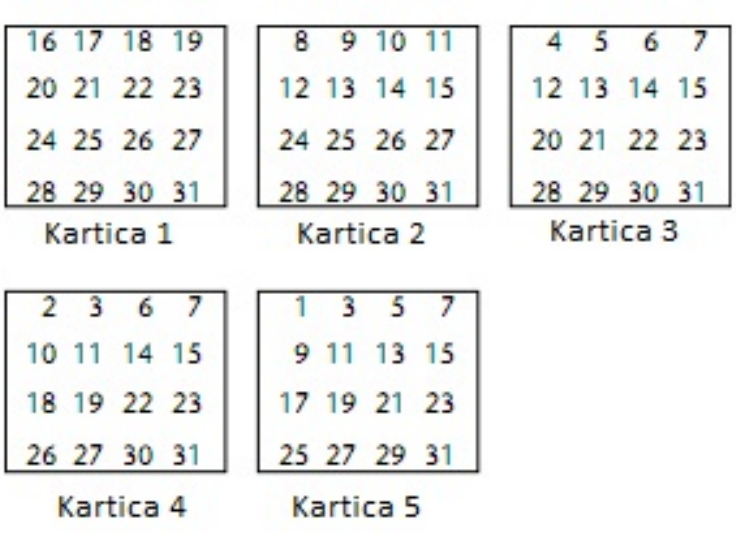


Slika 11

Stoga, naš zbroj je $(10001)_2$, a provjerom se može utvrditi da je to broj 17.

Postoje neke vrlo sofisticirane igre s karticama koje se temelje na prikazu broja s bazom 3, kao i s bazom 2. Evo jedne koja se često igra u višim razredima osnovne škole i u srednjoj školi.

Zadatak 21. *Učenika zamolimo da odabere broj između* 1 *i* 31 *bez da na glas kaže koji je broj odabrao. Zatim mu pokažete pet kartica koje možete vidjeti ispod na Slici 12.*



Slika 12

Zamolite učenika da vam pokaže svaku karticu na kojoj se nalazi taj broj te mu odmah možete reći koji je broj izabrao. Recimo, ako je odabrao kartice 1 *i* 2*, odmah mu kažete da je odabrao broj* 24*. Ako vam kaže kartice* 1*,* 3 *i* 5*, odmah mu kažete da je njegov broj* 21*. Kako funkcionira ovaj trik?*

Rješenje. Svaka kartica ima određenu vrijednost (koju možete napisati na poleđini kartice, ako želite). Prva kartica vrijedi 16, druga 8, treća 4, četvrta 2 i peta 1. Vodimo računa o zbroju kako napredujemo. Svaki puta kada učenik odabere prvu karticu, dodajemo broj 16, kada odabere drugu karticu, dodajemo 8. Kada odabere treću karticu, dodajemo broj 4, kada odabere četvrtu karticu, dodajemo 2 i kada odabere petu karticu, dodajemo broj 1.

Dakle, ako osoba odabere kartice 1 i 2, njegov broj je $16+8$ ili 24. Ako odabere kartice $1, 3$ i 5, njegov broj je $16+4+1$ ili 21.

Ovaj se trik bazira na binarnom prikazu brojeva. Uzmimo u obzir peteroznamenkasti binarni broj čije su znamenke a, b, c, d, e, te počevši s lijeva na desno, vrijednost tog broja je $a \cdot 2^4 + b \cdot 2^3 + c \cdot 2^2 + d \cdot 2^1 + e \cdot 2^0$, tj. kada zapisujete jedan od brojeva između 1 i 31 u binarnom obliku, rastavljate ga na onoliko šesnaestica koliko ih ima, zatim na koliko dodatnih osmica ima, koliko dodatnih četvorki ima, itd. Na kartici 1 imamo sve brojeve od 1 do 31 čija je znamenka a broj 1. Svi ovi brojevi onda imaju jednu 24 ili 16 u sebi, zbog čega zapisujemo broj 16 na poleđinu kartice. Na kartici 2, imamo brojeve od 1 do 31 čija je b znamenka 1. Oni sadrže jednu dodatnu 23 ili 8 u sebi. Zato zapisujemo broj 8 na poleđinu kartice 2. Na kartici 3 imamo brojeve od 1 do 31 koji sadrže dodatnu 4 u sebi, tj. njihova c znamenka binarnog prikaza

je 1. Ako je znamenka d broj 1, sadrže dodatnu dvojku, itd. Stoga, ako osoba samo odabere kartice 1 ili 2, govori vam da je binarni prikaz koji tražite 11000 ili jednostavno $1 \cdot 16 + 1 \cdot 8 + 0 \cdot 4 + 0 \cdot 2 + 0 \cdot 1$, tj. njegov broj je 24. Ako vam osoba kaže da se njegov broj nalazi samo na karticama $1, 3$ i 5, onda vam govori da je binarni prikaz broja kojeg tražite 10101, koji vrijedi $1 \cdot 16 + 1 \cdot 4 + 1$ ili broj 21.

7 Modularna aritmetika

Zadatak 22. *Leglo štenaca se okotilo u subotu,* 29. *ožujka. Rečeno mi je da ne mogu odnijeti jedno štene kući dok ne prođe najmanje* 56 *punih dana. Koji je prvi dan i datum kada ću moći preuzeti jedno štene? Može li ga pokloniti svojoj sestri za rođendan,* 6. *srpnja?*

Ovaj zadatak se može jednostavno riješiti uz pomoć kalendara i brojanja 56 dana. No na taj način, zadatak će biti dosta umarajući. Brži put do rješenja može se naći uz znanje o konceptima modularne aritmetike. Modularna aritmetika biti će tema ove cjeline, a proširiti će znanje o ostacima uz pomoć proučavanja osnove modularne aritmetike, čija je primjena značajna i utječe na nas na svakodnevnoj bazi.
Proučit ćemo i primjene modularne aritmetike na sigurnost podataka (poput podataka s kreditne kartice) prilikom kupovine proizvoda online. Sigurnosni sustavi su temelj dobrobiti svake zemlje, a većinom se temelje na modularnoj aritmetici.
Započet ćemo s tipičnim srednjoškolskim matematičkim problemom rekreacijske prirode.

Zadatak 23. *Zadajte učenicima sljedeću tablicu:*

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	*etc*						

Slika 13

i zamolite ih da odrede u koji stupac spada broj 283.

Rješenje. Nakon što se učenici poigraju sa zadatkom, primijetit će slijed. Svaki red ima skupinu od 8 uzastopnih brojeva. Da biste pronašli kojem stupcu pripada

broj 283, dijelite ga s 8 te će vam ostatak dati odgovor. Ako je vaš ostatak 1, pripada stupcu A, ako je ostatak 2, pripada stupcu B, itd. Kada 283 podijelimo s 8, ostatak je 3. Broj 283 pripada stupcu C.

Zadatak 24. *Uzela sam policu osiguranja* 4. *rujna. To je bio ponedjeljak. Polica će biti aktivirana nakon što prođe punih* 45 *dana. Htjela bih znati koji će to biti dan i datum. Koji je odgovor?*

Rješenje. Trebamo samo shvatiti da je svakih 7 dana ponedjeljak. Stoga, ako podijelimo 45 sa 7, dobijemo ostatak 3. Dakle, polica će biti aktivirana 3 dana iza ponedjeljka, tj. u četvrtak, 19. listopada.

Oba ova primjera koriste modularne ili satne sustave. U svakom takvom sustavu, ostatak je važna stavka. Nazivaju se satnim sustavima jer modeliraju satove. Na primjer, ako je sada 2 sata i želimo znati koliko će sati biti za 50 sati, trebamo samo shvatiti da je isto vrijeme svakih 12 sati (nebitno je li u pitanju vrijeme po danu ili noći). Stoga je jedino potrebno podijeliti 50 s 12 kako bi dobili 4 (grupe od 12) i ostatak 2. Ostatak nam govori koliko je sati nakon našeg početnog vremena. Dakle, za 50 sati bit će 4 sata. Sada kada shvaćamo koncept, prelazimo na apstraktnu matematičku analizu.

Pretpostavimo da su a i b cijeli brojevi i da je m pozitivan broj. Kažemo da je a kongruentan b modulo m, ako a i b imaju isti ostatak kada ih dijelimo s m. Pišemo $a \equiv b \pmod{m}$. Stoga, $12 \equiv 19 \pmod{7}$, budući da oba imaju ostatak 5 kada ih podijelimo sa 7. Postoji drugi način da provjerimo imaju li dva broja isti ostatak kada ih podijelimo s m bez da primijenimo postupak dijeljenja. Rezultat je koristan i prikazan u sljedećem teoremu:

Teorem 23. *$a \equiv b \pmod{m}$ ako i samo ako je $a - b$ djeljiv s m.*

Dokaz. Da bi dokazali ovaj teorem, moramo prvo dokazati dvije stavke.

(1) Ako je $a \equiv b \pmod{m}$, onda je $a - b$ djeljiv s $m(\Rightarrow)$, i

(2) ako je $a - b$ djeljiv s m, onda vrijedi da je $a \equiv b \pmod{m}(\Leftarrow)$.

$\Rightarrow$ Pretpostavljamo da je $a \equiv b \pmod{m}$ i želimo dokazati da je $a - b$ djeljiv s m. Budući da vrijedi $a \equiv b \pmod{m}$, a i b imaju isti ostatak r kada ih podijelimo

s m. Prema algoritmu dijeljenja, to znači $a = pm$+r i $b = qm + r$. Očito, ako oduzmemo ove dvije jednakosti, dobijemo $a - b = (p - q)m$. To znači da je $a - b$ djeljiv s m, što smo i nastojali dokazati.

$\Leftarrow$ Sada pretpostavljamo da je $a - b$ djeljiv s m i želimo pokazati da a i b imaju isti ostatak kada ih podijelimo s m. Pretpostavimo da, kada podijelimo a i b s m, dobijemo ostatke r_1 i r_2. Prema algoritmu dijeljenja, to znači da vrijedi

$$a = pm + r_1$$

i

$$a = qm + r_2$$

gdje su i r_1 i r_2 manji od m i nenegativni. Ako izračunamo $a - b$, dobijemo,

$$a - b = +(p - q)m + r_2 - r_1$$

Budući da nam je zadano da je $a - b$ djeljivo s m, $a - b = km$ i ove posljednje jednakosti se mogu napisati kao $km = (p-q)m+r_2-r_1$, ili $km-(p-q)m = r_2-r_1$. Lijeva strana je višekratnik broja m i može se zapisati kao $m[k-(p-q)] = r_2-r_1$ Desna strana jednakosti predstavlja razliku dva ne-negativna broja manja od m, stoga mora imaju apsolutnu vrijednost manju od m. Zbog toga, desna strana ne može biti višekratnik broja m osim ako je 0, tj. r_1 mora biti jednak r_2, a time smo dokazali da je ostatak jednak kada se oba broja, a i b, podijele s m.

Kako bismo provjerili jesu li 43 i 75 kongruentni $\pmod 6$, moramo ih samo oduzeti da bismo dobili 32, a budući da broj 32 nije djeljiv sa 6, nisu kongruentni $\pmod 6$, tj. imaju različite ostatke kada ih podijelimo sa 6. Dolje su navedeni neki odnosi koji vrijede kada radimo s kongruencijama.

Teorem 24. *Ako je* $a \equiv b \pmod m$ *i* $c \equiv d \pmod m$*, onda vrijedi*

(a) $a + c \equiv b + d \pmod m$

(b) $a - c \equiv b - d \pmod m$

(c) $ap \equiv bp \pmod m$ *za bilo koji cijeli broj* p

(d) $ac \equiv bd \pmod m$

(e) $a^n \equiv b^n \pmod{m}$ *za bilo koji pozitivni cijeli broj* n.

Dokaz.

(a) Prema Teoremu 15, moramo samo dokazati da je razlika $(a+c)-(b+d)$ djeljiva s m. Iz zadanih činjenica da $jea \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, opet je vidljivo, prema Teoremu 15, da je $a-b$ djeljivo s m te da je $c-d$ djeljivo s m. Dakle, njihov zbroj, $(a-b)+(c-d)$, mora biti djeljiv s m, ali ovaj zbroj možemo pojednostaviti do $(a+c)-(b+d)$. Stoga, $(a+c)-(b+d)$ mora biti djeljiv s m.

(b) Možemo dokazati na sličan način kao (a), samo što koristimo činjenicu da $(a-b)-(c-d)$, mora biti djeljivo s m.

(c) Prema Teoremu 15, moramo dokazati da je $ap-bp$ djeljivo s m. Ovu razliku možemo zapisati i kao $(a-b)p$, iz čega je vidljivo da je djeljivo sa m, budući da je prema Teoremu 15, da je $a-b$ djeljivo s m.

(d) Ovaj rezultat se može činiti iznenađujućim na početku. Budući da nam je zadano da $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, poznato nam je da su i $a-b$ i $c-d$ djeljivi s m. Stoga, $c(a-b)+b(c-d)$ također mora biti djeljiv s m prema Teoremima 2 i 3. Posljednji se rezultat može pojednostaviti u obliku $ac-bd$. Dakle, $ac-bd$ je djeljiv s m te iz Teorema 15 slijedi da je $ac \equiv bd \pmod{m}$.

(e) Dokaz ovoga teorema dobija se matematičkom indukcijom:

(B) Za $n=1$ dobijemo $a \equiv b \pmod{m}$, što je očito točno.

(P) $n=k$
Pretpostavimo da vrijedi $a^n \equiv b^n \pmod{m}$

(K) $n=k+1$
Dokažimo da vrijedi $a^{n+1} \equiv b^{n+1} \pmod{m}$
Budući je to ekvivalentno s $aa^n \equiv bb^n \pmod{m}$
Prema **(c)** i **(P)** slijedi dokaz.

Jedno važno opažanje je da ako je broj n djeljiv cijelim brojem k, onda vrijedi $n \equiv 0 \pmod{k}$. Na primjer, 6 je djeljiv s 3, stoga vrijedi $6 \equiv 0 \pmod{3}$.

Zadatak 25. *Koje su posljednje dvije znamenke broja* 3^{25}*?*

Rješenje. Posljednje dvije znamenke možemo dobiti tako da podijelimo broj sa 100 i vidimo koji je ostatak , tj. zanima nas $3^{25} \pmod{100}$. Promatramo da vrijedi $3^4 \equiv 81 \pmod{100}$ te kada kvadriramo obje strane dobijemo $3^8 \equiv 81^2 \pmod{100} \equiv 6561 \pmod{100} \equiv 61 \pmod{100}$, a kada kubiramo obje strane, dobijemo $3^{24} \equiv 61^3 \pmod{100} \equiv 226981 \pmod{100} \equiv 81 \pmod{100}$. Sada pomnožimo obje strane s 3 kako bismo dobili $3^{25} \equiv 243 \pmod{100} \equiv 43 \pmod{100}$. Dakle, posljednje dvije znamenke 3^{25} su 43. Kalkulator ne bi mogao izračunati ovaj broj jer je jednostavno prevelik. Kalkulator će zaokružiti odgovor i neke znamenke će se izgubiti.

Određena pravila vezana za kongruencije su poprilično očigledna. Na primjer, $a + b \equiv b + a \pmod{m}$, ali određena pravila koja vrijede za realne brojeve ne vrijede za kongruencije. Kao jedan od primjera, znamo da, ako je produkt dva realna broja 0, onda jedan od njih mora biti 0. Analogni rezultat za kongruencije ne vrijedi. Primjer bi bio $2 \cdot 3 = 6$, što je kongruentno $0 \pmod{6}$, ali ni 2 ni 3 nisu kongruentni $0 \pmod{6}$.

7.1 Primjena: RSA enkripcija

Poprilično sofisticirana i vrlo važna primjena modularne aritmetike je slučaj RSA enkripcije. Pretpostavimo da želimo poslati informacije nekome, ali ih želimo zaštititi od drugih ljudi koje bi te informacije zanimale (npr. kada koristite svoju kreditnu karticu u svrhu kupovine online s neke web-stranice, želite se pobrinuti da te informacije ne dođu u ruke drugim ljudima). Ovo se postiže uz pomoć RSA enkripcije. Naziv enkripcije dolazi od imena izumitelja ove metode, a to su bili Ron Rivest, Adi Shamir i Leon Adelman. Ova metoda je iznimno sigurna, a otkrivena je 1977. U RSA enkripciji, svaka znamenka broja kreditne kartice je promijenjena ili šifrirana. Stoga, broj koji pošaljemo ni ne sliči pravom broju kartice. Kada je šifrirana poruka poslana, primatelj mora imati „ključ“ da bi dešifrirao poruku koju pošaljete i dobio vaš pravi broj kreditne kartice. Ova metoda je vrlo jednostavno primjenjiva i skoro ju je nemoguće probiti. Otkrivanje ključa koji može dešifrirati kod zahtjeva faktorizaciju velikih brojeva, koje čak ni najnaprednija računala ne mogu obaviti u nekom realnom vremenu. U sljedećem dijelu je sažetak načina funkcioniranja šifriranja i dešifriranja u ovoj metodi. Nije prikazan potpun dokaz zašto metoda funkcionira, ali su opisane ideje koje su ranije predstaviljene u ovom radu, koje se mogu koristiti u ovom području. Svakako, ovo je jedna od onih situacija gdje praktično možete odgovoriti učenicima koje

zanima, „Kada ćemo uopće takvo nešto koristiti?“. Kao primjer uzet ćemo fiktivnu stranicu matematičkestvari.com koja koristi ovu metodu. Prilikom naručivanja nekih materijala za učionicu koristi se kreditna kartica. Kako su podaci osigurani?

1. RSA software zaprima dva prosta broja p i q i broj e koji je relativno primaran u odnosu na broj $\varphi = (p-1)(q-1)$. Obično su brojevi p i q veliki prosti brojevi, no za svrhe ovoga objašnjenja odabrani su mali. Slovo e predstavlja „eksponent enkripcije“.

2. Software pronalazi broj d koji je manji od $n = pq$ takav da vrijedi $ed \equiv 1 \pmod{\varphi}$. To se uvijek može postići, a takav broj se može pronaći uz pomoć Euklidovog algoritma. d označava „eksponent dešifriranja“.

3. Broj kreditne kartice, c, se potencira na e. Rezultat $\pmod{pq}$ se šalje. Ovo nazivamo porukom rezultata s. Da bi dobili pravi broj kreditne kartice c natrag, potenciramo poslanu poruku s na potenciju d, i uzimamo rezultat $\pmod{pq}$. Dobit ćemo c natrag. Ilustrirat ćemo to s manjim brojevima.

Zamislimo da naša kreditna kartica ima samo jedan broj, 9. Želimo ga šifrirati. Odaberemo proste brojeve, na primjer, brojeve 5 i 7, a zatim odaberemo broj e koji je relativno prost sa $\varphi = (5-1)(7-1)$, tj. 24. Neka je $e = 5$. Sada ćemo pronaći broj d takav da vrijedi $ed \equiv 1 \pmod{24}$. Takav broj d je broj 5, budući da vrijedi $ed = 25 \equiv 1 \pmod{24}$. Sada uzimamo našu originalnu poruku, 9, i potenciramo je na e te dobijemo rezultat $\pmod{35}$ (35 je pq). Znamo da je $95 \equiv 4 \pmod{35}$. Dakle, 4 je poruka koja je poslana. Da bismo pronašli originalnu poruku, potenciramo poslanu poruku, 4, na potenciju dešifriranja, 5, te izračunamo rezultat $\pmod{35}$. Dobijemo 45, a to je $\equiv 9 \pmod{35}$. Na taj način smo otkrili originalnu poruku.

Da bismo probili šifru, morali bi prvo naći p i q. To zahtijeva faktorizaciju pq. Ako su p i q veliki brojevi, recimo, svaki od njih ima više od 200 znamenki, čak i uz pomoć superračunala, taj bi pothvat bio ekstremno zahtjevan i mjeseci bi prošli dok bi to uspješno napravili. Naravno, tvrtke koje koriste RSA enkripciju konstantno mijenjaju velike proste brojeve p i q (neke na dnevnoj bazi) te na taj način probijanje šifre postaje nemoguća misija.

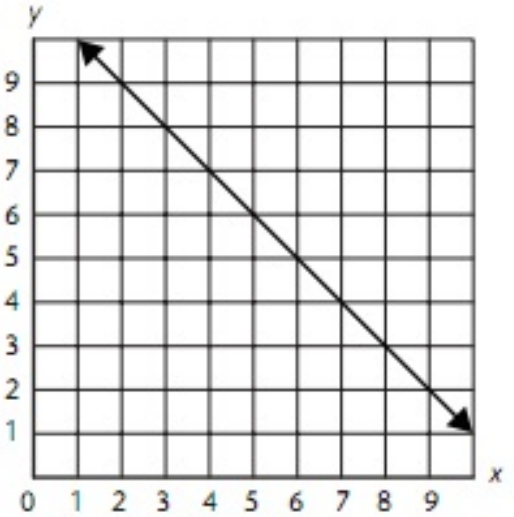
Mnoge se poruke u svijetu šalju uz pomoć RSA enkripcije. Poruke s riječima se transformiraju u brojeve uz pomoć različitih brojeva koji predstavljaju različita slova abecede, a to uključuje i točke, zareze i razmake između riječi. Poruka je poslana kao broj (koji

se zatim pretvara u binarni oblik), a rezultat se onda dešifrira natrag u riječi. RSA enkripcija je poprilično impresivan algoritam i koristi isključivo modularnu aritmetiku, koja se često predstavlja već u srednjim školama.
Postoji odlična web-stranica gdje se možete igrati sa šifriranim porukama i njihovim dešifriranjem. http://www.profactor.at/wstoec/rsa.html. Ova web-stranica pretvara izračune vezane za šifriranje i dešifriranja u bezbolne aktivnosti s kojima se zabavno igrati.

8 Diofantska analiza

Zadatak 26. *Koliko rješenja postoji za linearnu jednadžbu,* $3x + 6y = 4$*? Dajte tri primjera uređenih parova* (x, y) *koja mogu biti rješenje ove jednadžbe. Sastoje li se vaši određeni parovi od vrijednosti* x *i* y *koji su cijeli brojevi?*

Rješenje. Nemoguće je pronaći rješenje jednadžbe $3x + 6y = 4$ u obliku cijelog broja. Postoji li općenita metoda uz pomoć koje možete odmah zaključiti ima li neka linearna jednadžba rješenja u obliku cijelih brojeva?
Sljedeći dio biti će fokusiran na područje algebre i na rješavanje linearnih jednadžbi, što je povezano s brojevnim konceptima koji su tema ovog poglavlja.
Jednadžba poput $2x + 1 = 5$ ima samo jedno rješenje, a to je $x = 2$.
Jednadžba poput $x + 1 = 11$, ima beskonačno puno rješenja, poput $x = 2, y = 9, x = 3, y = 8, x = 4, 2, y = 6, 8$, itd. Sva rješenja ove jednadžbe možemo grafički prikazati. Leže na pravcu koji je grafički prikaz $x + y = 11$. Taj pravac je prikazan na Slici 14 ispod.



Slika 14

Zadatak 27. *Čovjek kupi poštanske marke za* 14 *kuna, a marke koštaju po* 4 *kune i po* 5 *kune. Koliko je kojih poštanskih marki čovjek kupio?*

Rješenje. Ne treba puno vremena da bi shvatili da je kupio jednu marku od 4 kune i dvije od 5 kuna. Međutim, ako želimo, možemo postaviti jednadžbu za ovu situaciju kao što slijedi: ako je x broj kupljenih marki od 4 kune, onda je cijena ovih markica $4x$, a ako je y broj kupljenih markica od 5 kuna, onda je cijena ovih markica $5y$. Dakle,

$$4x + 5y = 14$$

Da smo nasumce napisali ovu jednadžbu, mogli bismo reći, „Oh, ova jednadžba ima beskonačan broj rješenja, stoga postoji veliki broj načina kupovine ovih poštanskih marki da bi ukupan račun bio 14 kuna.“ Ali, odmah ćemo shvatiti da se ova jednadžba razlikuje od jednadžbe $x+y = 11$ koja je ranije navedena te da je ovo praktičan zadatak. Broj svakog tipa marki može imati samo nenegativne vrijednosti. Štoviše, oni moraju biti cijeli brojevi. Dodatno, ako je x veći od 3, ukupna cijena premašuje 14 kuna. To nas, dakle, dodatno ograničava. Zaključak je da x može imati samo vrijednosti cijelih brojeva između 0 i 3, a y može imati samo vrijednosti cijelih brojeva od 0 do 2. Ako uzmemo da je $x = 0, 1, 2, 3$ i riješimo gornju jednadžbu kako bi dobili y, vidimo da je jedini slučaj u kojem je y cijeli broj slučaj kada je $x = 1$, a u tom slučaju, $y = 2$. Dakle, postoji samo jedno rješenje ovog praktičnog zadatka.

Diofantska jednadžba je jednadžba čija rješenja moraju biti cijeli brojevi (što je detaljno proučavao matematičar Diofant). One ne moraju biti linearne kao u ranijem primjeru. Mogu biti kvadratne, kubne, itd. Stoga, $x^2 = y^3 + 1$ također može biti diofantska jednadžba ako nam rješenja trebaju biti cijeli brojevi. Štoviše, ne moraju uopće biti pozitivni cijeli brojevi. Mogu biti bilo koji cijeli brojevi, iako u specifičnim zadacima samo pozitivni cijeli brojevi imaju smisla. Diofantske jednadžbe mogu imati veliki broj rješenja koji variraju od 0 do beskonačno. Razmotrit ćemo nekoliko takvih jednadžbi. Bavit ćemo se samo linearnim diofantskim jednadžbama.

Zadatak 28. *Pronađite sve cijele brojeve za* x *i* y *za koje vrijedi* $2x + 4y = 7$.

Rješenje. Kada bolje pogledamo zadatak, lako je uočiti da ne postoje rješenja ove jednadžbe u obliku cijelih brojeva jer, ako su x i y cijeli brojevi, onda je $2x$ bio djeljiv s 2, $4y$ je također djeljiv s 2, dakle, $2x+4y$ je djeljiv s 2. Stoga, njihov zbroj nikada ne bi mogao biti 7 jer broj 7 nije djeljiv s 2. Zaključak je da ova jednadžba nema rješenja. Ovaj primjer ilustrira općeniti princip da, ako najvećim zajedničkim djeliteljem brojeva a i b ne možemo podijeliti broj c, onda diofantska jednadžba $ax+by=c$ nema rješenje.

Kao suprotan ekstrem imamo sljedeći primjer:

Zadatak 29. *Riješite diofantsku jednadžbu* $3x+4y=7$.

Rješenje. Moramo upamtiti da, kada koristimo riječ diofantska, tražimo da naša rješenja jednadžbe budu cijeli brojevi. Na prvo pogled se $x=1$ i $y=1$ javlja kao jedino moguće rješenje. Zapravo, u ovom slučaju, postoji beskonačno mnogo rješenja u obliku cijelih brojeva, a to su $x=1+4t$ i $y=1-3t$ za svaki cijeli broj t. Mogli bi isprobati različite vrijednosti broja t i vidjeti funkcionira li to, ali puno je jednostavnije zamijeniti ove vrijednosti onima iz prvotne jednadžbe i provjeriti funkcionira li. Dolje su navedeni koraci.

$$\begin{aligned} 3x+4y &= 3(1+4t)+4(1-3t) \\ &= 3+12t+4-12t = 7 \end{aligned}$$

Može se primijetiti da se općenito rješenje navedeno iznad, $x=1+4t$ i $y=1-3t$, sastoji od dva dijela, prvotnog rješenja jednadžbe, $x=1$ i $y=1$, i višekratnika broja t koji su bili koeficijenti jednadžbe, ali u obrnutom redoslijedu. Rješenje za x je uključivalo koeficijent uz y, a rješenje za y je uključivalo koeficijent uz x u prvotnoj jednadžbi, ali sa suprotnim predznakom. Istina je da, ako možemo pronaći jedno rješenje u obliku cijelog broja za neku diofantsku jednadžbu, onda možemo pronaći beskonačno mnogo takvih rješenja i da su oni u ovakvom obliku. Proučit ćemo još jedan primjer prije nego li prikažemo općenito rješenje.

Zadatak 30. *Razmotrite jednadžbu* $3x-4y=8$. *Jedno rješenje u obliku cijelih brojeva je da je* $x=4$, *a* $y=1$. *Pokažite da ova diofantska jednadžba ima beskonačno mnogo takvih rješenja.*

Rješenje. Slijedeći ranije predstavljene upute, iskušat ćemo postupak $x=4-4t$ i $y=1-3t$, gdje je t bilo koji cijeli broj. Kada to uvrstimo u jednadžbu, dobijemo

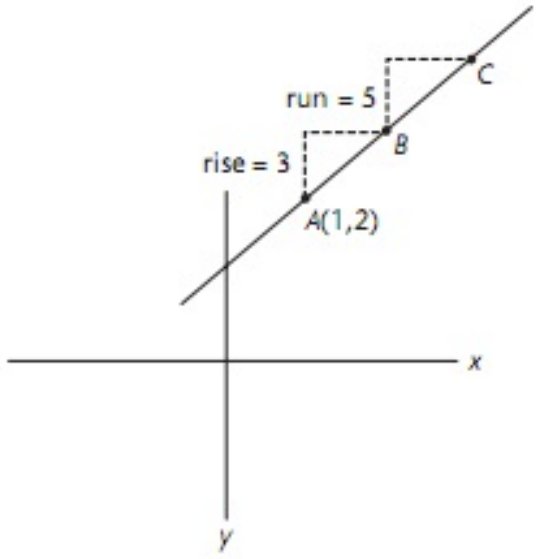
$$3x-4y = 3(4-4t)-4(1-3t)$$

$$= 12 - 12t - 4 + 12t = 8$$

Dakle, funkcionira. Ovo ćemo predstaviti kao teorem.

Teorem 25. *Ako je (x_0, y_0) rješenje diofantske jednadžbe $ax + by = c$, gdje su a, b i c cijeli brojevi, onda vrijedi da su $x = x_0 + bt$, $y = y_0 - at$ također rješenja u obliku cijelih brojeva ove jednadžbe za bilo koji cijeli broj t.*

Učenici uče crtati grafičke prikaze tako da prvo određuju neku točku (x_0, y_0) i zatim uz pomoć koeficijenta smjera pravca određuju drugu točku. Ilustrirajmo to primjerom. Ako želimo nacrtati pravac koji prolazi kroz točke $A = (1, 2)$ s koeficijentom smjera pravca $\frac{3}{5}$, počevši od $A = (1, 2)$, podižemo ga za 3 i mičemo za 5 udesno kako bi pronašli drugu točku, točku B, na pravcu. Od te točke, opet ga podižemo za 3 i mičemo za 5 udesno kako bi dobili treću točku, točku C, na pravcu (Pogledati Sliku 13 ispod).



Slika 15

Možemo podizati koliko god puta želimo, na primjer, t broj puta te dok god to radimo, pronalazit ćemo nove točke na pravcu, tj. točke na pravcu se dobiju na način $x = 1 + 5t$ (prvotni x plus t pomaka za 5) i $y = 2 + 3t$ (prvotni y plus t podizanja za 3). Sada ćemo se vratiti na našu diofantsku jednadžbu, $ax + by = c$, koeficijent smjera pravca je $\frac{-a}{b}$. Počevši od neke točke (x_0, y_0) na crti, pomičemo t puta broj b i podižemo $-a$ puta kako bi došli do nove točke na pravcu. Nova točka je $x = x_0 + bt$ i $y = y_0 - at$. Ovo je razlog zbog kojeg teorem vrijedi. Dakle, znamo kako stvoriti beskonačno mnogo rješenja u obliku cijelih brojeva ukoliko već imamo jedno takvo rješenje. Ali, kako uopće znamo da imamo makar jedno rješenje? Naposljetku, ako

nemamo rješenja, onda gubimo vrijeme tražeći. Sljedeći dokaz nam daje odgovor na to pitanje.

Dokaz. Možemo pronaći cijele brojeve x_0 i y_0 takve da vrijedi $ax_0 + by_0 = 1$. Ako obje strane ove jednadžbe pomnožimo sa c, dobijemo $cax_0 + cby_0 = c$ ili, drugačije rečeno, $a(cx_0) + b(cy_0) = c$. Dakle, cijeli brojevi cx_0 i cy_0 oboje rješavaju zadanu jednadžbu.

Ako a i b nisu relativno prosti, onda će jednadžba $ax + by = c$ imati rješenje samo ako je $nzd(a, b)$ djeljiv sa c. Sada se okrećemo pitanju kako pronaći određeno rješenje za $ax + by = c$. Postoje dva pristupa ovome, koja su manje-više ista. Jedan pristup uključuje modularnu aritmetiku. Prvo ćemo pristup bez modova.

Zadatak 31. *Pronađi određeno rješenje u obliku cijelih brojeva za jednadžbu* $6x+5y = 13$.

Rješenje. Izrazimo y preko x. Dobijemo

$$y = \frac{13 - 16x}{5} = 2\frac{3}{5} - (1\frac{1}{5})x$$

Sada odvojimo dio sa cijelim brojevima svakog od izraza s desne strane i dobijemo

$$y = 2 + \frac{3}{5} - (1 + \frac{1}{5})x$$

$$y = 2 + \frac{3}{5} - x - \frac{1}{5}x$$

ili

$$y = 2 - x + \frac{3 - x}{5}$$

Znamo da x mora biti cijeli broj. To sugerira da je izraz $2-x$, koji se pojavljuje s desne strane gornje jednadžbe, cijeli broj. To znači da je jedini način da y s lijeve strane bude cijeli broj da je $\frac{3-x}{5}$ s desne strane također cijeli broj. Možemo isprobati druge cijele vrijednosti za x (između 0 i 4) i vidjeti koje vrijednosti čine izraz $\frac{3-x}{5}$ cijelim brojem, ali je očigledno da $x = 3$ to uspješno potvrđuje. Kada to uvrstimo u prvu jednadžbu, vidimo da je $y = -1$ rješenje. Dakle, rješenje je $(3, -1)$. Sada možemo pronaći beskonačno mnogo rješenja, kao što smo to napravili gore kada smo uzeli da je $x = 3 + 5t$ i $y = -1 - 6t$ za bilo koju cijelu vrijednost broja t

Ova metoda prikazana gore uvijek funkcionira, ali može se napisati u puno kraćem obliku. Gore navedeni postupak je naveden samo radi boljeg shvaćanja. Započinjemo

s $y = \frac{13-6x}{5}$ i dijelimo brojnik s 5 te razmatramo samo ostatke. Kada 13 podijelimo s 5, ostatak je 3. Kada $6x$ dijelimo s 5, ostatak je $1x$, ali zadržavamo negativan predznak. Stoga, preostali izraz je $3 - x$, koji mora biti djeljiv s 5. Dalje nastavljamo postupak kao i ranije.
Riješimo još jedan primjer.

Zadatak 32. *Riješi:*

$$5x - 3y = 7$$

za x i y cijele brojeve.

Rješenje. Kada izrazimo y, dobijemo

$$y = \frac{5x - 7}{3}$$

Nadalje, kada $5x$ dijelimo s 3, ostatak je $2x$. Kada 7 dijelimo s 3, ostatak je 1, ali zadržavamo negativan predznak. Dakle, ostatak je $2x - 1$, koji mora biti djeljiv s 3. Isprobamo koja od opcija za $x = 0, 1, 2$ funkcionira i otkrijemo da $x = 2$ funkcionira. Kada to uvrstimo u jednadžbu, dolazimo do toga da je $y = 1$. Sada možemo doći do beskonačno mnogo rješenja: $x = 2 - 3t$ i $y = 1 - 5t$.
Sljedeće ćemo predstaviti pristup uz pomoć modova na istom zadatku. Možemo iskoristiti ili $\pmod 3$ ili $\pmod 5$, budući da su oba koeficijenti varijabli. Iskoristit ćemo $\pmod 3$ budući da smo gore praktički primijenili djeljivost s brojem 3. Prvo ćemo promotriti da je bilo koji višekratnik broja 3 zapravo $\equiv 0 \pmod 3$, dakle, $3y$ je kongruentan $0 \pmod 3$. Također, $5x \equiv 2x \pmod 3$. Dakle, $5x - 3y \equiv (2x - 0) \pmod 3$ ili jednostavno, $2x \pmod 3$. Slično tome, desna strana jednadžbe, $7 \equiv 1 \pmod 3$. Stoga, kad iskoristimo $\pmod 3$ na obje strane jednadžbe, ona dobiva sljedeći oblik, $2x \equiv 1 \pmod 3$. Sada samo uvrstimo brojeve za x, neka to budu brojevi $0, 1$ i 2, i odmah vidimo da je $x = 2$ rješava kongruenciju. Dakle, jedno rješenje je $x = 2$, kao što smo to i ranije dobili. Sada to uvrstimo u jednadžbu i dobijemo da je $y = 1$.

Izostavljeno je nešto. Rekli smo da, ako možemo pronaći jedno rješenje linearne diofantske jednadžbe, $ax + by = c$, onda možemo pronaći beskonačno mnogo takvih rješenja, kao što smo to ranije i dokazali, ali nikada nismo pokazali da rješenja do kojih smo došli uz pomoć te metode predstavljaju **sva** takva rješenja. To ćemo sljedeće napraviti.

Teorem 26. *Ako je (x_0, y_0) rješenje diofantske jednadžbe $ax + by = c$, gdje su a i b relativno prosti brojevi, a c je također cijeli broj, onda su sva rješenja ove jednadžbe u obliku $x = x - 0 + bt$, $y = y_0 - at$ gdje t ima sve cijele vrijednosti.*

Dokaz. Pokazat ćemo da, ako je (x_0, y_0) bilo koje cijelo rješenje $ax + by = c$, onda vrijedi $x_1 = x_0 + bt$, $y_1 = y - 0 - at$ za neki broj t, tj. x i y se nalaze u željenom obliku. Budući da (x_1, y_1) zadovoljava $ax + by = c$, vrijedi,

$$ax_1 + by_1 = c$$

. Također, budući da je (x_0, y_0) rješenje $ax + by = c$,

$$ax_0 + by_0 = c$$

. Oduzimajući te izraze, dobijemo $a(x_1 - x_0) + b(y_1 - y_0)$, što sugerira da je $a(x_1 - x_0) = -b(y_1 - y_0)$). Posljednji izraz možemo preoblikovati na sljedeći način:

$$(x_1 - x_0) = \frac{b(y_0 - y_1)}{a}$$

Sada je lijeva strana cijeli broj, a budući da je razlika cijelih brojeva, i desna strana također mora biti cijeli broj. S obzirom da a i b nemaju zajedničkih faktora, $y_0 - y_1$ mora biti djeljivo s a. To znači da vrijedi $(y_0 - y_1) = at$ za neki broj t. To se može preoblikovati i dobivamo $y_1 = y_0 - at$.
Kada to iskoristimo, dobijemo sljedeće,

$$(x_1 - x_0) = \frac{b}{a}(y_0 - (y_0 - at)) = bt$$

koje, kada preoblikujemo, dobijemo, $x_1 = x_0 + bt$, što smo i željeli pokazati.

9 Zaključak

Smatram da u današnjoj nastavi matematike postoji već dosta tema koje se dotiču teorije brojeva, ali bi trebalo posvetiti više pažnje pojašnjavanju pravila, točnije neformalnim dokazima. U svemu tome ključna je edukacija nastavnika koji bi ove koncepte i dokaze trebali vrlo dobro znati i shvaćati. Osim toga, zadaća nastavnika je približiti gradivo učenicima, a kroz ovaj rad ste mogli vidjeti da se to može učiniti u svakom djelu školovanja. Istraživajući teme koje ste upoznali u ovom radu, učenicima se može dati prilika da vide matematiku na jedan drugačiji, zanimljiviji način. To je prilika da mnogi uživaju u matematici i uvide da je ona zaista dio svakodnevnog života.

Sažetak

Teme u ovome radu baziraju se na elementarnoj teoriji brojeva i većina primjera i zadataka koje dokazujemo obrađuju se na nastavi osnovnih škola. No, posljednja poglavlja najprirodnije se uklapaju u nastavu srednjih škola. Važno je napomenuti kako rad ne obuhvaća čitavu granu matematike.

Najprije je uveden pojam djeljivosti kao jedan od najjednostavnijih, ali i ujedno najvažnijih pojmova u teoriji brojeva. Zadatcima i primjerima prikazane su djeljivosti s brojevima 2,3,4,6,11,5,8 i 9. Potom su uslijedili elementarni pojmovi prostih i složenih brojeva te najveći zajednički djeljitelj i najmanji zajednički višekratnik. Osvrnuli smo se i na Euklidov algoritam i temeljne sustave brojeva, a rad je zaokružen modularnom aritmetikom i diofantskom analizom.

Svi teoremi popraćeni su dokazima, formulacije problema pogodne da učenike zainteresira za sadržaj, a cilj rada je ovladati teorijom brojeva i upoznati se s mnogim njezinim primjenama pokazanim u raznim maštovitim primjerima.

Ključne riječi: teorija brojeva, nastava, parnost, djeljivost, primjena, prosti i složeni brojevi, faktorizacija, najveći zajednički djelitelj, najmanji zajednički višekratnik, brojevni sustavi, kongruencija, enkripcija, Diofantska jednadžba.

Summary

Topics in this paper are based on the elementary number theory and most examples and tasks and proofs are for primary school education of mathematics. But the last chapters are beter fit for teaching in high school. It is important to know that the complete knowledge of this branch of mathematics is not covered in this paper.

First, concept of divisibility is introduced as one of the simplest, but also one of the most important concepts in number theory. Rules of divisibility by numbers

2,3,4,6,11,5,8 and 9 are shown through tasks and examples, followed by prime and composite numbers, greatest common divisor and least common multiple. We will also mention the Euclidean algorithm and different base number systems, and the work is completed by modular arithmetic and Diophantine analysis.

All theorems are accompanied by proofs, problems suitable for students interested in the content who aim to master the number theory and become familiar with many of its applications demonstrated in different interesting examples.

Key words: number theory, teaching, even and odd numbers, divisibility, application, prime and complex numbers, factorization, greatest common divisor, lowest common multiple, number system, congruence, encription, Diophantine equation.

Literatura

[1] Matić, I.; *Uvod u teoriju brojeva*, Sveučilište u Osijeku, Osijek,2013.

[2] Reys, R. , Lindquist, M. , Lambdin, D. , Smith, N.; *Helping children learn mathematics*, John Wiley & Sons,2009.

[3] Shroeder, M. R.; *Teorija brojeva u znanosti i komunikaciji*, Springer, Göttingen 1988.

[4] Sultan, A., Artzt, A.F.; *The mathematics that every secondary school math teacher needs to know*,Routlege, New York i London,2011.

[5] Zazkis, R. Campbell, S.R.; *Number theory in mathematics education*, Lawrence Erlbaum Associates, New Jersey,2006.

Životopis

Zovem se Srđana Obradović i rođena sam 20. studenog 1992. godine u Beogradu. Živim u obiteljskoj zajednici s ocem Slavkom, majkom Vesnom i s dvije mlađe sestre Sonjom i Tanjom. Osnovnu školu Borovo u Borovu sam upisala 1999. godine. Tijekom osnovnoškolskog, a kasnije i srednjoškolskog obrazovanja, sudjelovala sam na natjecanjima iz matematike, fizike i geografije. Osim toga aktivno se bavim košarkom već 14 godina. Budući sam osnovnu školu završila izvrsnim uspjehom, 2007. godine upisujem opću gimnaziju u Gimnaziji Vukovar u Vukovaru. 2011. godine upisala sam integrirani nastavnički studij matematike i informatike na Odjelu za matematiku, Sveučilišta J. J. Strossmayera u Osijeku.