

jeva manjih od zadatog broja.

Na primer, ako želimo pronaći sve proste brojeve manje od 100, prvo ćemo ispisati spisak svih prirodnih brojeva od 1 do 100. Zatim pronalazimo prvi broj drugačiji od 1 (2) i precrtamo sve njegove sadržioce. Nakon toga, pronaći ćemo prvi broj koji nije precrtan (3), a razlikuje se od prvog broja, te precrtamo i njegove sve sadržioce. Ovaj proces ponavlja se toliko puta koliko je to moguće. Na kraju će svi brojevi koji nisu prošli kroz sito davati raspon prostih brojeva od 1 do 100. Uopšteno govoreći, za pronalazak svih prostih brojeva manjih od broja N nije potrebno vršiti ovaj dugačak proces za sve cele brojeve do N . Može se dokazati da je dovoljno prosejati cele brojeve manje ili jednake od $\sqrt{N}$. Prema našem primeru, dovoljno je prosejati brojeve manje od $\sqrt{100} = 10$.

Eratostenovo sito jedan je od efikasnijih metoda za pronalaženje malih prostih brojeva, tj. prostih brojeva manjih od deset milijardi. Naravno, ne radi se o prosejavanja pomoću papira i olovke. Budući da živimo u informatičkom dobu, imamo na raspolaganju nekoliko algoritama koji nam omogućavaju

da koristimo ovaj metod u računarskom programu takvom brzinom da nam se ne isplati čuvati dugačke liste prostih brojeva jer će program pronaći brojeve mnogo brže nego bilo koji računar koji mora da iščitava listu na hard-disku.

•Prostih brojeva je beskonačno mnogo

Postoje desetine dokaza o beskonačnosti prostih brojeva. Neki od njih su temeljno razrađeni, na primer onaj koji je 1955. godine predstavio Firstenberg uz pomoć topoloških prostora. Međutim, najelegantniji, odnosno najjednostavniji dokaz smislio je već Euklid. Glasi ovako: pretpostavimo da postoji konačan broj prostih brojeva. U tom slučaju, postojace jedan broj veći od svih ostalih, možemo ga nazvati broj P . Sada ćemo da pomnožimo sve proste brojeve do P te ćemo slovom N označiti rezultat, $N = 2 \times 3 \times 5 \times 7 \times 11 \times \dots \times P$.

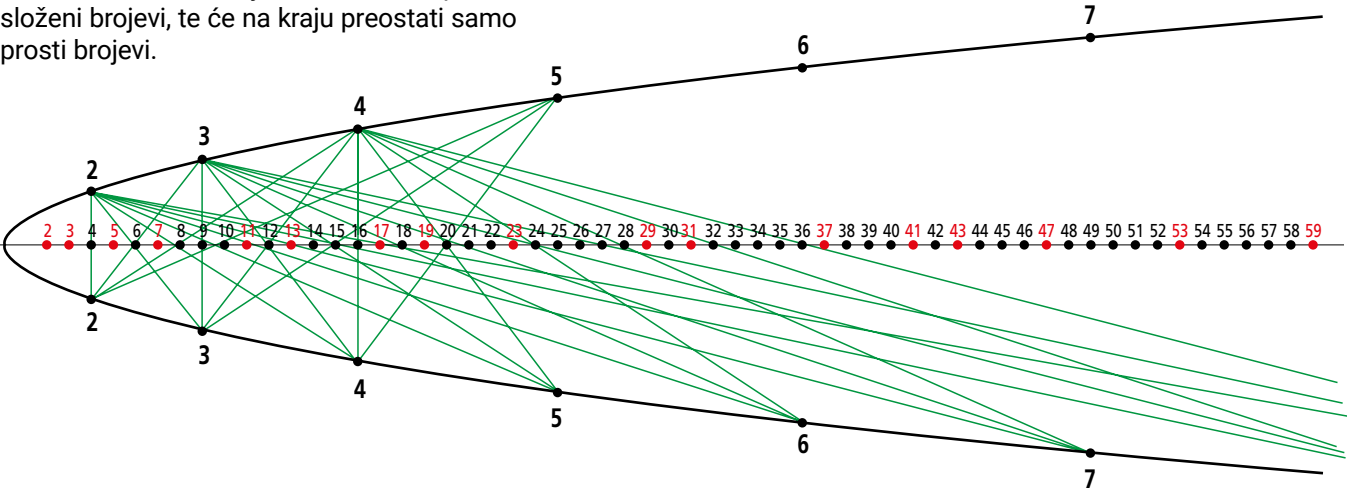
Pogledajmo šta će da se desi sa brojem $N + 1$. Očigledno je da se ovaj broj ne može deliti sa 2 zato što je reč o jednom od delilaca broja N , stoga bi ostao ostatak 1. Iz istog razloga ne može se deliti ni brojem 3, to je ponovo delilac broja N i opet bi nam ostao ostatak 1. Ovakvim rasuđivanjem dolazimo do zaključka da $N + 1$ nije deljiv nijednim prostim brojem do P . To znači ili da je sam broj prost ili da je deljiv prostim brojem većim od P . Iz toga proizlazi da je $N + 1$ prost broj pošto pretpostavljamo da ne postoje prosti brojevi

▲ I to nije sve... Eratosten je postao besmrtno ne samo zahvaljujući svojim otkrićima nego i po tome što je krater na Mesecu nazvan po njemu.



Moderno sito

Genijalni naučnici mogu da vide neobične veze između naizgled veoma različitih stvari. Šta to zajedničko mogu imati prosti brojevi i parabola? Ruski matematičari Jurij Matijasevič i Boris Stečkin otkrili su sledeće pažnje vredno svojstvo ove krive u 20. veku. Uzastopne cele brojeve moguće je obostrano prikazati na dvema granama parabole. Duž koja će spajati bilo koje dve tačke seći će Y osu parabole u tački koja tačno odgovara njihovom proizvodu. Sistematskim unošenjem duži na osu parabole eliminisaće se svi složeni brojevi, te će na kraju preostati samo prosti brojevi.



veći od P . To nije u skladu sa pretpostavkom da je P najveći prost broj. Budući da smo došli do spora, početna hipoteza je pogrešna.

•Nepredvidljivije od vremena

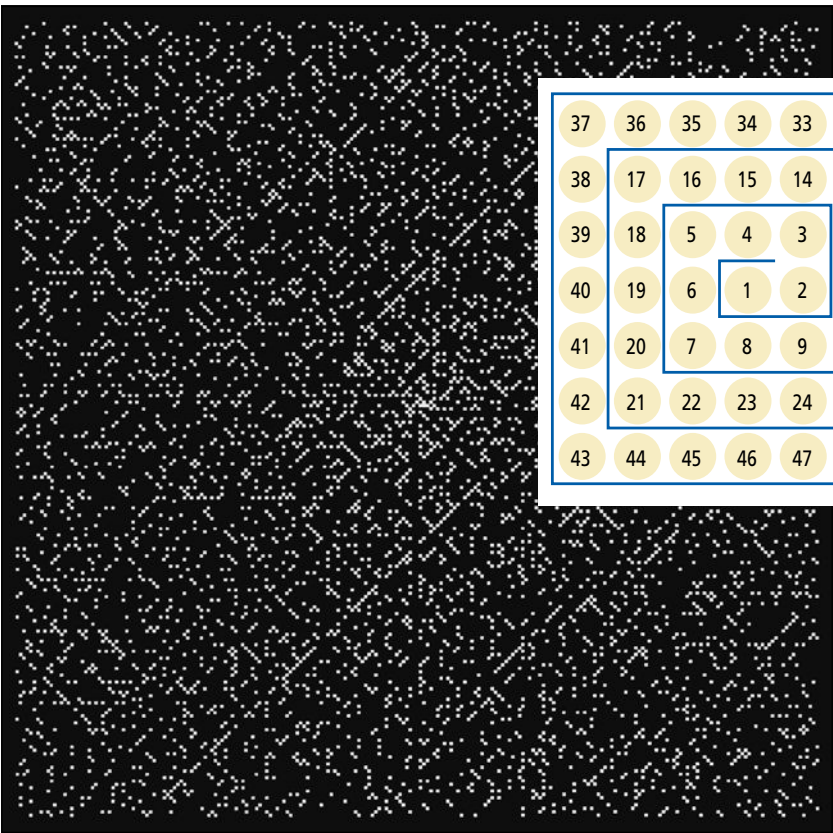
Lakše je predvideti kakvo će vreme biti negde u maloj varoši za dve godine ili koliko će se maksimalno spustiti akcijske cene, nego pretpostaviti koliko će se prostih brojeva pojaviti u nizu prirodnih brojeva. Na primer, između brojeva 1 i 100 postoji više prostih brojeva nego između brojeva 101 i 200. Međutim, između brojeva 1 i 1 000 ima 168 prostih brojeva, dok se između hiljade brojeva od 10^{100} do $10^{100} + 1 000$ nalazi samo dva prosta broja. Postoji teorema (čiju formulaciju i dokaz neki matematičari smatraju čudom), koja nam daje približnu učestalost pojave prostih brojeva među celim brojevima. Pretpostavimo da je $P(N)$ broj prostih brojeva manjih od N . Na primer, $P(8)$ je 4, zato što se ispred broja osam nalaze četiri prosta broja, a to su 2, 3, 5 i 7. Navedena teorema, koju matematičari nazivaju teoremom prostih brojeva, kaže da će se sa povećanjem N odnos $N / P(N)$ sve više približavati prirodnom logaritmu N . Ovu naizgled konfuznu rečenicu razjasnićemo na sledeći način: pretpostavimo da nas neko pita koliko mislimo da ima prostih brojeva među prvih hiljadu brojeva. Uzmimo u ruke kalkulator i sledimo sledeće korake:

- 1) unesimo broj 1 000,
- 2) pritisnimo dugme $\ln$ (logaritam),
- 3) pritisnimo dugme $1/x$,
- 4) pomnožimo rezultat sa hiljadu.

Rezultat je 144,7648270108394255037630630554, što nam govori da se između brojeva 1 i 1 000 javlja otprilike 145 prostih brojeva. Približan rezultat nije nimalo fascinant jer tih brojeva zapravo ima 168. Ali ipak, ne zaboravimo da teorema postaje preciznija sa povećanjem broja N . Tada nam omogućava da sa velikom sigurnošću možemo reći da, na primer, prvih milijardu brojeva čini samo 3,6 % prostih brojeva.

Ovaj izvanredan rezultat prvi je zabeležio nemački talenat Karl Fridrih Gaus 1792. godine,

N	P (N)	N/ln(N)
1 000	168	145
10 000	1 229	1 089
100 000	9 592	8 696
1 000 000	78 498	72 464
10 000 000	664 579	621 118
100 000 000	5 761 455	5 434 783
1 000 000 000	50 847 478	48 309 185
10 000 000 000	455 052 511	434 782 650



▲◀ O rasporedu prostih brojeva još uvek ne znamo mnogo. Godine 1963. Stanislav Ulam, američki matematičar poljskog porekla, došao je na ideju da raspodeli cele brojeve u spiralu čiji bi početak bio u sredini mreže. Tada je primetio da se

prosti brojevi ne pojavljuju baš sasvim slučajno, nego da se često formiraju u oblicima neobičnih zraka ili dijagonalnih vlakana (označeno roze bojom na slici). Sa leve strane, ove zanimljive strukture prikazane su u mreži dimenzija 399 x 399.