Predavanje 11

O PROSTIM BROJEVIMA

Skup prostih brojeva $\{2, 3, 5, 7, 11, \dots\}$ je jedan od najjednostavnije zadatih, ali istovremeno i jedan od "najmisterioznijih" skupova u matematici uopšte. Ovde polazimo najpre od njegovih svojstava koja su bila poznata antičkim matematičarima, te se pojavljuju već u Euklidovim *Elementima*.

Tvrđenje 11.1. *Skup prostih brojeva je beskonačan.*

Dokaz. Pretpostavimo suprotno: da postoji samo konačno mnogo prostih brojeva $p_1, \dots, p_k$. Posmatrajmo broj

$$A = p_1 \cdots p_k + 1.$$

Kako je $A \equiv -1 \pmod{p_i}$, sledi da $p_i \nmid A$ za sve $1 \leqslant i \leqslant k$. Međutim, po osnovnoj teoremi aritmetike, A je proizvod prostih brojeva; specijalno, A ima neki prost delilac p, koji je pri tome različit od svih brojeva $p_1, \dots, p_k$. Kontradikcija. □

Neka p_n označava n-ti po redu prost broj, $n \geqslant 1$, pri čemu je $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, itd.

Posledica 11.2.

$$p_n < 2^{2^n}.$$

Dokaz. Nejednakost dokazujemo totalnom indukcijom. Ona je očito tačna za $n = 1$. Uz pretpostavku da posmatrana nejednakost važi za sve $n \leqslant m$, dobijamo

$$\begin{aligned} p_{m+1} &\leqslant p_1 \cdots p_m + 1 < 2^{2^1} \cdots 2^{2^m} + 1 = \\ &= 2^{2^1 + \cdots + 2^m} + 1 = 2^{2^{m+1} - 2} + 1 < 2^{2^m}, \end{aligned}$$

pri čemu prva od nejednakosti u nizu sledi iz dokaza prethodnog tvrđenja. □

Eratostenovo sito. Eratostenovo sito je konceptualno jednostavan postupak (algoritam) za određivanje svih prostih brojeva ne većih od nekog zadatog broja N. Tokom njega će određeni brojevi biti *zaokruženi*, dok će neki biti *precrtani*.

(1) Ispišimo sve prirodne brojeve od 2 do N.
(2) Potražimo prvi broj sleva koji nije ni zaokružen, ni precrtan; neka je to k.
(3) Ako je $k^2 > N$, onda STOP. U suprotnom, nastavimo sa radom.
(4) Zaokružimo broj k i precrtajmo sve njegove umnoške $qk \leqslant N$, $q \geqslant 2$.
(5) Vratimo se na korak (2).

Tvrđenje 11.3. *Za svaki prirodan broj $N \geqslant 2$, skup brojeva koji su po okonačanju gornjeg algoritma zaokruženi ili neobeleženi poklapa se sa skupom prostih brojeva ne većih od N.*

Dokaz. Jasno, ako je broj $n \leqslant N$ precrtan tokom posmatranog algoritma, tada on mora biti složen, jer su svi precrtani brojevi oblika qk za neko $q, k \geqslant 2$.

Obratno, pretpostavimo da je broj $n \leqslant N$ složen; neka je $n = ab$ tako da je $a \leqslant b$. Tada je $a^2 \leqslant n$, pa n mora imati prost faktor p takav da je $p^2 \leqslant n$. Budući da je p prost, on ne može biti precrtan tokom algoritma. Međutim, očigledno je da se algoritam neće zaustaviti sve dok postoji neobeleženi broj čiji je kvadrat $\leqslant N$; pošto je $p^2 \leqslant N$, sledi da p mora biti zaokružen tokom algoritma. Ali, tada će zbog $p \mid n$ broj n biti precrtan. □

Uobičajeno je da se za (u načelu realan broj) $x > 0$ sa $\pi(x)$ označi broj svih prostih brojeva ne većih od x (tj. broj svih prostih brojeva u intervalu $[0, x]$). Fundamentalan rezultat analitičke teorije brojeva, *teorema o prostim brojevima*, daje asimptotsko ponašanje funkcije $\pi(x)$ kada $x \to \infty$; u izvesnom smislu, ova teorema opisuje "gustinu" prostih brojeva u skupu $\mathbb{N}$. Nju su 1896. nezavisno dokazali francuski matematičari de la Vallée-Poussin i Hadamard koristeći kompleksnu analizu; prvi "elementaran" dokaz (koji se oslanja samo na realnoanalitičke metode) dali su 1949. Erdős Pál i Atle Selberg.

Teorema 11.4 (Teorema o prostim brojevima)**.** *Važi $\pi(x) \sim x/\ln x$ kada $x \to \infty$; drugim rečima,*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Prema tome, verovatnoća da je slučajno izabran broj iz skupa $\{1, \ldots, N\}$ prost je (uz uniformnu raspodelu i dovoljno veliko N) približno jednaka $1/\ln N$.

Posledica 11.5. *Važi:*

$$\lim_{n\to\infty} \frac{p_n}{n \ln n} = 1.$$

Prema tome, postoje konstante $c_1, c_2 > 0$ tako da za dovoljno veliko n važi

$$c_1 n \ln n < p_n < c_2 n \ln n.$$

Međutim, iako ovi rezultati na "globalnom nivou" grubo određuju ponašanje niza prostih brojeva, "lokalno" gledajući njihova distribucija je veoma složena, tj. javljaju se razne nepravilnosti. Koliko se malo zna o tim nepravilnostima svedoči i činjenica da nije poznat odgovor čak ni na sledeće pitanje.

Problem 1 (Problem blizanaca). Dva prosta broja p i q su *blizanci* ako je $|p-q| = 2$ (na primer, to su $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$,...). Koliko ima prostih blizanaca – konačno ili beskonačno mnogo?

S druge strane, niz prostih brojeva sadrži proizvoljno velike "rupe".

Tvrđenje 11.6. *Za svaki prirodan broj $N \geqslant 1$ postoji niz od N uzastopnih prirodnih brojeva koji su svi složeni.*

Dokaz. Posmatrajmo brojeve $n+2, \ldots, n+N+1$, gde je $n = (N+1)!$. Očigledno, za sve $2 \leqslant k \leqslant N+1$ važi

$$n + k = k\left(\frac{(N+1)!}{k} + 1\right),$$

pa zaključujemo da su svi posmatrani brojevi složeni. □

Ipak, ove "rupe" stoje u vezi sa veličinom prostih brojeva između kojih se javljaju. Naime, po čuvenoj teoremi Čebiševa (poznatoj i kao *Bertranov postulat* iz vremena kada ona još nije bila dokazana), odnos dva uzastopna člana niza prostih brojeva nikada nije veći od 2 ! Prema tome, prost broj koji sledi nakon p manji je od $2p$, što znači da se ovde može realizovati "rupa" dužine najviše $p-1$.

Teorema 11.7 (Čebišev)**.** *Za svaki prirodan broj $n \geqslant 1$ postoji prost broj p tako da je*

$$n < p \leqslant 2n.$$

Problem 2. Da li za svaki prirodan broj n postoji prost broj p tako da je

$$n^2 < p < (n+1)^2 \ ?$$

Posebnu tematiku koja se tiče raspodele prostih brojeva u skupu $\mathbb{N}$ čini pitanje prisustva prostih brojeva u aritmetičkim progresijama. Jedan od centralih rezultata u tom smislu čini poznata Dirihleova teorema.

Teorema 11.8 (Dirichlet)**.** *Neka su $a > 0$ i b celi brojevi takvi da je $(a, b) = 1$. Tada (beskonačna) aritmetička progresija $ak+b$, $k = 0, 1, 2, \ldots$ sadrži beskonačno mnogo prostih brojeva.*

Mi ćemo ovde dokazati dva specijalna slučaja.

Tvrđenje 11.9. *Postoji beskonačno mnogo prostih brojeva oblika $4k + 3$.*

Dokaz. Imitiramo dokaz Tvrđenja 11.1. Pretpostavimo da postoji samo konačno mnogo prostih brojeva $p_1 = 3, \ldots, p_r$ koji daju ostatak 3 pri deljenju sa 4. Posmatrajmo tada broj

$$A = 4p_1 \cdots p_r - 1.$$

Jasno, A nije deljiv nijednim od prostih brojeva $p_1, \ldots, p_r$, kao ni sa 2. Prema tome, svi prosti faktori q_i broja $A = q_1 \cdots q_s$ su oblika $4k + 1$, odakle lako sledi da je $-1 \equiv A \equiv 1 \pmod 4$; kontradikcija. □

Tvrđenje 11.10. *Postoji beskonačno mnogo prostih brojeva oblika $4k + 1$.*

Dokaz. Pretpostavimo da postoji samo konačno mnogo prostih brojeva $p_1 = 5, \ldots, p_r$ koji daju ostatak 1 pri deljenju sa 4. Sada ćemo posmatrati broj

$$A = (2p_1 \cdots p_r)^2 + 1.$$

On nije deljiv brojevima $2, p_1, \ldots, p_r$, pa sledi da svi njegovi prosti faktori moraju biti oblika $4k + 3$. Neka je q jedan od njih. Tada na osnovu $q \mid A$ sledi

$$(2p_1 \cdots p_r)^2 \equiv -1 \pmod q.$$

Dakle, -1 je kvadratni ostatak po modulu q, što je po Tvrđenju 9.3 (iii) moguće ako i samo ako je $q \equiv 1 \pmod 4$. Kontradikcija. □

Pitanje egzistencije prostih brojeva u aritmetičkim progresijama se u izvesnom smislu može "obrnuti": da li postoje konačne aritmetičke progresije proizvoljne dužine u skupu prostih brojeva? (Veoma lako se pokazuje da ne postoji beskonačna aritmetička progresija čiji su svi članovi prosti.) Potvrdan odgovor na ovo pitanje dokazali su 2004. Ben J. Green i Terence Tao.

Teorema 11.11 (Green & Tao)**.** *Za svako $N \geqslant 1$ postoji aritmetička progresija od N članova koja se sastoji od isključivo prostih brojeva.*

Evo još nekoliko otvorenih problema vezanih za proste brojeve.

Problem 3 (Goldbahova hipoteza). Da li se svaki paran broj $\geqslant 4$ može prikazati kao zbir dva prosta broja?

Problem 4. Da li postoji beskonačno mnogo prostih brojeva oblika $k^2 + 1$?

Problem 5. Da li postoji beskonačno mnogo prostih brojeva oblika $2^k - 1$? (Mersenovi prosti brojevi)

Problem 6. Da li postoji beskonačno mnogo prostih brojeva oblika $2^k + 1$? (Fermaovi prosti brojevi)

Zanimljivo je da se i Mersenovi i Fermaovi prosti brojevi pojavljuju u različitim kontekstima u teoriji brojeva, algebri i drugim oblastima matematike. Navodimo dva primera koji ovo ilustruju.

Teorema 11.12. *Broj n je* savršen *ako je jednak zbiru svih svojih delitelja različitih od samog n. Paran broj n je savršen ako i samo ako je oblika*

$$n = 2^{p-1}(2^p - 1),$$

gde je $2^p - 1$ Mersenov prost broj.

Problem 7. Da li postoji neparan savršen broj?

Teorema 11.13 (Gauss)**.** *Neka je $N \geqslant 3$ prirodan broj. Pravilan N-tougao se može konstruisati pomoću lenjira i šestara ako i samo ako se N može prikazati kao proizvod stepena dvojke i različitih Fermaovih prostih brojeva.*