$\pi\mathrm{l}\alpha y\sqrt{\mathbf{mat}\chi}$

Prosti i relativno prosti brojevi

Marina Šlišković

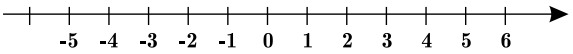
Jednom mi je cimerica rekla da je u jednoj zagrebačkoj knjižnici naišla na knjigu, ništa tanju od Klaićeva *Rječnika stranih riječi*, na kojoj je pisalo *"Osnove fizike"*. U početku mi je, priznajem, bilo pomalo i smiješno, ali sam, radeći na ovom članku, shvatila kako bi se neki fizičar mogao dobro nasmijati istom *„štosu"* kada bi vidio knjigu u koja bi obuhvaćala *osnove teorije brojeva*. Štoviše, teorija brojeva tek je dio matematike!

Naime, namjera mi je bila napisati članak od nekoliko stranica, ali dok sam tražila zanimljive primjere i iskoristive poučke, među mojim se bilješkama našlo toliko "najosnovnijih" zadataka, teorema i ideja da bi ovaj časopis teoriji brojeva duže vrijeme trebao posvećivati popriličan broj stranica kako bi ih sve objavio. Jednostavno se na jedan zadatak sam od sebe vezao drugi! No, što je - tu je.

Nekako sam uspjela naći osnove među osnovama i napisala članak za one koji i ne znaju što je to teorija brojeva, ali i za one koji već odavno barataju njome (neka mi oni iskusniji oproste ako sam izgubila neki bitni ili samo lijepi dio ovog područja). Svejedno, i ovim drugima preporučujem da ga pročitaju − možda se nađe neka zanimljiva priča ili nepoznat detalj... Dakle...

Osnove

Ako cijele brojeve smjestimo na brojevni pravac (kao na slici), primijetit ćemo da su simetrično raspoređeni s obzirom na nulu.



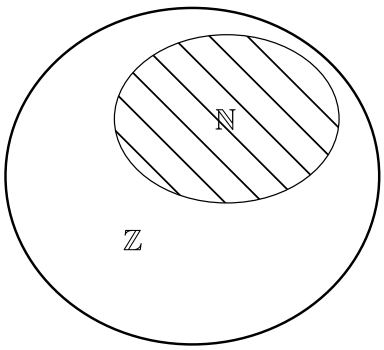
Slika 1.

Cijele brojeve veće od 0 nazivamo prirodnim brojevima i skup svih takvih brojeva označavamo $\mathbb{N}$ (od latinskog *naturalis* - prirodan). Dakle, to su brojevi skupa

$$\{1, 2, \ldots, n-1, n, n+1, \ldots\}.$$

Primijetimo da je skup prirodnih brojeva beskonačan. Tu su činjenicu uočili već stari Grci:

"Mnogo ima zrnaca pijeska u moru
i mnogo je kapljica kiše palo na zemlju,
ali ima brojeva većih i od tog broja."



Slika 2.

Kako je tekao razvoj matematike, sve se češće koristio broj 0. Javila se potreba da se i taj broj negdje *smjesti*. Skup prirodnih brojeva kojima je pridružena nula označavamo $\mathbb{N}_0$ (*"en-nula"*).

Proširimo li i taj skup na skup svih cijelih brojeva $\mathbb{Z}$, dobili smo područje koje proučava **teorija brojeva**.

Dakako, postoje brojevi na brojevnom pravcu koji ne spadaju u dane skupove i čak brojevi koji se uopće ne nalaze na (danom) brojevnom pravcu, ali o tome drugi put.

Za skupove $\mathbb{N}$ i $\mathbb{N}_0$ kažemo da su podskupovi skupa $\mathbb{Z}$ jer je svaki član skupova N i $\mathbb{N}_0$ ujedno i član skupa $\mathbb{Z}$, ali ne i obrnuto. To pišemo:

$$\mathbb{N} \subseteq \mathbb{Z},\ \mathbb{N}_0 \subseteq \mathbb{Z} \quad (\text{"en je podskup od ze"}).$$

Ako želimo označiti da neki broj a pripada nekom skupu brojeva S, pišemo:

$$a \in S \quad (\text{"a iz es"}, \text{"a element od es"}).$$

Djeljivost

Često se spominje podjela cijelih brojeva na parne i neparne. Za one koji (slučajno) ne znaju: parni su oni brojevi koji su djeljivi s 2 (tj. pri dijeljenju sa 2 daju cjelobrojan količnik i ostatak 0). Ostali cijeli brojevi su neparni. ☺ (Za one koji ne znaju i 0 je **paran** broj, jer je $0 = 2 \cdot 0 + 0$.)

Znamo da broj 5 dijeli broj 10 jer je $10 = 5 \cdot 2$. To pišemo: $5|10$.

Osnovna svojstva djeljivosti

Dakle, ako neki cijeli broj a dijeli neki cijeli broj b, tj. ako postoji $k \in \mathbb{Z}$ takav da je $b = k \cdot a$, pišemo: $a|b$. Dva su osnovna svojstva djeljivosti.

1. Ako $a|b$ i $b|c$, onda $a|c$.

Zaista, postoje $k, l \in \mathbb{Z}$ takvi da je $b = k \cdot a$ i $c = l \cdot b$ pa je $c = (kl) \cdot a$, tj. $a|c$.

2. Ako $a|b$ i $a|c$, onda $a|xb + yc$, $\forall x, y \in \mathbb{Z}$ (*"za svaki x, y iz* $\mathbb{Z}$*"*).

Neka je $b = ka$ i $c = la$. Vrijedi: $xb + yc = (xk + yl)a$, tj. $a|xb + yc$, $\forall x, y \in \mathbb{Z}$.

Prosti i složeni brojevi

Često se spominje pojam **prostih** i **složenih** brojeva.

Prosti (***prim***) brojevi imaju točno dva prirodna djelitelja: broj 1 i sami sebe. Dakle, oni se ne mogu zapisati kao umnožak dvaju prirodnih brojeva manjih od njih samih. Takvi su, primjerice

$$2, 3, 5, 7, \ldots, 97, \ldots$$

Brojeve koji imaju više od dva djelitelja (broj 1, sebe i barem još jedan djelitelj) nazivamo složenim brojevima. Takvi su, npr.,

$$10, 15, 18, \ldots, 232, \ldots$$

Svi se složeni brojevi mogu na jedinstven način zapisati kao umnožak prostih brojeva. Lijepo je to izrečeno u knjizi *Stric Petros i Goldbachova slutnja*[1], gdje **A. Doxiadis** kaže da su prosti brojevi

"nedjeljive kvantne čestice brojevnog sustava".

Primijetimo da broj 1 nije ni **složen** ni **prost**. Kako su ***pitagorejci*** razvrstavali brojeve ovisno o broju njihovih djelitelja, smatrali su da 1 **uopće nije broj**! Također, broj 2 je jedini **parni prosti** broj jer su svi ostali parni brojevi djeljivi brojem 2 pa imaju barem tri djelitelja: 1, 2 i sebe. Dakle, nisu prosti.

ZADATAK 1. Odredi prosti broj p ako su brojevi $p + 10$ i $p + 14$ također prosti.

Rješenje. Lako se dokaže da je 3 traženi prosti broj. Primijetimo da brojevi p, $p + 10$ i $p + 14$ daju različite ostatke pri dijeljenju s 3. Dakle, jedan od njih mora biti djeljiv s 3, tj. mora biti jednak 3. To je moguće samo ako je $p = 3$. ✓

[1] Za više o toj knjizi vidi prikaz Martine Nimac i Darije Popović u *PlayMath*-u br. **1**(2003.), str. 48-49.

$\pi \mathrm{l} \alpha y \sqrt{\mathbf{mat}\chi}$

ZADATAK 2. Dokaži da za svaki $n \in \mathbb{N}$ postoji n uzastopnih složenih brojeva.

Rješenje. Primijetimo da su brojevi

$$(n+1)!+2,\ (n+1)!+3,\ (n+1)!+4,\ \ldots\ (n+1)!+n,\ (n+1)!+n+1$$

svi složeni. Uz to, to je n uzastopnih brojeva. ✓

Napomena. $n!$ predstavlja umnožak prvih n prirodnih brojeva tj. $n! = n \cdot (n-1) \cdots 2 \cdot 1$.

ERATOSTENOVO SITO

Sljedeći algoritam kojim se mogu odrediti prosti brojevi nazivamo Eratostenovim sitom prema starogrčkom matematičaru koji je primjenjivao tu metodu dobivanja prostih brojeva. Napišimo redom nekoliko uzastopnih prirodnih brojeva. Npr.:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, \ldots$$

Prvo prekrižimo broj 1 (nije ni prost ni složen).

Dolazimo do broja 2. On je prost pa ga zaokružimo. Sada prekrižimo sve brojeve koji su djeljivi s 2.

Dolazimo do broja 3. Taj je broj prost pa ga zaokružimo. Sada prekrižimo sve višekratnike broja 3, itd.

Svaki put kad dođemo do broja koji nije prekrižen, možemo zaključiti da je prost pa ga zaokružimo i nastavimo križati njegove višekratnike. Na našem se primjeru dobije:

$$\not{1}, \boxed{2}, \boxed{3}, \not{4}, \boxed{5}, \not{6}, \boxed{7}, \not{8}, \not{9}, \not{10}, \boxed{11}, \not{12}, \boxed{13}, \not{14}, \not{15}, \not{16}, \boxed{17}, \not{18}, \boxed{19}, \not{20}, \not{21}, \not{22}, \boxed{23}, \not{24}, \not{25}, \ldots$$

Dakle, prosti brojevi do 25 su: 2, 3, 5, 7, 11, 13, 17, 19 i 23. Ispravnost ovog postupka dokazana je poučkom 2. koji ćete kasnije vidjeti.

Relativno (uzajamno) prostim brojevima nazivamo brojeve koji nemaju zajedničkih prostih djelitelja.

Primjerice, 2 i 8 nisu relativno prosti jer 2 dijeli i 2 i 8 (tj. $2|2$ i $2|8$).

Primjer relativno prostih brojeva su 10 i 21. Jesu li brojevi relativno prosti, lako provjerimo ako ih rastavimo na proste faktore. Npr.:

$$10 = 2 \cdot 5,$$
$$21 = 3 \cdot 7.$$

Vidimo da 10 i 21 nemaju zajedničkog prostog djelitelja pa su relativno prosti.

Najveći zajednički djelitelj dvaju brojeva je najveći broj kojim su djeljiva ta dva broja. Na isti se način definira i najveći zajednički djelitelj nzd više brojeva. Npr., najveći zajednički djelitelj brojeva 2 i 8 je 2. Pišemo:

$$\mathrm{nzd}(2, 8) = 2$$

ili ponekad pišemo $M(2, 8) = 2$ (*mjera*). Primijetimo da je najveći zajednički djelitelj relativno prostih brojeva jednak 1 pa je $\mathrm{nzd}(10, 21) = 1$.

Najmanji zajednički višekratnik dvaju ili više brojeva je najmanji broj koji je djeljiv svim tim brojevima. Tako je najmanji zajednički višekratnik (nzv) brojeva 6 i 4 jednak 12. Dakle:

$$\mathrm{nzv}(6, 4) = 12$$

ili ponekad kraće $v(6, 4) = 12$ (*višekratnik*).

Toliko o osnovama. Slijedi dio *za velike*, a nadam se da će ga i *mali* razumjeti.

EUKLIDOV ALGORITAM Za prirodne brojeve a i b vrijedi:

$$\mathrm{nzd}(a, b) = \mathrm{nzd}(a, a-b).$$

Dokaz. Neka je $\mathrm{nzd}(a, b) = d$, tj. $a = dk$, $b = dl$, pri čemu su k i l relativno prosti brojevi (inače je $\mathrm{nzd}(a, b) > d$). Vrijedi: $a - b = dk - dl = d(k - l)$.

Znači, $\mathrm{nzd}(a, a-b) = \mathrm{nzd}(dk, d(k-l))$. Kako je broj k djeljiv svim svojim djeliteljima (☺), a l nije djeljiv ni jednim od djelitelja broja k (jer su relativno prosti), ni broj $k - l$ nema zajedničkih djelitelja s k. Zato je $\mathrm{nzd}(dk, d(k-l)) = d$, čime je dokazana ispravnost algoritma. ■

Poseban slučaj koji se često koristi prilikom rješavanja zadataka je

$$\mathrm{nzd}(n, n+1) = \mathrm{nzd}(n, n+1-n) = \mathrm{nzd}(n, 1) = 1. \qquad (*)$$

Dakle, dva uzastopna broja **uvijek** su relativno prosta.

ZADATAK 3. Dokaži da je razlomak $\dfrac{21n+4}{14n+3}$ neskrativ za svaki prirodan broj n.

Rješenje. Po Euklidovom algoritmu je:

$$\begin{aligned}\mathrm{nzd}(21n+4, 14n+3) &= \mathrm{nzd}(21n+4-14n-3, 14n+3) = \mathrm{nzd}(7n+1, 14n+3)\\ &= \mathrm{nzd}(7n+1, 14n+3-7n-1) = \mathrm{nzd}(7n+1, 7n+2) = 1.\end{aligned}$$

Dakle, brojnik i nazivnik zadanog razlomka uvijek su relativno prosti brojevi, tj. on nikada nije skrativ. ✓

Slijede neki poznati poučci o prostim brojevima.

Teorem 1. *Postoji beskonačno mnogo prostih brojeva.*
Već je Euklid poznavao ovu činjenicu. Također je naveo dokaz ove tvrdnje koji koristi elementarno znanje teorije brojeva. Teško da će se ikada pronaći jednostavniji dokaz ovako bitne činjenice. Dakle...

Dokaz. Pretpostavimo suprotno, tj. da postoji konačno mnogo prostih brojeva. Neka su svi prosti brojevi koji postoje redom $p_1, p_2, \ldots, p_n$. Označimo s P njihov umnožak, tj. $P := p_1 p_2 \cdots p_n$. Tada bi $P+1$ trebao biti složen broj. Primijetimo da broj $P+1$ pri dijeljenju svim postojećim prostim brojevima daje ostatak 1. Dakle, broj $P+1$ mora biti prost. Dolazimo do kontradikcije pa početna tvrdnja ne može biti točna. Dakle, postoji beskonačno mnogo prostih brojeva. ■

Teorem 2. *Prirodan broj n prost je ako i samo ako nema ni jednog djelitelja, osim broja* 1*, manjeg ili jednakog* $\sqrt{n}$*.*

Dokaz. Pretpostavimo da je $n = ab$, pri čemu je $a \leq b$. Tada je $a^2 \leq n$, tj. $a \leq \sqrt{n}$. Ako ne postoji prirodan broj a koji zadovoljava prethodno, broj se ne može rastaviti na faktore, tj. prost je. Ako postoji takav broj, n se može rastaviti na faktore, tj. složen je. ■

Napomena. Ovim je dokazana ispravnost Eratostenovog sita.

Teorem 3. *Svi prosti brojevi, osim* 2 *i* 3*, oblika su* $6k \pm 1$ *(*$k \in \mathbb{N}$*).*

Dokaz. Osim oblika navedenog oblika, prirodni brojevi mogu imati oblik $6k$, $6k+2$ ili $6k+3$. U prvim dvama slučajima broj je djeljiv s 2, a u trećem s 3. Kako su ti brojevi veći od 3, moraju biti složeni. Dakle, vrijedi tvrdnja teorema. ■

Napomena. Ne vrijedi obrat navedene tvrdnje! Tako, npr., broj $35 = 6 \cdot 6 - 1$ ima navedeni oblik, ali nije prost $(35 = 7 \cdot 5)$.

ZADATAK 4. Dokaži da je za prosti broj $p \geq 5$ broj $p^2 - 1$ djeljiv s 24.

Rješenje. Sama konstrukcija zadatka navodi nas da iskoristimo poučak 3. Dakle, za proste brojeve $p \geq 5$ vrijedi:

$$\begin{aligned}p^2 - 1 &= (6k \pm 1)^2\\ &= 36k^2 \pm 12k\\ &= 12k(3k \pm 1).\end{aligned}$$

Kako su brojevi k i $3k \pm 1$ različite parnosti, dani izraz djeljiv je s 24. ✓

Toliko za sada. U idućim brojevima *PlayMath*-a moći ćete doznati još ponešto o teoriji brojeva. U dokazivanju nekih zadataka u daljnjem dijelu koristit ću svojstva kongruencija. Onima koji ne znaju ta svojstva i općenito pojam *kongruencija*, toplo preporučujem članak Azre Tafro iz *PlayMath*-a br. **3**(2003.).