ACTA MATHEMATICA SPALATENSIA
Series didactica
Vol.6 (2023) 55–64

Zaprimljen: 23. veljače 2023
Prihvaćen: 9. lipnja 2023.

Prosti brojevi i aritmetički nizovi

Ivan Matić

Sažetak

U ovom ćemo radu prikazati dva fundamentalna problema koji povezuju proste brojeve i aritmetičke nizove, dva elementarna pojma koji često imaju značajnu ulogu u vrlo kompliciranim i interesantnim problemima. Iznijet ćemo poznate važne rezultate te riješiti nekoliko srodnih problema korištenjem osnovnih metoda teorije brojeva.

Ključni pojmovi: prosti brojevi, djeljivost, aritmetički nizovi, uzastopni članovi.

1. Uvod

Prosti brojevi pripadaju među najistraživanije teme u čitavoj matematici, što zbog svojih posebnih svojstava, a što zbog različitih primjena i važnog mjesta koje zauzimaju kao temeljni gradivni blokovi svakog prirodnog broja većeg od 1 što je iskazano u Osnovnom teoremu aritmetike. Nešto manje istaknutu, ali itekako značajnu ulogu u istraživanjima zauzimaju aritmetički nizovi, kao specijalna i relativno jednostavna vrsta nizova realnih brojeva.

Veza između ovih dvaju objekata tijekom dugog niza godina predstavlja izazov i zadaje glavobolje brojnim matematičarima. U ovom ćemo radu izdvojiti neke od najvažnijih ostvarenih rezultata, popraćenih ilustrativnim primjerima. Pri tome nećemo zadirati duboko u stoljećima razvijane alate, već ćemo nastojati da iskazi i riješeni primjeri budu razumljivi i srednjoškolcima i zaljubljenicima u teoriju brojeva. Upravo ćemo iz tog razloga izbjegavati i korištenje nešto poznatijih i standardnijih alata teorije brojeva, poput kongruencija.

Podsjetimo, za prirodan broj n, $n > 1$, kažemo da je prost ukoliko su jedini njegovi djelitelji 1 i n. Primjerice, brojevi 2, 5, 37 i 55555544444441 su prosti, pri čemu treba primijetiti kako često nije jednostavno ispitati je li broj s većim brojem znamenki prost.

Navedimo kratko neka korisna svojstva, koja se mogu pronaći u [1, 3, 4]:

Lema 1. *1. Postoji beskonačno mnogo prostih brojeva.*

2. Ako prost broj dijeli produkt, tada dijeli i neki od faktora.

3. (Osnovni teorem aritmetike) Svaki se prirodan broj veći od 1 *može prikazati u obliku produkta prostih brojeva, pri čemu je takav prikaz jedinstven do na poredak faktora.*

Kažemo da je niz aritmetički ako je razlika svaka dva uzastopna člana tog niza jednaka, odnosno konstantna. Kako bi potpuno zadali aritmetički niz, dovoljno je zadati njegov prvi član te razliku dvaju uzastopnih članova. Označimo li aritmetički niz s (a_n), pri čemu smatramo da je a_n n-ti član tog niza, prvi član niza s a_1 te razliku dvaju uzastopnih članova s d, tada je drugi član niza dan s $a_2 = a_1 + d$, treći član s $a_3 = a_2 + d = a_1 + 2d$ te, općenito, n-ti je član dan s $a_1 + (n-1)d$.

Nas će zanimati aritmetički nizovi čiji su članovi prirodni brojevi pri čemu je prvi član označen s a, dok je razlika uzastopnih članova niza označena s d. Takav niz se, radi jednostavnosti zapisa, obično zadaje s $a + nd$, pri čemu su a i d prirodni brojevi, dok je n nenegativan cijeli broj.

2. Prosti brojevi u aritmetičkim nizovima

Prvi interesantan problem koje povezuje proste brojeve i aritmetičke nizove je pitanje pojavljivanja prostih brojeva u danom aritmetičkom nizu. Odaberemo li prvi član niza a i razliku uzastopnih članova niza d, postavlja se pitanje uz koje će se uvjete u nizu prirodnih brojeva $a+nd$, $n = 0, 1, 2, \ldots$, pojavljivati prosti brojevi te koliko će ih biti.

Naravno, ovo se pitanje može iskazati i u obliku formulacije često korištene u teoriji brojeva: Koliko postoji prostih brojeva oblika $a+nd$?

Kako bismo izbjegli trivijalni slučaj konstantnog niza, želimo da je d prirodan broj. Promotrimo najprije važan specijalni slučaj. Prisjetimo se da za dva prirodna broja kažemo da su relativno prosti ako je njihov najveći zajednički djelitelj jednak 1, odnosno ako nisu oba djeljivi s niti jednim prirodnim brojem većim od 1.

Pretpostavimo najprije da a i d nisu relativno prosti te neka je k njihov najveći zajednički djelitelj. Tada je s k djeljiv i $a + nd$, koji je

strogo veći i od a i od d za $n \geq 1$. Budući da je $k < a + nd$ i $k > 1$, onda $a + nd$ ne može biti prost broj za $n \geq 1$.

Prema tome, ako a i d nisu relativno prosti te a nije prost broj, aritmetički niz koji se sastoji od brojeva $a + nd$, $n = 0, 1, 2, \ldots$, ne sadrži niti jedan prost broj. Ako a i d nisu relativno prosti te je a prost, tada je jedini prost član aritmetičkog niza $a + nd$, $n = 0, 1, 2, \ldots$, upravo a.

Ovim smo pokazali kako je nužan uvjet da se u aritmetičkom nizu $a + nd$, $n = 0, 1, 2, \ldots$, pojavljuje više od jednog prostog broja upravo da a i d moraju biti relativno prosti. Da je ovaj uvjet i dovoljan, prvi je pokazao Dirichlet 1837. godine:

Teorem 2 (Dirichlet)**.** *Ako su a i d relativno prosti prirodni brojevi, tada postoji beskonačno mnogo prostih brojeva oblika $a + nd$, gdje je n prirodan broj.*

Dokaz općenitog Dirichletova rezultata uvelike nadilaze okvire ovog rada te se, primjerice, može pronaći u osmom poglavlju knjige [6].

Kako za svaki prirodan broj d vrijedi da je najveći zajednički djelitelj brojeva 1 i d jednak 1, iz teorema 2 slijedi da za svaki prirodan broj d postoji beskonačno mnogo prostih brojeva oblika $dn+1$. Također, kako su svaka dva uzastopna prirodna broja relativno prosta, za svaki prirodan broj k postoji beskonačno mnogo prostih brojeva oblika $nk + k + 1$ i oblika $n(k + 1) + k$.

U nastavku ćemo vidjeti kako se mogu dokazati neke specijalni slučajevi teorema 2. Pri tome će nam koristiti Mali Fermatov teorem:

Teorem 3 (Mali Fermatov teorem)**.** *Ako je p prost broj koji ne dijeli cijeli broj a, tada p dijeli $a^{p-1} - 1$.*

Također će nam biti potrebna i iduća elementarna lema.

Lema 4. *Neka je t prirodan broj te neka su a, b, c i d cijeli brojevi takvi da t dijeli $a - b$ i t dijeli $c - d$. Tada t dijeli i $ac - bd$. Posebno, ukoliko t dijeli razliku $a - b$, tada t dijeli i razliku $a^m - b^m$ za svaki prirodan broj m.*

Dokaz. Neka su k i l cijeli brojevi takvi da je $a - b = kt$ i $c - d = lt$. Tada je

$$ac - bd = ac - bc + bc - bd = (a - b)c + b(c - d) = ktc + ltb = t(kc + lb)$$

pa t dijeli $ac - bd$. Uzmemo li $c = a$ i $d = b$ dobivamo da t dijeli i razliku $a^2 - b^2$ te, ponavljanjem ovog postupka, slijedi da t dijeli i razliku $a^m - b^m$. $\square$

Pokažimo da aritmetički niz $a+nd$, $n=0,1,2,\ldots$ sadrži beskonačno mnogo prostih brojeva u slučaju $a=1$ i $d=4$. Podsjetimo, za prirodan broj n s $n!$ označavamo produkt prirodnih brojeva od 1 do n, odnosno $n!=1\cdot 2\cdots n$.

Teorem 5. *Postoji beskonačno mnogo prostih brojeva oblika* $4n+1$, $n\in\mathbb{N}$.

Dokaz. Neka je m proizvoljan prirodan broj veći od 1 te neka je $M=(m!)^2+1$.

Kako je $m>1$, slijedi da je broj $m!=1\cdot 2\cdots m$ paran te je veći ili jednak 2. Zato je broj M neparan i veći ili jednak 5. Označimo s p najmanji prost djelitelj broja M.

Kako bi pokazali da je $p>m$, pretpostavimo najprije da je $p\leq m$. Tada se p pojavljuje u produktu $2\cdot 3\cdots m=m!$ pa p dijeli $m!$ te dijeli i $(m!)^2$. Kako p dijeli i M, p mora dijeliti i razliku $M-(m!)^2=1$, što nije moguće. Zato je $p>m$ i očito neparan jer je $m\geq 2$.

Budući da p dijeli $M=(m!)^2+1=(m!)^2-(-1)$ i kako je $\frac{p-1}{2}$ prirodan broj, koristeći lemu 4 dobivamo da p dijeli i $((m!)^2)^{\frac{p-1}{2}}-(-1)^{\frac{p-1}{2}}=(m!)^{p-1}-(-1)^{\frac{p-1}{2}}$.

Primijetimo da p ne dijeli $m!$, jer kada bi prost broj p dijelio produkt $1\cdot 2\cdots m$, morao bi, prema dijelu (2) leme 1 dijeliti i neki od njegovih faktora, što nije moguće jer je $p>m$. Stoga, koristeći Mali Fermatov teorem dobivamo da p dijeli $(m!)^{p-1}-1$.

Prema tome, p dijeli i $(m!)^{p-1}-(-1)^{\frac{p-1}{2}}$ i $(m!)^{p-1}-1$ pa p mora dijeliti i razliku

$$(m!)^{p-1}-(-1)^{\frac{p-1}{2}}-\big((m!)^{p-1}-1\big)=1-(-1)^{\frac{p-1}{2}}.$$

Kako je $p>2$, slijedi $(-1)^{\frac{p-1}{2}}=1$, odnosno $\frac{p-1}{2}$ je paran te iz $\frac{p-1}{2}=2n$ dobivamo $p=4n+1$ za neki prirodan broj n. Dakle, za proizvoljan prirodan broj m veći od 1 postoji prost broj oblika $4n+1$ koji je veći od m, što povlači da postoji beskonačno mnogo prostih brojeva tog oblika. $\square$

Na nešto jednostavniji način možemo pokazati da aritmetički niz $a+nd$, $n=0,1,2,\ldots$ sadrži beskonačno mnogo prostih brojeva u slučaju $a=3$ i $d=4$.

Teorem 6. *Postoji beskonačno mnogo prostih brojeva oblika* $4n+3$, $n\in\mathbb{N}$.

Dokaz. Neka je m proizvoljan prirodan broj veći od 3 te neka je $M=(m!)-1$. Tada je $m!$ djeljivo s 4 pa je M oblika $4k-1$, za neki prirodan

broj k. Primijetimo da je $(4r+1)(4s+1) = 4(4rs+r+s)+1$ te zato ne mogu svi prosti faktori od M biti oblika $4l+1$, jer bi tada i M morao biti tog oblika. Prema tome, postoji prost faktor p od M oblika $p = 4n+3$. Na isti način kao u dokazu prethodnog teorema možemo vidjeti da je $p > m$ pa smo za proizvoljan broj m, $m \geq 4$, pronašli prost broj p oblika $4n+3$ koji je veći od m. Dakle, postoji beskonačno mnogo prostih brojeva tog oblika. $\square$

Pogledajmo u nastavku i neke primjene teorema 2.

Primjer 1. *Neka je k proizvoljan prirodan broj. Pokažimo da postoji prost broj p kojem je barem k znamenki jednako nuli.*

Rješenje. Kako su prirodni brojevi 1 i 10^{k+1} relativno prosti, iz teorema 2 uz $a = 1$ i $d = 10^{k+1}$ slijedi da postoji prirodan broj n takav da je $p = 10^{k+1}n + 1$ prost broj. Zadnjih $k+1$ znamenki broja $10^{k+1}n$ su nule pa su zadnjih $k+1$ znamenki prostog broja k nula te jedna jedinica. Prema tome, prost broj p ima barem k znamenki jednako nuli.

Primjer 2. *Neka je k proizvoljan prirodan broj. Pokažimo da postoji prost broj p čija je suma znamenki veća od k.*

Rješenje. Kako su prirodni brojevi 10^k i $10^k - 1$ uzastopni, onda su i relativno prosti. Uz $a = 10^k - 1$ i $d = 10^k$, iz teorema 2 slijedi da postoji prirodan broj n takav da je $p = 10^k n + 10^k - 1$ prost. Zadnjih k znamenki broja $10^k n$ su nule, dok se zapis broja $10^k - 1$ sastoji od k devetki. Prema tome, u zapisu prostog broja p se pojavljuje k devetki pa je suma znamenki broja p veća od k.

Primjer 3. *Neka su a i d relativno prosti prirodni brojevi te neka je m prirodan broj. Pokažimo da u aritmetičkom nizu $a + nd$, $n = 0, 1, 2, \ldots$, postoji beskonačno mnogo članova koji se mogu prikazati u obliku produkta m različitih prostih brojeva.*

Rješenje. Kako bi dokazali ovu tvrdnju, koristit ćemo matematičku indukciju. Za $m = 1$ je navedeni rezultat upravo tvrdnja teorema 2.

Pretpostavimo sada da tvrdnja vrijedi za prirodan broj k te ju dokažimo za prirodan broj $k+1$. Iz pretpostavke slijedi da postoji prirodan broj n_1 takav da je $a + n_1 d = p_1 p_2 \cdots p_k$, pri čemu su $p_1, p_2, \ldots, p_k$ različiti prosti brojevi te možemo uzeti da je $p_1 < p_2 < \cdots < p_k$. Kako su brojevi 1 i d relativno prosti, prema teoremu 2 postoji beskonačno mnogo prostih brojeva oblika $1 + nd$, te postoji i beskonačno mnogo prostih brojeva oblika $1 + nd$ koji su veći od p_k. Označimo jedan takav prost broj s p te neka je n_2 prirodan broj za koji vrijedi $p = 1 + n_2 d$. Definirajmo $t = p_1 p_2 \cdots p_k n_2 + n_1$.

Tada je

$$a + td = a + (p_1p_2 \cdots p_kn_2 + n_1)d = a + n_1d + p_1p_2 \cdots p_kn_2d =$$
$$p_1p_2 \cdots p_k + p_1p_2 \cdots p_kn_2d = p_1p_2 \cdots p_k(1 + n_2d) = p_1p_2 \cdots p_kp.$$

Na ovaj način za svaki prost broj p oblika $1 + nd$ koji je veći od p_k dobivamo broj $a+td$ koji se može prikazati u obliku produkta $k+1$ prostih brojeva $p_1, p_2, \ldots, p_k, p$. Kako postoji beskonačno mnogo takvih prostih brojeva p, dobivamo beskonačno mnogo članova aritmetičkog niza $a+nd$, $n = 0, 1, 2, \ldots$, koji se mogu prikazati u obliku produkta $k + 1$ prostih brojeva. Prema principu matematičke indukcije tvrdnja vrijedi za svaki prirodan broj m.

Primjer 4. *Pokažimo da za svaki prirodan broj m postoji prost broj p takav da $p + 1$ ima više od m djelitelja.*

Rješenje. Neka je q proizvoljan prost broj. Kako su brojevi q^m i $q^m - 1$ relativno prosti, prema teoremu 2 postoji prost broj p, $p > q^m - 1$, oblika $q^mn + q^m - 1$. Tada je $p + 1 = q^md + q^m = q^m(d + 1)$ pa je $p + 1$ djeljiv s q^m te je djeljiv i brojevima $1, q, q^2, \ldots, q^m$, odnosno ima više od m djelitelja.

3. Aritmetički nizovi prostih brojeva

Prema teoremu 2, uz uvjet da su prvi član aritmetičkog niza i njegova razlika relativno prosti, u tom aritmetičkom nizu postoji beskonačno mnogo prostih brojeva. No, ovaj nam rezultat ne govori ništa o tome kako su prosti brojevi raspoređeni u tom nizu, odnosno hoće li eventualno neki od njih biti i uzastopni članovi niza. To nas pitanje dovodi do problema koji se pokazuju mnogo izazovnijima. Kako bismo ih mogli jasnije iskazati, za aritmetički niz $a + nd$, $n = 0, 1, 2, \ldots$, i prirodan broj k, uređenu ćemo k-torku $(a, a + d, \ldots, a + (k - 1)d)$ nazvati *aritmetički niz duljine k*. Primijetimo kako se ustvari radi o zapisu prvih k članova aritmetičkog niza.

Prirodno je postaviti sljedeća pitanja. Za koji prirodan broj k postoji aritmetički niz duljine k koji se sastoji od prostih brojeva? Naravno, uz uvjet da je razlika tog niza različita od nule. Može li se nešto zaključiti u vezi odnosa između broja k i razlike takvog aritmetičkog niza duljine k? Možemo li za neki k odrediti aritmetički niz duljine k koji se sastoji od prostih brojeva?

Prethodna pitanja također datiraju unazad više stotina godina, a bilo je potrebno mnogo rada i truda kako bi se došlo do odgovora. Dugoočekivano je rješenje objavljeno prije 15-ak godina ([2, Theorem 1.1]):

Teorem 7 (Green-Tao). *Za svaki prirodan broj k postoji beskonačno mnogo aritmetičkih nizova duljine k čiji su svi članovi prosti brojevi.*

Teorem 7 predstavlja izuzetno dubok rezultat koji je čisto egzistencijalne prirode. Ovaj nam rezultat garantira da u skupu prostih brojeva postoje aritmetički nizovi proizvoljne duljine, ali ne otkriva recept kako do njih doći. Pogledajmo jedan djelomičan rezultat u tom smjeru.

Propozicija 8. *Neka su a i d prirodni brojevi. Ako su svi članovi $a, a+d, \ldots, a+(k-1)d$ aritmetičkog niza duljine k, $k > 1$, neparni prosti brojevi, tada je d djeljiv svakim prostim brojem manjim od k.*

Dokaz. Kako je a neparan prost broj, vrijedi $a \geq 3$. Također je i $a \geq k$, jer bi iz $a < k$ slijedilo da se u aritmetičkom nizu $(a, a+d, \ldots, a+(k-1)d)$ duljine k nalazi i $a + ad = a(1+d)$, koji nije prost jer je djeljiv i s a i s $1+d$.

Neka je p prost broj manji od k. Primijetimo da niti jedan od brojeva $a, a+d, \ldots, a+(p-1)d$ nije djeljiv s p, jer su svi ovi brojevi prosti i veći od p. Prema tome, ostatci koje ovih p brojeva daju pri dijeljenju s p su elementi skupa $\{1, 2, \ldots, p-1\}$. Zato postoje dva različita broja iz skupa $\{a, a+d, \ldots, a+(p-1)d\}$ koji daju isti ostatak pri dijeljenju s p. Drugim riječima, postoje $r, s \in \{0, 1, \ldots, p-1\}$ takvi da je $r > s$ i p dijeli $(a+rd) - (a+sd) = rd - sd = (r-s)d$. Kako je p prost i dijeli umnožak $(r-s)d$, p mora dijeliti i neki od faktora $r-s$ i d. Zbog $r, s \in \{0, 1, \ldots, p-1\}$ i $r > s$ je $r - s \in \{1, 2, \ldots, p-1\}$ te p ne može dijeliti $r-s$. Zato p dijeli d te je d djeljiv svakim prostim brojem manjim od k. $\square$

Ukoliko su svi članovi $a, a+d, \ldots, a+(k-1)d$ aritmetičkog niza duljine k prosti brojevi, tada jedino a može biti paran, jer je $a + d > a$. Ako je i d paran, tada je paran i $a+d$, koji je također i veći od 2 pa ne može biti prost. Ako je d neparan, tada je $a + 2d$ paran te ne može biti prost. Prema tome, za paran a duljina k ne može biti veća od 2. Ukoliko su i a i d neparni, tada je $a+d$ paran broj veći od 2 te ne može biti prost. Prema tome, duljina k može biti veća od 2 jedino kada je a neparan i d paran te su tada svi $a, a+d, \ldots$ neparni. Primijetimo da se tada upravo radi o situaciji opisanoj propozicijom 8.

Iz te propozicije slijedi da ukoliko su svi $a, a+d, \ldots, a+(k-1)d$ neparni prosti te ako označimo proste brojeve manje od k s $p_1, p_2, \ldots, p_s$, tada d mora biti djeljiv s produktom $p_1 p_2 \cdots p_s$.

Primjerice, ako su svi članovi aritmetičkog niza duljine 10 prosti brojevi, tada je razlika d djeljiva s $2 \cdot 3 \cdot 5 \cdot 7 = 210$, dok razlika aritmetičkog niza duljine 20 čiji su svi članovi prosti brojevi mora biti djeljiva čak s $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = 9699690$.

Primjer 5. *Odredimo aritmetički niz duljine* 6 *čiji su svi članovi prosti brojevi, s najmanjim mogućim posljednjim članom.*

Rješenje. Trebamo odrediti prirodne brojeve a i d takve da su svi brojevi $a, a+d, a+2d, a+3d, a+4d, a+5d$ neparni prosti te da je $a+5d$ najmanji mogući, odnosno ako za neke prirodne brojeve a' i d' vrijedi da su svi $a', a'+d', a'+2d', a'+3d', a'+4d', a'+5d'$ neparni prosti tada je $a+5d \leq a'+5d'$. Kako je duljina traženog aritmetičkog niza jednaka 6, iz propozicije 8 slijedi da d mora biti djeljiv s 2, 3 i 5 te je najmanji mogući d jednak 30.

Kako a mora biti neparan prost, najmanje vrijednosti koje može poprimiti su $3, 5$ i 7. Ako je $a \in \{3, 5\}$, tada je $a+d = a+30 \in \{33, 35\}$ pa $a+d$ nije prost broj. Zato a može najmanje biti jednak 7. Za $a = 7$ dobivamo aritmetički niz $(7, 37, 67, 97, 127, 157)$ duljine 6 čiji su svi članovi prosti brojevi.

Primijetimo da svaki drugi aritmetički niz duljine 6 čiji su svi članovi prosti brojevi te čija je razlika jednaka 30 ima zadnji član veći od 157. Promatramo li aritmetičke nizove duljine 6 čiji su svi članovi prosti brojevi te im je razlika različita od 30, dobivamo da je njihova razlika veća ili jednaka 60, jer mora biti djeljiva s 30. Odatle slijedi da je zadnji član takvog aritmetičkog niza duljine 6 veći do $5 \cdot 60 = 300$. Zato je $(7, 37, 67, 97, 127, 157)$ traženi aritmetički niz duljine 6.

Najdulji trenutno poznati aritmetički niz $a, a+d, \ldots, a+(k-1)d$ čiji su svi članovi prosti brojevi konstruiran je 2019. godine. Duljina je tog niza jednaka 27 te se on dobiva za

$$a = 224584605939537911$$

i

$$d = 81292139 \cdot 223092870 = 81292139 \cdot (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23).$$

Napomenimo kako je u trenutku objave rezultata [2] najdulji poznati aritmetički niz čiji su svi članovi prosti brojevi bio duljine 23 i dobivao se u slučaju $a = 56211383760397$ i $d = 44546738095860$, dok je u trenutku objave knjige [4] najdulji poznati aritmetički niz čiji su svi članovi prosti brojevi bio duljine 19 te se dobivao za $a = 8297644387$ i $d = 4180566390$. Naravno, radi se o rezultatima koji su u tom trenutku bili poznati autorima navedenih referenci, a iz kojih se može razaznati i napredak u numeričkom određivanju nizova s traženim svojstvom, ali i koliko je komplicirano konstruirati takve nizove veće duljine, unatoč prednostima koje pružaju moderna računala.

U nastavku pogledajmo i dva slučaja koja dobivamo kada promatramo aritmetičke nizove duljine k s fiksiranom razlikom.

Primjer 6. *Odredimo najveći k za koji postoji aritmetički niz duljine k čiji su svi članovi prosti brojevi te je razlika tog niza jednaka* 10. *Za takav k odredimo sve aritmetičke nizove duljine k čiji su svi članovi prosti brojevi i razlika je tog niza jednaka* 10.

Rješenje. Ako je $k \geq 4$, tada bi prema propoziciji 8 razlika tog niza morala biti djeljiva s 3. Kako 10 nije djeljivo s 3, slijedi da je $k \leq 3$. Pogledajmo možemo li konstruirati aritmetički niz $(a, a+10, a+20)$ duljine 3 čiji su članovi prosti brojevi. Za $a = 3$ dobivamo aritmetički niz $(3, 13, 23)$ duljine 3 čiji su svi članovi prosti brojevi. Prema tome, najveći traženi k je zaista jednak 3.

Kako je a prost, ukoliko je različit od 3 mora biti ili oblika $3m+1$ ili oblika $3m+2$ za neki nenegativan cijeli broj m. Ako je $a = 3m+1$, tada je $a + 20 = 3m + 21 = 3(m+7)$, što nije prost broj jer je djeljiv s 3. Ako je $a = 3m+2$, tada je $a + 10 = 3m + 12 = 3(m+4)$, što također nije prost broj. Prema tome, $(3, 13, 23)$ je jedini aritmetički niz duljine 3 čiji su svi članovi prosti brojevi i kojem je razlika jednaka 10.

Primjer 7. *Pokažimo da ne postoji aritmetički niz duljine veće od* 2 *čiji su svi članovi prosti brojevi te je razlika tog niza jednaka* 100.

Rješenje. Kako 100 nije djeljivo s 3, na isti način kao u rješenju prethodnog primjera vidimo da ne postoji traženi aritmetički niz duljine veće od 3. Preostaje pokazati da ne postoji niti takav niz duljine 3. Pretpostavimo da postoji takav niz duljine 3 te ga označimo s $(a, a+100, a+200)$. Ako je a oblika $3m+1$, za neki nenegativan cijeli broj m, tada je $a+200$ djeljivo s 3. Ako je a oblika $3m+2$ za neki nenegativan cijeli broj m, tada je $a+100$ djeljivo s 3. Preostaje jedino mogućnost $a = 3$, no tada $a + 2d = 203$ nije složen broj jer je $203 = 7 \cdot 29$. Prema tome, ne postoji niti niz duljine 3 s traženim svojstvom.

Literatura

[1] A. Dujella, *Number Theory*, Školska knjiga, Zagreb, 2021.

[2] B. Green, T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. 167, 2(2008), 481-547

[3] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište u Osijeku, Osijek, 2014.

[4] W. Sierpiński, *Elementary theory of numbers*, North-Holland Publishing Co., Amsterdam; PWN–Polish Scientific Publishers, Warsaw, 1988.

[5] W. Sierpiński, 250 *problems in elementary number theory*, American Elsevier Publishing Co., Inc., New York; PWN–Polish Scientific Publishers, Warsaw, 1970.

[6] E. Trost, *Primzahlen*, Verlag Birkhäuser, Basel-Stuttgart, 1953.

Ivan Matić
Fakultet primijenjene matematike i informatike, Sveučilište J.J. Strossmayera u Osijeku
E-mail adresa: imatic@mathos.hr