

Uvod u teoriju brojeva

Goran Ivanković, Zagreb



Uvod

Teorija brojeva je grana u matematici koja se bavi proučavanjem prirodnih i cijelih brojeva. Tu su nam posebno zanimljivi i prosti brojevi. U ovom tekstu obradit ćemo neke osnovne termine kojima se koristimo u teoriji brojeva, doći ćemo do nekih jednostavnih rezultata te ih zatim iskoristiti u rješavanju nekoliko primjera. Pogledat ćemo najčešće metode koje se koriste na **zadacima s natjecanja** i na kraju ćemo nešto reći o primjeni svega toga u svijetu oko nas. Recimo prvo nešto o problemima s kojima se susrećemo.

Diofantske jednadžbe

Rješavanje zadataka tipa *Riješi u skupu cijelih brojeva jednadžbu* $37x - 4y = 21$ često se svodi na pitanje djeljivosti. Ovakve jednadžbe koje traže rješenje u skupu cijelih ili prirodnih brojeva zovemo **diofantskim jednadžbama**, a jedan od prvih matematičara koji ih je proučavao bio je stari Grk Diofant. Njihovo rješavanje nije uvijek jednostavno i ne postoji univerzalna formula. To se vidi i na jednadžbi $x^n + y^n = z^n$ koja nema prirodna rješenja x, y, z za $n > 2$. Problem je postavio francuski matematičar Fermat još u 17. st. Iako problem zvuči sasvim jednostavno i shvatljiv je gotovo svima, ostao je nedokazan sve do kraja 20. st. Pokušajte sami i vidjet ćete da nije trivijalno!

Mi se, naravno, nećemo baviti tako teškim diofantskim jednadžbama, već ćemo se držati onih koje znamo riješiti. Pa započnimo! (Predlažem da sve primjere koje vidite pokušate prvo sami riješiti ne gledajući rješenja.)

Djeljivost

Prisjetimo se osnova djeljivosti. Neka su a i b cijeli brojevi. Broj b je djeljiv brojem a ako postoji cijeli broj k takav da je $b = k \cdot a$. Pišemo $a \mid b$ te čitamo broj a *dijeli broj* b . Također, pišemo $a \nmid b$ ako broj b nije djeljiv brojem a . Tada čitamo a *ne dijeli* b .

Neka su a, b, c cijeli brojevi takvi da $a \mid b$ i $a \mid c$. Tada su i zbroj $b + c$ i razlika $b - c$ djeljivi s a . Također, ako $a \mid b$ i ako je x proizvoljan cijeli broj, tada je umnožak $b \cdot x$ djeljiv s a .

Ove rezultate koristit ćemo u svim narednim zadacima.

Primjer 1. Vidimo da $5 \mid (10 + 15)$, tj. $5 \mid 25$, također $11 \mid 33$ te $11 \mid 33 \cdot 3$, tj. $11 \mid 99$.

Primjer 2. Odredi sve parove cijelih brojeva x i y čiji je umnožak pet puta veći od njihovog zbroja.

Državno natjecanje 1992., 7. razred

Zapišimo prvo zadatak u obliku jednadžbe. Tražimo $x, y \in \mathbf{Z}$ za koje vrijedi $xy = 5(x + y)$. Ideja je rješenje svesti na pitanje djeljivosti. Prvo transformiramo izraz. Pokušajmo riješiti jednadžbu po jed-

noj varijabli, recimo y , te se u dobivenom brojniku riješiti nepoznanica.

Iz $xy - 5y = 5x$, slijedi

$$y = \frac{5x}{x-5} = \frac{5(x-5) + 25}{x-5} = 5 + \frac{25}{x-5}.$$

Sada zaključujemo da će y biti cijeli broj samo ako je $x-5$ djelitelj od 25, tj. $x-5 \in \{\pm 1, \pm 5, \pm 25\}$. Rješavanjem ovih šest jednačbi dobivamo $x \in \{6, 4, 10, 0, 30, 20\}$. Računajući odgovarajuće vrijednosti dobivamo tražene parove cijelih brojeva: $(6, 30)$, $(4, -20)$, $(10, 10)$, $(0, 0)$, $(30, 6)$, $(-20, 4)$.

Zadatak 1. Odredi sve cijele brojeve a za koje je razlomak $\frac{a^2 - 11a + 24}{a^2 - 9a + 8}$ isto cijeli broj.
Općinsko natjecanje 1995., 8. razred

Zadatak 2. Odredi sve cijele brojeve a za koje je izraz $\frac{a^2 + 1}{a - 1}$ također cijeli broj.
Republičko natjecanje 1990., 8. razred

Metoda faktORIZACIJE

Glavna ideja ove metode je svesti izraz s jedne strane jednačbe na umnožak polinoma, a s druge strane imati cijeli broj. Taj cijeli broj rastavljamo na sve moguće faktore te zatim izjednačavamo faktore s polinomima. Zamislite to ovako: ako je s lijeve strane jednakosti umnožak cjelobrojnih nepoznanica, a na desnoj strani složen broj, lijeva strana treba zapravo biti rastav tog broja na faktore.

Primjer 3. Riješi u skupu cijelih brojeva jednačbu $xy - 2x + y = 5$.

Jednačbu prvo možemo zapisati kao $x(y-2) + y = 5$. Oduzmemo li s obje strane 2, dobivamo $x(y-2) + y - 2 = 3$. Faktorizirajmo sada lijevu stranu:

$$x(y-2) + y - 2 = 3$$

$$(x+1)(y-2) = 3.$$

Za rastavljanje broja 3 na faktore imamo četiri mogućnosti: $3 = 3 \cdot 1 = (-3) \cdot (-1) = 1 \cdot 3 =$

$(-1) \cdot (-3)$. Budući da su x i y cijeli brojevi, cijeli brojevi moraju biti $x+1$, $y-2$. Stoga imamo četiri slučaja:

$$\text{I)} \quad x+1 = 3, y-2 = 1$$

$$\text{II)} \quad x+1 = -3, y-2 = -1$$

$$\text{III)} \quad x+1 = 1, y-2 = 3$$

$$\text{IV)} \quad x+1 = -1, y-2 = -3.$$

Dakle, jedina cjelobrojna rješenja jednačbe su $(2, 3)$, $(-4, 1)$, $(0, 5)$, $(-2, -1)$.

Uz ovu metodu često je korisna supstitucija kako bismo si olakšali faktoriziranje.

Primjer 4. Odredi sve parove prirodnih brojeva (m, n) koji zadovoljavaju jednačbu

$$mn^2 = 100(n+1).$$

Kako je broj s desne strane jednak lijevoj strani, on je djeljiv s n^2 . No, $n+1$ i n su relativno prosti, pa su tako i $n+1$ i n^2 relativno prosti. (Prisjetimo se, brojevi su relativno prosti kada im je 1 najveći zajednički djelitelj.) Stoga mora biti 100 djeljiv s n^2 . Sada rastavljanjem broja 100 na faktore dobivamo samo četiri moguća slučaja.

$$\text{I)} \quad n^2 = 1, \text{ dakle } n = 1 \text{ pa je } m = \frac{100 \cdot (n+1)}{n^2} = \frac{100 \cdot 2}{1} = 200$$

$$\text{II)} \quad n^2 = 4, \text{ dakle } n = 2 \text{ pa je } m = \frac{100 \cdot 3}{4} = 75$$

$$\text{III)} \quad n^2 = 25, \text{ dakle } n = 5 \text{ pa je } m = \frac{100 \cdot 6}{25} = 24$$

$$\text{IV)} \quad n^2 = 100, \text{ dakle } n = 10 \text{ pa je } m = \frac{100 \cdot 11}{100} = 11.$$

Dakle, jedina rješenja su parovi prirodnih brojeva $(200, 1)$, $(75, 2)$, $(24, 5)$, $(11, 10)$.

Zadatak 3. Odredi sve parove cijelih brojeva (x, y) koji zadovoljavaju jednačbu $x^2 - xy - 2y^2 = 18$.
Republičko natjecanje 1989., 8. razred

Zadatak 4. Odredi sva cjelobrojna rješenja jednačbe $x^2 + 11^2 = y^2$.

Županijsko natjecanje 2007., 1. razred, A varijanta

Zadatak 5. Odredi sva cjelobrojna rješenja jednadžbe $x^3 - y^3 = 91$.

Općinsko natjecanje 2008., 2. razred, A varijanta

Metoda ostataka

Često je u kontekstu prirodnih brojeva dobro proučavati ostatke pri dijeljenju nekim drugim brojem. Za male brojeve možemo popisati sve mogućnosti i zatim ih proučavati, pogotovo kada su u pitanju ostaci pri dijeljenju s 2 ili 3. Tada možemo zapisati broj x kao $x = 2k$ za parne, odnosno $x = 2k - 1$ za neparne, za neki prirodan broj k . Slično radimo i za ostatke pri dijeljenju s 3. Nakon ovakvog zapisa lakše nam je obavljati aritmetičke operacije. No, ne smijemo zaboraviti promotriti sve moguće slučajeve!

Primjer 5. Dokaži da je za bilo koja dva prirodna broja a i b uvijek točna barem jedna od ove četiri tvrdnje:

- (1) broj a djeljiv je s 3
- (2) broj b djeljiv je s 3
- (3) zbroj $a + b$ djeljiv je s 3
- (4) razlika $a - b$ djeljiva je s 3.

Neka su a i b proizvoljni prirodni brojevi. Pretpostavimo da za te brojeve ne vrijede ni tvrdnja (1) ni tvrdnja (2). Dokažimo da sada sigurno vrijedi jedna od tvrdnji (3) i (4).

Prvo vidimo da a i b ne mogu davati ostatak 0 pri dijeljenju s 3. Stoga daju ostatak 1 ili 2. Dakle imamo, četiri slučaja:

- I) $a = 3m + 1$, $b = 3n + 1$. Tada je $a - b = 3(m - n)$, što je djeljivo s 3 pa vrijedi tvrdnja (4).
- II) $a = 3m + 1$, $b = 3n + 2$. Tada je $a + b = 3(m + n + 1)$, što je djeljivo s 3 pa vrijedi tvrdnja (3).
- III) $a = 3m + 2$, $b = 3n + 1$. Tada je $a + b = 3(m + n + 1)$, što je djeljivo s 3 pa vrijedi tvrdnja (3).
- IV) $a = 3m + 2$, $b = 3n + 2$. Tada je $a - b = 3(m - n)$, što je djeljivo s 3 pa vrijedi tvrdnja (4).

Tako smo dokazali da vrijedi barem jedna od navedenih tvrdnji.

Želimo li dokazati da diofantska jednadžba nema rješenja, možemo pokazati da su ostaci s lijeve i desne strane jednadžbe pri dijeljenju s nekim brojem različiti. Pogledajmo na primjeru.

Primjer 6. Riješi jednadžbu $x^2 - 4y + 5 = 0$ u skupu prirodnih brojeva.

Zapišimo jednadžbu u obliku $x^2 = 4y - 5$. Na desnoj strani jednakosti je izraz $4y - 5 = 4y - 8 + 3 = 4(y - 2) + 3$ koji pri dijeljenju s 4 daje ostatak 3, no kvadrati prirodnih brojeva uvijek daju ostatak 0 ili 1 pri dijeljenju s 4. Zato lijeva i desna strana jednadžbe ne mogu biti jednake pa dana jednadžba nema rješenja u skupu prirodnih brojeva.

Lema 1. *Kvadrati prirodnih brojeva daju ostatak 0 ili 1 pri dijeljenju s 4.*

Ako je $x = 2k$, tada je $x^2 = 4k^2$ što je djeljivo s 4. Ako je $x = 2k + 1$, tada je $x^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$, pa x^2 daje ostatak 1 pri dijeljenju s 4.

Metoda različitih ostataka

Recimo da imamo umnožak pet uzastopnih prirodnih brojeva, primjerice: $13 \cdot 14 \cdot 15 \cdot 16 \cdot 17$. Primijetimo da svaki od njih daje drukčiji ostatak pri dijeljenju s 5 (3, 4, 0, 1, 2). Kako postoji točno pet mogućih ostataka pri dijeljenju s 5, među tim brojevima sigurno se nalazi broj koji je djeljiv s 5, tj. daje ostatak 0. U ovom slučaju to je 15 i zato je cijeli umnožak djeljiv s 5. Također, vidimo da ćemo tada među njima sigurno imati i barem dva parna broja (ovdje su to 14 i 16) i barem jedan broj djeljiv s 3 (broj 15). Slični zaključci vrijede općenito. Zato nam je u zadacima s djeljivosti često korisno dani izraz prikazati kao umnožak uzastopnih cijelih brojeva.

Primjer 7. Neka je $A = n^3 + 6n^2 + 8n$. Dokaži da je broj A djeljiv brojem 3.

U ovakvim zadacima prvo je uvijek najbolje faktORIZIRATI jer time dobivamo umnožak koji je korisniji od zbroja pri proučavanju djeljivosti.

Prvo vidimo da možemo izlučiti n , pa imamo $A = n(n^2 + 6n + 8)$. Nadalje, izraz u zagradi možemo faktorizirati pa dobivamo $A = n(n^2 + 4n + 2n + 8) = n(n(n + 4) + 2(n + 4)) = n(n + 2)(n + 4)$.

Konačno, vidimo da brojevi n , $n + 2$, $n + 4$ daju različite ostatke pri dijeljenju s 3, pa točno jedan od njih mora biti djeljiv s 3.

Primjer 8. Ako je veći od dvaju uzastopnih prirodnih brojeva kvadrat nekog prirodnog broja, dokaži da je umnožak tih dvaju uzastopnih prirodnih brojeva djeljiv s 12.

Najprije zapišimo to "matematički". Neka je k^2 veći od tih dvaju brojeva. Tada je manji od njih jednak $k^2 - 1$ (primijetimo da je tada $k > 1$, inače $k^2 - 1$ ne bi bio prirodan broj za $k = 1$).

Njihov umnožak je tada jednak $k^2 \cdot (k^2 - 1)$. Možemo uočiti i faktorizirati razliku kvadrata čime dobivamo izraz oblika $k^2(k - 1)(k + 1)$. Sada vidimo da su $k - 1$, k , $k + 1$ tri uzastopna broja pa točno jedan mora biti djeljiv s 3, a tada i umnožak mora biti djeljiv s 3. Preostalo je dokazati da je umnožak djeljiv s 4. Imamo 2 slučaja.

Prvi slučaj: k je paran broj. Tada je $k^2 = k \cdot k$ djeljiv s 4 pa je i umnožak djeljiv s 4.

Drugi slučaj: k je neparan. Tada su $k - 1$ i $k + 1$ parni pa je njihov umnožak djeljiv s 4. Stoga je i traženi umnožak djeljiv s 4. Kako je traženi umnožak djeljiv i s 3 i s 4, on je djeljiv i s $3 \cdot 4 = 12$ (jer su 3 i 4 relativno prosti), čime je tvrdnja dokazana.

Primijetimo da ako je broj a djeljiv s b i c , tako da b i c nisu relativno prosti, broj a ne mora nužno biti djeljiv s $b \cdot c$. Primjer: $a = 12$, $b = 4$, $c = 6$.

Metoda nejednakosti

Ponekad ćemo uspjeti lako pronaći jedno rješenje diofantske jednadžbe i naslutiti da je to jedino rješenje, ali i to je potrebno i dokazati. Ovdje nam mogu dobro doći nejednakosti, tako da ograničimo izraz koji promatramo i dokažemo da ne postoje rješenja veća, odnosno manja od našeg pronađenog rješenja. Pogledajmo primjer:

Primjer 9. Riješi jednadžbu u skupu prirodnih brojeva $3^x + 4^x = 5^x$.

Očito je $x = 2$ jedno rješenje ove jednadžbe. Dijeljenjem zadane jednadžbe s 5^x dobivamo

$$\left(\frac{3}{5}\right)^x + \left(\frac{4}{5}\right)^x = 1.$$

Kako su $\frac{3}{5}$ i $\frac{4}{5}$ između 0 i 1, za $x < 2$ je $\left(\frac{3}{5}\right)^x + \left(\frac{4}{5}\right)^x > \left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$, a za $x > 2$ je $\left(\frac{3}{5}\right)^x + \left(\frac{4}{5}\right)^x < \left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$ te osim

$x = 2$ jednadžba nema drugih rješenja.

Primjena

Danas su rezultati iz ovog područja (pogotovo računi s ostacima pri dijeljenju) iznimno korisni u kriptografiji. Možemo reći da matematika čuva naše podatke sigurnima na internetu, omogućava nam sigurno slanje poruka, transakcije novca i još mnogo toga. Osim toga, teoriju brojeva koristimo i u mnogim algoritmima za generiranje nasumičnih brojeva u računalu. Sasvim nasumičan broj računalu je vrlo teško osmisliti, pa čak je i ljudima vrlo teško. Ako pitate čovjeka da odabere nasumičan broj od 1 do 10, gotovo 27 % odabrat će 7 (provjereno na uzorku studenata PMF-a). Zato postoje razni algoritmi koji koriste velike proste brojeve za generiranje prividno nasumičnih brojeva.

Vratimo se na kriptografiju. Kako nam točno matematika pomaže u sigurnosti podataka?

Recimo da Fran želi Luki poslati poruku: znači poruka treba doći od njegovog računala, pa preko javnih servera i konačno do Lukinog računala. Fran ne želi da itko na javnim serverima može pročitati poruku. Zato trebaju imati **ključ** kojim će šifrirati poruku i za koji neće znati nitko drugi. Takav tip komunikacije zove se **end to end** enkripcija. Ali opet dolazimo do problema. Kako će si poslati ključ putem javnih servera, a da ga nitko ne otkrije? Problem rješava algoritam **Diffie-Hellmanova razmjena ključeva** [2]. Pogledajmo kako. U narednom ćemo tekstu koristiti notaciju **(mod 19)**

što označava ostatak pri dijeljenju s brojem 19. (Općenito, ako brojevi $a, b \in \mathbf{Z}$ daju isti ostatak pri dijeljenju s brojem $c \in \mathbf{N}$, pišemo $a \equiv b \pmod{c}$.)

Prvo će zajedno odabrati prosti broj p , na primjer 19, te poseban broj g , recimo 3. Sada će svatko od njih osmisliti svoj lokalni ključ (prirodni broj manji od p) koji neće nikome podijeliti. Neka je Fran odabrao $a = 5$, a Luka $b = 4$. Sada svatko od njih s pomoću g i p sastavlja tzv. poluključ te ga šalje drugome. Poluključ slažu tako da potenciraju g na broj a (b) pa uzmu ostatak dobivenog broja pri dijeljenju s p .

Dakle, Fran će dobiti $A = 15$ jer je $g^a = 3^5 = 243 \equiv 15 \pmod{19}$, a Luka će dobiti $B = 5$ jer je $g^b = 3^4 = 81 \equiv 5 \pmod{19}$. Sada međusobno izmjenjuju poluključeve. Zatim će uzeti dobivene poluključeve od druge osobe te ih potencirati na broj svog lokalnog ključa. Tako će dobiti konačni ključ.

Fran računa $B^a = 5^5 = 3125 \equiv 9 \pmod{19}$, a Luka $A^b = 15^4 = 50625 \equiv 9 \pmod{19}$. Vidimo da su dobili isti ključ $K = 9$! Primijetite da ako niste Fran ili Luka i pokušate iz poluključeva A i B i brojeva p i g dobiti brojeve a i b (koji su potrebni za sastavljanje ključa), zadatak nije jednostavan. Dakle, ako znate samo brojeve A, B, p i g , trebat ćete puno računanja da sa sigurnošću odredite brojeve a i b . Trebate zapravo isprobati sve mogućnosti. Zamislite sada da su brojevi p i g ogromni, zadatak postaje gotovo nemoguć, čak i za superračunala!

Zadatci za vježbu

1. Odredi sve parove cijelih brojeva x i y koji zadovoljavaju jednadžbu

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{xy} = 1.$$

Županijsko natjecanje 1995., 7. razred

2. Ako je zbroj $u^2 + uv + v^2$ djeljiv s 9, tada su brojevi u i v djeljivi s 3. Dokaži.

Državno natjecanje 1991., 8. razred

3. Odredi sva cjelobrojna rješenja jednadžbe $x^3 - y^3 = 91$.

Općinsko natjecanje 2008., 2. razred, A kategorija

4. Nađi posljednju znamenku broja $1! - 2! + 3! - 4! + \dots + 99!$.

artofproblemsolving.com

5. Odredi sve parove nenegativnih cijelih brojeva (a, b) koji zadovoljavaju jednadžbu:

$$2^a \cdot 3^b - 3^{b+1} + 2^a = 13.$$

Županijsko natjecanje 2010., 1. razred, A varijanta

6. Postoji li 8-znamenkasti broj bez znamenke 0 u dekadskom zapisu koji pri dijeljenju sa svojom prvom znamenkom daje ostatak 1, pri dijeljenju s drugom znamenkom daje ostatak 2, ..., te pri dijeljenju s osmom znamenkom daje ostatak 8?

artofproblemsolving.com

7. Nađi sva cjelobrojna rješenja jednadžbe

$$10x^3 + 20y^3 + 8xyz = 1999z^3.$$

Županijsko natjecanje 1999., 2. razred

LITERATURA

- 1/ https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
- 2/ V. Bajrović (2003.): *Zbirka zadataka za dodatnu nastavu u 7. i 8. razredu osnovne škole*, Tiskara Malenica, Šibenik.
- 3/ <http://www.antonija-horvatek.from.hr/natjecanja-iz-matematike>
- 4/ <https://artofproblemsolving.com/community/>