Prosti brojevi i testovi prostosti

Gurdon, Ana

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Ana Gurdon

Prosti brojevi i testovi prostosti

Završni rad

Osijek, 2020.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Ana Gurdon

Prosti brojevi i testovi prostosti

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2020.

Sažetak

Tema ovog rada su prosti brojevi i testovi prostosti. Rad se sastoji od tri dijela. U prvom dijelu definirat ćemo proste brojeve te navesti neka njihova svojstva. Također, upoznat ćemo se sa specijalnim brojevima vezanim uz proste brojeve. U drugom dijelu nabrojat ćemo nekoliko testova prostosti te na primjerima pokazati kako navedeni testovi funkcioniraju. U posljednjem dijelu navest ćemo nekoliko zanimljivosti vezanih uz proste brojeve i vidjet ćemo na koji se način prosti brojevi mogu vizualizirati.

Ključne riječi

prosti brojevi, Osnovni teorem aritmetike, testovi prostosti

Prime numbers and primality tests

Summary

The subject of this paper is prime numbers and primality tests. In the first part, we will define prime numbers and their properties as well as special numbers. In the second part, primality test will be defined and corresponding examples will be given. Finally, we will mention some interesting fact about prime numbers including their visualisation.

Key words

prime numbers, Fundamental theorem of arithmetic, primality tests

Sadržaj

Uvod

Teorija brojeva jedna je od središnjih i najznačajnijih grana matematike, ponekad poznata i kao kraljica matematike. Ova grana matematike proučava svojstva cijelih brojeva, djeljivost brojeva te njihovu faktorizaciju. Značajnu ulogu u teoriji brojeva imaju prosti brojevi. Sami početci prostih brojeva pripisuju se Euklidu, grčkom matematičaru koji je živio u razdoblju od 330. do 275. pr. Kr. Njegovo najznačajnije djelo su *Elementi*. Ono se sastoji od 13 knjiga (kasnije su Hipsikl i Izidor dodali još dvije knjige) te sadrži svu dotad poznatu matematiku. Knjiga VII bavi se teorijom brojeva i u njoj se nalaze 22 definicije. Među njima nalazi se prva definicija prostih brojeva koja glasi: *prost je broj onaj koji se može izmjeriti samo jedinicom*. Također, u knjizi VII mogu se pronaći još neka svojstva o prostim brojevima. Neke od njih ćemo iskazati i dokazati u ovome radu. Detaljnije o samoj povijesti prostih brojeva može se pronaći u [1].
Slike u okviru ovoga rada preuzeli smo s https://www.monticellocollege.org/author/euclid, https://hr.wikipedia.org/wiki/Pierre_de_Fermat, https://en.wikipedia.org/wiki/Ulam_spiral, https://en.wikipedia.org/wiki/Marin_Mersenne te https://commons.wikimedia.org/wiki/File:Largest_known_prime_number.svg.

Slika 1: Euklid

1 Prosti brojevi

Grčki filozofi su za proste brojeve koristili izraz *prôtos* što znači "*prvo u smislu postojanja*". Naziv prosti brojevi dolazi od latinske riječi *primus*, što znači prvi po važnosti (vidi [9]). Prema nazivu može se primijetiti da prosti brojevi imaju veliku ulogu u teoriji brojeva, ali i u samoj matematici.

1.1 Pojam prostih brojeva

Prije nego što definiramo proste brojeve, ponovit ćemo definiciju djeljivosti.

Definicija 1. *Neka su a i b cijeli brojevi, $a \neq 0$. Kažemo da je* ***b djeljiv s a****, tj. da* ***a dijeli b****, ako postoji cijeli broj d takav da je $b = a \cdot d$. Tada broj a nazivamo* ***djeliteljem*** *broja b, a broj b nazivamo* ***višekratnikom*** *broja a i pišemo $a|b$. U suprotnom, tj. ako* ***a ne dijeli b****, pišemo $a \nmid b$.*

Definicija 2. *Za prirodni broj n, $n > 1$, kažemo da je* ***prost*** *ako je djeljiv samo s 1 i sa samim sobom. Za broj koji nije prost, kažemo da je složen.*

Primjer 1. *Broj 17 je prost broj jer je djeljiv jedino s 1 i 17. Broj 22 je složen broj jer je djeljiv s 1, 2, 11 i 22.*

Promotrimo skup $\mathbb{N}_0$. Možemo primijetiti da je broj 0 djeljiv s bilo kojim prirodnim brojem jer je $0 = a \cdot 0$, $a \in \mathbb{N}$. Po dogovoru se uzima da broj 0 nije ni prost ni složen. Broj 2 je jedini paran prost broj.
Prirodni brojevi podijeljeni su u 3 klase:

- Broj 1,
- Složeni brojevi,
- Prosti brojevi.

Primjer 2. *Ako su $8p - 1$ i p prosti brojevi, pokažimo da je $8p + 1$ složen.*
Možemo primjetiti kako su $8p - 1$, $8p$ i $8p + 1$ tri uzastopna broja. Dakle, jedan od njih djeljiv je brojem 3. Znamo da je broj $8p - 1$ prost broj, pa nije djeljiv brojem 3. Imamo dva moguća slučaja:
1. slučaj: $p = 3$. U ovom slučaju je $8p + 1 = 25$, a 25 je složen broj.
2. slučaj: $8p + 1$ djeljiv je brojem 3, a prema tome i složen, čime je tvrdnja pokazana.

Definicija 3. *Neka su $b, c \in \mathbb{Z}$. Cijeli broj a koji dijeli i b i c nazivamo* ***zajednički djelitelj*** *brojeva b i c. Ako je barem jedan od brojeva b i c različit od nule, tada zajedničkih djelitelja od b i c ima konačno mnogo. Najveći među njima naziva se* ***najveći zajednički djelitelj*** *brojeva b i c koji označavamo s* ***(b, c)****.*

Definicija 4. *Neka su $a, b \in \mathbb{Z}$. Ako je $(a, b) = 1$, kažemo da su brojevi a i b* ***relativno prosti****.*

Primjer 3. *Brojevi 25 i 48 su relativno prosti jer je $(25, 48) = 1$, dok brojevi 14 i 56 nisu relativno prosti jer je $(14, 56) = 2$.*

1.2 Svojstva prostih brojeva

U ovom potpoglavlju navest ćemo neka bitnija svojstva prostih brojeva te iskazati i dokazati nekoliko teorema o istim. Među njima nalazi se jedan od najvažnijih teorema teorije brojeva, Osnovni teorem aritmetike.

Teorem 1 (vidjeti [3, Teorem 2.10.]). *Svaki prirodni broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

Dokaz: Dokaz ćemo provesti matematičkom indukcijom.

- Broj 2 je prost broj.
- Neka je $k > 2$. Pretpostavimo da se svaki prirodni broj manji ili jednak k može prikazati kao produkt prostih brojeva.
- Pokažimo da tvrdnja vrijedi i za prvih $k+1$ brojeva. U nastavku dokaza, umjesto $k+1$ pisat ćemo n. Ako je n prost broj, dokaz je gotov. U suprotnom, n je složen te vrijedi $n = k_1 \cdot k_2$, $k_1, k_2 \in \mathbb{N}$. Kako su $k_1, k_2 < n$, prema pretpostavci indukcije oni se mogu prikazati kao produkti prostih brojeva. Iz toga slijedi da se i broj n, odnosno $k+1$, može prikazati kao produkt prostih brojeva.

□

Napomena 1. *Dio teorema u zagradi odnosi se na to da se prost broj smatra umnoškom jednog prostog faktora, a složen broj produktom više prostih faktora.*

Idući teorem koristi se za dokazivanje drugih bitnih tvrdnji o prostim brojeva. Njegov dokaz izostavljamo, a isti se može pronaći u [6].

Teorem 2 (vidjeti [3, Teorem 1.2.]). *Neka su a, $b \in \mathbb{Z}$. Najmanji prirodni broj m za kojeg postoji cjelobrojno rješenje jednadžbe $ax + by = m$ je (a,b). Jednadžba $ax + by = m$ ima cjelobrojno rješenje ako i samo ako (a,b) dijeli m.*

Napomena 2. *Kao posljedicu Teorema 2 dobivamo idući rezultat: brojevi a i b relativno su prosti ako i samo ako jednadžba $ax + by = 1$ ima cjelobrojno rješenje.*

U nastavku dokazat ćemo korisnu lemu koja nam je potrebna za dokazivanje nekih drugih rezultata o prostim brojevima.

Lema 1 (vidjeti [6, Lema 1.4.1.]). *Ako je p prost broj i ako $p|ab$, tada $p|a$ ili $p|b$.*

Dokaz: Neka je p prost broj takav da $p|ab$. Bez smanjenja općenitosti, neka vrijedi $p \nmid a$. Trebamo pokazati da p dijeli broj b. Kako p ne dijeli broj a, a p je prost broj, slijedi da su a i p relativno prosti brojevi, tj. $(a, p) = 1$. Prema prethodnom teoremu, postoje cijeli brojevi x i y takvi da je $ax + py = 1$. Pomnožimo li tu jednakost s b, dobivamo $abx + pby = b$. Kako p dijeli ab, slijedi da p dijeli b, čime je dokaz gotov.

□

Slijedi općenitiji oblik prethodne leme. Dokazuje se matematičkom indukcijom, a njen dokaz može se pronaći u [6].

Lema 2 (vidjeti [6, Lema 1.4.2.]). *Ako je p prost broj i ako $p|a_1 \cdot a_2 \cdot \cdots a_n, n \in \mathbb{N}$, tada p dijeli barem jedan od faktora $a_i, i \in \{1, 2, ..., n\}$.*

Sljedeći teorem jedan je od najvažnijih teorema teorije brojeva, ali i matematike općenito. To je *Osnovni teorem aritmetike*. Njega je prvog iskazao i dokazao Gauss početkom 19. stoljeća.

Teorem 3 (Osnovni teorem aritmetike, vidjeti [6, Teorem 1.4.3.]). *Prikaz svakog prirodnog broja većeg od 1 u obliku produkta potencija prostih brojeva jedinstven je do na poredak faktora.*

Dokaz: Neka je $n > 1$ prirodni broj. Pretpostavimo da se n može prikazati kao produkt prostih faktora na dva različita načina, tj. $n = p_1 p_2 \cdots p_k$ i $n = q_1 q_2 \cdots q_l$, $k, l \in \mathbb{N}$. Tada vrijedi: $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$. Prema definiciji djeljivosti, p_1 dijeli izraz s desne strane. Prema prethodnoj lemi, dobivamo $p_1 \mid q_i$, $i \in 1, ..., l$. Kako su i p_1 i q_i prosti, slijedi $p_1 = q_i$. Promjenom redoslijeda faktora $q_1, q_2, ..., q_l$, možemo uzeti $i = 1$. Ako izraz $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$ podijelimo s p_1, dobivamo $p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l$. Ako nastavimo na isti način, dobivamo $p_2 = q_2, p_3 = q_3, ..., p_k = q_k$ i $k = l$. Time je dokazan Osnovni teorem aritmetike. □

Svaki prirodni broj n, $n > 1$, može se zapisati izrazom

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{1}$$

$k \in \mathbb{N}$, pri čemu su $p_1, p_2, ..., p_k$ međusobno različiti prosti brojevi, a $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$ potencije prostih brojeva. Izraz (1) nazivamo faktorizacija, odnosno kanonski zapis prirodnog broja n.

Primjer 4. *Broj 1260 zapisan kao produkt potencija prostih brojeva:* $1260 = 2 \cdot 2 \cdot 5 \cdot 3 \cdot 3 \cdot 7 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$.

U sljedećem primjeru lako se pokaže da se svi prosti brojevi mogu prikazati u posebnom obliku.

Primjer 5. *Svi prosti brojevi, osim 2 i 3, su oblika* $6k \pm 1, k \in \mathbb{N}$.
Svaki prirodni broj može se prikazati u jednom od sljedećih oblika:

$$6k,\ 6k+1,\ 6k+2,\ 6k+3,\ 6k+4,\ 6k+5.$$

Broj $6k$ uvijek je djeljiv sa 6, a samim time je i složen broj. Nadalje, možemo primjetiti kako su brojevi $6k+2$ i $6k+4$ parni brojevi za bilo koji $k \in \mathbb{N}$ te da je broj $6k+3$ uvijek djeljiv brojem 3. Dakle, preostaju nam oblici $6k+1$ i $6k+5$.
Ako izraz $6k+5$ zapišemo kao $6(k+1)-1 = 6t-1$ pri čemu je t također prirodni broj, tvrdnja iz primjera pokazana.

Napomena 3. *Obrat tvrdnje iz Primjera 5 ne vrijedi. Odnosno, ako je broj oblika $6k \pm 1$, taj broj ne mora biti prost. Za protuprimjer možemo uzeti broj 65. Za njega vrijedi $65 = 6 \cdot 11 - 1$, ali 65 nije prost broj.*

1.3 Skup prostih brojeva

Skup svih prostih brojeva označavamo s $\mathcal{P}$. Idući teorem govori o brojnosti toga skupa.

Teorem 4 (vidjeti [6, Teorem 1.4.5])**.** *Skup $\mathcal{P}$ je beskonačan.*

Teorem je prvi iskazao i dokazao Euklid oko 300. g. pr. Kr. u devetoj knjizi Elemenata. Postoje dva dokaza ovog teorema. Ovaj koji ćemo mi navesti je Euklidov. Drugi dokaz ovog teorema koristi metode matematičke analize i on se može pronaći u [6].

Dokaz: Pretpostavimo suprotno, tj. pretpostavimo da je skup $\mathcal{P}$ konačan. U tom slučaju skup $\mathcal{P} = \{p_1, p_2, ..., p_k\}, k \in \mathbb{N}$, sadrži sve proste brojeve.
Promotrimo broj $n = 1 + p_1 \cdot p_2 \cdot \cdots p_k$. Možemo primjetiti kako je $n > 1$ te da n nije djeljiv ni s jednim od brojeva iz skupa $\mathcal{P}$. Nadalje, $n > p_i, \forall i = 1, ..., k$. Iz toga možemo zaključiti da je n prost broj, što je u kontradikciji s pretpostavkom da je skup $\mathcal{P}$ konačan. □

1.4 Distribucija prostih brojeva

Definicija 5. *S $\pi(x)$ označavat ćemo broj prostih brojeva p takvih da je $p \leq x$.*

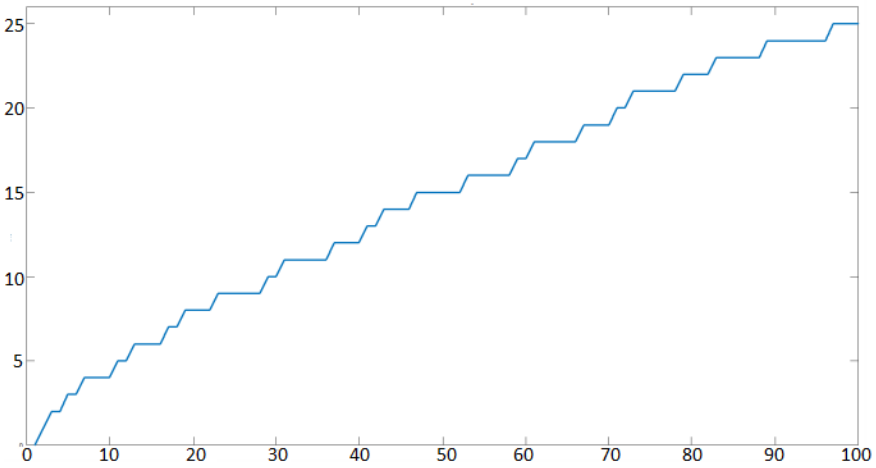
Pogledajmo kako to funkcionira na jednom jednostavnom primjeru.

Primjer 6. *Odredimo* $\pi(20)$.
Prosti brojevi koji su manji ili jednaki 20 *su:* 2, 3, 5, 7, 11, 13, 17, 19. *Prema tome je* $\pi(20) = 8$.

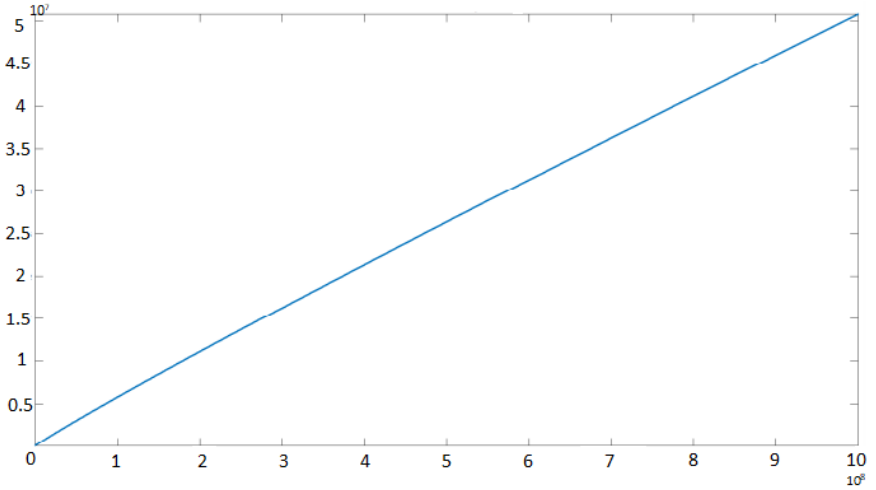
U sljedećim tablicama i grafovima možemo vidjeti kako se funkcija π ponaša za $0 \leq x \leq 100$ te $0 \leq x \leq 10^9$:

x	$\pi(x)$
10	4
20	8
30	10
40	12
50	15
60	17
70	19
80	22
90	24
100	25

x	$\pi(x)$
10	4
10^2	25
10^3	168
10^4	1229
10^5	9592
10^6	78498
10^7	664579
10^8	5761455
10^9	50847534



Slika 2: Graf funkcije π za $0 \leq x \leq 100$.



Slika 3: Graf funkcije π za $0 \leq x \leq 10^9$.

U prethodnom potpoglavlju dokazali smo da prostih brojeva ima beskonačno mnogo. Prema tome je funkcija π rastuća te vrijedi $\lim_{x\to\infty} \pi(x) = \infty$. Prema navedenim tablicama i grafovima, intuitivno možemo vidjeti da se za sve veće brojeve prosti brojevi pojavljuju sve nasumičnije. Stoga bismo voljeli preciznije opisati asimptotsko ponašanje funkcije π. O tome nam govori sljedeći teorem, koji je ujedno i osnovni rezultat o distribuciji prostih brojeva.

Teorem 5 (Teorem o prostim brojevima, vidjeti [3])**.**

$$\pi(x) \sim \frac{x}{\ln x}, \quad kada \quad x \to \infty. \tag{2}$$

Prethodni teorem možemo interpretirati kao $\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$.

Teorem je krajem 18. stoljeća postavio Gauss. Prvi su ga dokazali, neovisno jedan o drugome, Hadamard i de la Vallée-Poussin 1896. godine. Jednostavnije dokaze otkrili su Selberg, Erdős

i Newman u 20. stoljeću.
Još bolja aproksimacija za funkciju π je *logaritamsko − integralna funkcija*

$$\mathrm{li}(x) = \int_2^x \frac{1}{\ln t} dt, \quad za\ x > 0,\ x \neq 1.$$

Prema L'Hospitalovu pravilu dobivamo

$$\lim_{x\to\infty} \frac{\mathrm{li}(x)}{x/\ln(x)} = 1,$$

iz čega slijedi da je *Teorem o prostim brojevima* ekvivalentan s $\pi(x) \sim \mathrm{li}(x)$, kada $x \to \infty$ (vidjeti [10]).
U nastavku ćemo iskazati još nekoliko rezultata vezanih za distribuciju prostih brojeva. Definirajmo prije toga binomni koeficijent te iskažimo Binomni teorem.

Definicija 6. *Za svaki $n \in \mathbb{N},\ k \in \mathbb{N}_0,\ k \leq n$ definira se* ***binomni koeficijent*** *s*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k},$$

te je $\binom{n}{0} = 0,\ \forall n \in \mathbb{N}$.

Teorem 6 (Binomni teorem, vidjeti [3, Teorem 1.2.])**.** *Za $n \in \mathbb{N}$ te za sve $x,\ y \in \mathbb{C}$ vrijedi*

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + y^n.$$

Lema 3 (vidjeti [3, Lema 7.1.])**.** *Za $n \in \mathbb{N}$ vrijedi:*
(i) $2^n \leq \binom{2n}{n} < 2^{2n}$.
(ii) $\prod_{n<p\leq 2n}$ *p dijeli $\binom{2n}{n}$, gdje je p prost broj.*
(iii) Neka je $r(p) = \lfloor \log_p 2n \rfloor$. Tada $\binom{2n}{n}$ dijeli $\prod_{p\leq 2n} p^{r(p)}$.
(iv) Ako je $n > 2$ i $\frac{2n}{3} < p \leq n$, onda p ne dijeli $\binom{2n}{n}$.
(v) $\prod_{p\leq n} p < 4^n$.

Dokaz. Dokaz se može pronaći u [5]. □

Slijedi nešto slabiji rezultat od Teorema o prostim brojevima.

Teorem 7 (vidjeti [3, Teorem 7.2.])**.** *Za $n \geq 2$ vrijedi:*

$$\frac{n}{8ln\ n} < \pi(n) < \frac{6n}{ln\ n}.$$

Dokaz. Iz Leme 3 *(ii)* i *(iii)* $\prod_{n<p\leq 2n}$ p dijeli $\binom{2n}{n}$ te $\binom{2n}{n}$ dijeli $\prod_{2\leq 2n} p^{r(p)}$, iz toga slijedi

$$n^{\pi(2n)-\pi(n)} \leq \prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq \prod_{p\leq 2n} p^{r(p)} \leq (2n)^{\pi(2n)}.$$

Nadalje, iz Leme 3 (i) slijedi

$$n^{\pi(2n)-\pi(n)} < 2^{2n} \quad \text{i} \quad 2^n \leq (2n)^{\pi(2n)}. \tag{3}$$

Ako u gore dobivene nejednakosti, umjesto n uvrstimo 2^k, dobivamo

$$2^{k(\pi(2\cdot 2^k)-\pi(2^k))} < 2^{2\cdot 2^k} \quad \text{i} \quad 2^{2^k} \leq (2\cdot 2^k)^{\pi(2\cdot 2^k)}.$$

Djelovanjem funkcijom $\log_2$ koja je rastuća dobivamo

$$k(\pi(2^{k+1}) - \pi(2^k)) < 2^{k+1} \quad \text{i} \quad 2^k \leq (k+1)\pi(2^{k+1}).$$

S obzirom da je 2 jedini paran prost broj, vrijedi $\pi(2^{k+1}) \leq 2^k$ te imamo

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) < \pi(2^{k+1}) + 2^{k+1} \leq 3\cdot 2^k.$$

Ako u gornji izraz za k uvrstimo $m, m-1, ..., 1, 0$ te sve zbrojimo, dobivamo sljedeće:

$$(m+1)\pi(2^{m+1}) \leq 3(2^m + 2^{m-1} + \cdots + 2^1 + 1) < 3\cdot 2^{m+1}.$$

Iz toga i iz (3) imamo

$$\frac{2^m}{m+1} \leq \pi(2^{m+1}) < \frac{3\cdot 2^{m+1}}{m+1}. \tag{4}$$

Neka je sada $n \in \mathbb{N},\ n \leq 2$ te neka je $m = \lfloor \log_2 n \rfloor - 1$. Tada vrijedi $2^{m+1} = 2^{\lfloor \log_2 n \rfloor} \leq n < 2^{\lfloor \log_2 n \rfloor + 1} = 2^{m+2}$. Primijetimo kako za svaki $x > 0$ vrijedi $\ln 2^x = x \ln 2 < x$ i $\ln 2^x > \frac{x}{2}$. Sada iz (4) dobivamo

$$\pi(n) \leq \pi(2^{m+2}) < \frac{3\cdot 2^{m+2}}{m+2} < \frac{6\cdot 2^{m+1}}{\ln(2^{m+2})} < \frac{6n}{\ln n},$$

$$\pi(n) \geq \pi(2^{m+1}) > \frac{2^m}{m+1} = \frac{2^{m+2}}{8\cdot \frac{m+1}{2}} > \frac{2^{m+2}}{8\ln(2^{m+1}} > \frac{n}{8\ln n}$$

iz čega slijedi tvrdnja teorema. □

Idući teorem prvi je naslutio Bertrand 1845. godine. On je svoju slutnju provjerio za $n < 3\cdot 10^6$. Teorem je za sve prirodne brojeve prvi dokazao Čebišev 1852. godine.

Teorem 8 (Bertrandov postulat, vidjeti [3, Teorem 7.3])**.** *Za svaki prirodni broj n postoji prost broj p takav da je $n < p \leq 2n$.*

Dokaz. Za $n = 1, 2, 3$ dokaz je trivijalan. Tada imamo:

$$1 < 2 \leq 2, \quad 2 < 3 \leq 4, \quad 3 < 5 \leq 6.$$

Pretpostavimo da tvrdnja ne vrijedi za neki $n > 3$. Prema Lemi 3 (iv) slijedi da za sve proste faktore od $\binom{2n}{n}$ vrijedi $p \leq \frac{2n}{3}$. Neka je $p^{s(p)}$ najveća potencija od p koja dijeli $\binom{2n}{n}$. Prema Lemi 3 (iii), vrijedi $p^{s(p)} \leq p^{r(p)} \leq 2n$.

Ako je $s(p) \geq 2$, onda je $p \leq \sqrt{2n}$ te se u tom slučaju najviše $\lfloor 2n \rfloor$ prostih brojeva pojavljuje u razvoju od $\binom{2n}{n}$ s potencijom većom ili jednakom 2. Zato je

$$\binom{2n}{n} \leq (2n)^{\lfloor \sqrt{2n} \rfloor} \cdot \prod_{p \leq \frac{2n}{3}} p.$$

Među svim binomnim koeficijentima $\binom{2n}{k}$ najveći je onaj u sredini, odnosno $\binom{2n}{n}$. Iz $2^{2n} = (1+1)^{2n} = 1 + \cdots + \binom{2n}{n} + \cdots + 1 < (2n+1)\binom{2n}{n}$ slijedi $\binom{2n}{n} > \frac{4^n}{2n+1}$. Prema Lemi 3 (v), imamo

$$\frac{4^n}{2n+1} < (2n)^{\lfloor \sqrt{2n} \rfloor} \cdot \prod_{p \leq \frac{2n}{3}} p < 4^{2n/3} \cdot (2n)^{\sqrt{2n}}.$$

S obzirom da vrijedi $2n + 1 < (2n)^2$, dobivamo $4^{n/3} < (2n)^{2+\sqrt{2n}}$, tj.

$$\frac{n \ln 4}{3} < (2 + \sqrt{2n}) \ln 2n.$$

Promotrimo sada funkciju $f(x) = \frac{x \ln 4}{3} - (2 + \sqrt{2x}) \ln 2x$.
Vrijedi

$$f'(x) = \frac{\ln 4}{3} - \frac{\ln 2x}{\sqrt{2x}} - \frac{2 + \sqrt{2x}}{x}.$$

Može se provjeriti da je $f'(x) > 0$ za $x \geq 200$. Također vrijedi i $f(507) > 0$. Prema tome vrijedi $f(x) > 0, \forall x > 507$. Iz toga zaključujemo da je funkcija f za dovoljno velike x-ove rastuća i pozitivna. Time je dokaz gotov za $n \geq 507$.
Preostaje nam dokazati tvrdnju za $n < 507$. To direktno proizlazi iz činjenice da je u sljedećem nizu prostih brojeva

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631$$

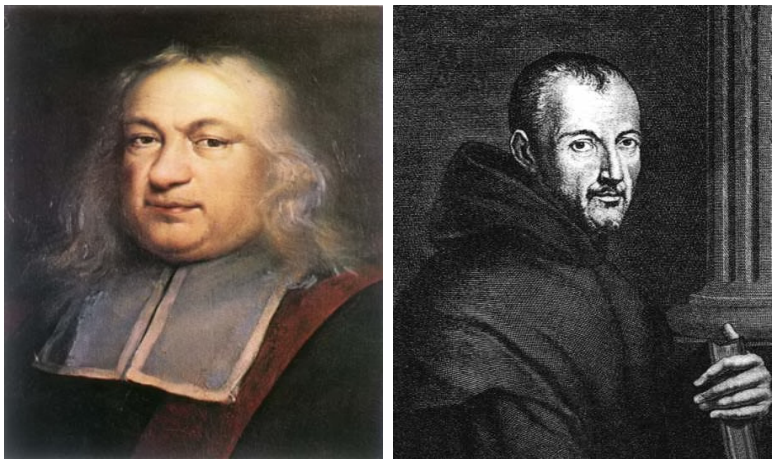
svaki član manji od dvostrukog prethodnog člana. □

1.5 Specijalni brojevi

U teoriji brojeva postoje mnogi specijalni brojevi. U ovom potpoglavlju upoznat ćemo se s dvije vrste specijalnih brojeva koje su povezane s prostim brojevima. To su Fermatovi i Mersennovi brojevi.

1.5.1 Fermatovi brojevi

Fermatovi brojevi su oblika $F_n = 2^{2^n} + 1$, gdje je n nenegativan cijeli broj. Ime su dobili po francuskom matematičaru Pierre de Fermatu iz 17. stoljeća. Fermat je smatrao da su svi brojevi tog oblika prosti. Leonhard Euler je dokazao da je $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$ složen, te na taj način opovrgnuo Fermatovu tvrdnju o prostosti brojeva tog oblika. Do danas nije poznat niti jedan prost broj oblika $2^{2^n} + 1$, za $n > 4$. U teoriji brojeva postoje neka otvorena pitanja vezana uz Fermatove brojeve kao što je i pitanje je li F_4 najveći prost Fermatov broj.



Slika 4: Fermat i Mersenne

1.5.2 Mersenneovi brojevi

Brojevi oblika, $M_n = 2^n - 1$ gdje je n prirodni broj nazivaju se Mersenneovi brojevi. Nazvani su po Marinu Mersenneu, francuskom matematičaru i fizičaru koji je živio u 17. stoljeću. Među Mersenneovim brojevima ima i prostih i složenih brojeva. Prosti brojevi oblika $2^n - 1$ nazivaju se Mersenneovi prosti brojevi. Do danas nije dokazana tvrdnja da postoji beskonačno mnogo prostih Mersenneovih brojeva.

Propozicija 1 (Cataldi-Fermat, vidjeti [6, Propozicija 1.4.8.]). *Ako je M_n prost broj, tada je i n prost broj.*

Dokaz: Općenito vrijedi $x^n - 1 = (x-1)(x^{n-1} + \cdots x + 1),\ n \in \mathbb{N}$.
Pretpostavimo da je $n \in \mathbb{N}$ složen broj pa postoje prirodni brojevi r i s veći od 1 takvi da je $n = rs$. Tada vrijedi $M_n = 2^n - 1 = 2^{rs} - 1 = (2^s - 1)(2^{s(r-1)} + \cdots + x^s + 1)$ iz čega slijedi da $2^s - 1$ dijeli M_n, odnosno da je M_n složen. □

Prije sljedećeg teorema ponovit ćemo nekoliko pojmova koji su nam potrebni za njegov iskaz. Neka je $n \in \mathbb{N}$:

- $\sigma(n)$ označava sumu svih pozitivnih djelitelja broja n,
- $\tau(n)$ je oznaka za broj svih pozitivnih djelitelja od n.

Definicija 7. *Za prirodan broj n kažemo da je **savršen** ako je $\sigma(n) = 2n$.*

Karakterizacija nekih prirodnih brojeva u obliku savršenih navedena je u sljedećem teoremu.

Teorem 9 (vidjeti [6, Teorem 1.4.7.]). *Paran prirodan broj n je savršen ako i samo ako se može prikazati u obliku*

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

gdje je broj $2^k - 1$ prost.

Dokaz. Dokaz se može pronaći u [6]. □

Primjer 7. *Provjerimo jesu li brojevi 60 i 28 savršeni.*

- *n=60, pozitivni djelitelji broja 60 su: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60*

$$\sigma(60) = 168,\ \tau(60) = 12\ ,\ \sigma(60) \neq 2 \cdot 60 \Rightarrow \textit{broj 60 nije savršen.}$$

- *n= 28, pozitivni djelitelji broja 28 su: 1, 2,4, 7, 14, 28*

$$\sigma(28) = 56,\ \tau(28) = 6,\ \sigma(28) = 2 \cdot 28 \Rightarrow \textit{broj 28 je savršen.}$$

2 Testovi prostosti

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Njen glavni cilj je omogućiti dvjema osobama (pošiljalac i primalac) sigurnu komunikaciju, tako da treća osoba (protivnik) ne može razumjeti njihove poruke. U kriptografiji veliku ulogu imaju upravo prosti brojevi te je u kriptografiji javnog ključa važno odrediti je li prirodan broj složen ili prost. Više o samoj kriptografiji možemo pronaći u [4] i [5].
Sada ćemo navesti osnovne pojmove i rezultate koji se najčešće koriste u kriptografiji a važni su i u samim testovima prostosti.

Definicija 8. *Neka je $n \in \mathbb{N}$ i $a, b \in \mathbb{Z}$. Ako n dijeli razliku $a-b$, kažemo da je a kongruentan b modulo n, ili da su a i b kongruentni modulo n. To pišemo $a \equiv b (mod\ n)$.*

Teorem 10 (Wilson, vidjeti [3, Teorem 3.13.])**.** *Ako je p prost broj, tada je $(p-1)! \equiv -1 (mod\ p)$.*

Dokaz. Za $p = 2$ i $p = 3$ imamo: $1! \equiv -1 (\text{mod } 1)$ i $2! \equiv -1 (\text{mod } 3)$.
Pretpostavimo da je $p > 3$. Grupirajmo članove skupa $\{2, 3, ..., p-2\}$ u parove (i, j) za koje vrijedi $i \cdot j \equiv (\text{mod } p)$. Očito je $i \neq j$ jer bi u suprotnom $p|(i^2 - 1)$, tj. broj $(i-1)(i+1)$ bi bio djeljiv s p, što je nemoguće zbog $0 < i - 1 < i + 1 < p$. Takvih parova ima $\frac{p-3}{2}$ i ako pomnožimo odgovarajućih $\frac{p-3}{2}$ kongruencija dobivamo

$$2 \cdot 3 \cdot ... \cdot (p-2) \equiv 1 (\text{mod } p),$$

pa je

$$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 (\text{mod } p).$$

□

Primjer 8. *Odredimo ostatak pri djeljenju broja* 15! *sa 17.*
S obzirom da je 17 prost broj, prema Wilsonovom teoremu vrijedi:

$$\begin{aligned} 16! &\equiv -1 (\text{mod } 17) \\ 16 \cdot 15! &\equiv -1 (mod\ 17) \\ -1 \cdot 15! &\equiv -1 (\text{mod } 17) \\ 15! &\equiv 1 (\text{mod } 17) \end{aligned}$$

Dakle, ostatak pri djeljenju broja 15! sa 17 je 1.

Iako se pretpostavlja da je teorem otkrio Ibn al-Hayhama još u 10. stoljeću, on se pripisuje Johnu Wilsonu u 18. stoljeću. Po njemu je teorem i dobio ime. Teorem je prvi dokazao Lagrange 1770. godine. Vrijedi i obrat Wilsonovog teorema:

Propozicija 2 (vidjeti [6, Propozicija 2.3.2.])**.** *Ako za prirodni broj n vrijedi $(n-1)! \equiv -1 (\text{mod } n)$ tada je n prost.*

Dokaz. Neka vrijedi $(n-1)! \equiv -1 (\text{mod } n)$ te pretpostavimo da je n složen broj. Tada postoji prirodan broj m, $1 < m < n$, koji dijeli n. Iz $(n-1)! \equiv -1 (\text{mod } n)$ slijedi $(n-1)! \equiv -1 (\text{mod } m)$. Kako je $m < n$, slijedi $m|(n-1)!$. Prema tome vrijedi i $m| - 1$, čime dolazimo do kontradikcije. Dakle, n je prost broj. □

Primjerice, jer je $(11-1)! \equiv 10! \equiv -1 (\text{mod } 11)$ znamo da je 11 prost broj.
Wilsonov teorem daje karakterizaciju prostih brojeva te može poslužiti kao svojevrsni test je li zadani prirodni broj prost ili nije. Međutim, za velike brojeve teško je računati faktorijele te nam Wilsonov teorem nije jednostavan za provjeru.
Zbog navedenog nedostatka, potrebni su nam drugačiji testovi prostosti kako bismo mogli odrediti je li zadani prirodni broj prost ili složen. Testove prostosti možemo definirati kao kriterije koje prirodan broj p mora zadovoljiti da bismo mogli zaključiti da je p prost. U suprotnom, tj. ako p ne zadovolji sve kriterije, zaključujemo da je p složen. Za velike prirodne brojeve p teško je odrediti je li taj broj sigurno prost. Zbog toga, testovima prostosti često provjeravamo je li broj p "vjerojatno prost". Test prostosti može nam dati samo pozitivan ili negativan odgovor. Ako je odgovor pozitivan, broj p je vjerojatno prost. Ako nam test prostosti da negativan odgovor, p sigurno nije prost broj.
Probno (pokusno) dijeljenje (eng. *trial division*) je najjednostavniji test prostosti. Ovaj test prvi je opisao Fibonacci u knjizi Liber Abaci u 13. stoljeću. Provjeravamo je li zadani broj p djeljiv s nekim od prostih brojeva koji su manji ili jednaki od $\sqrt{p}$. Ako ne postoji ni jedan prost broj manji ili jednak od $\sqrt{p}$ koji dijeli p, onda je p prost. U suprotnom je p složen broj. Pogledajmo na jednostavnom primjeru kako funkcionira opisani test.

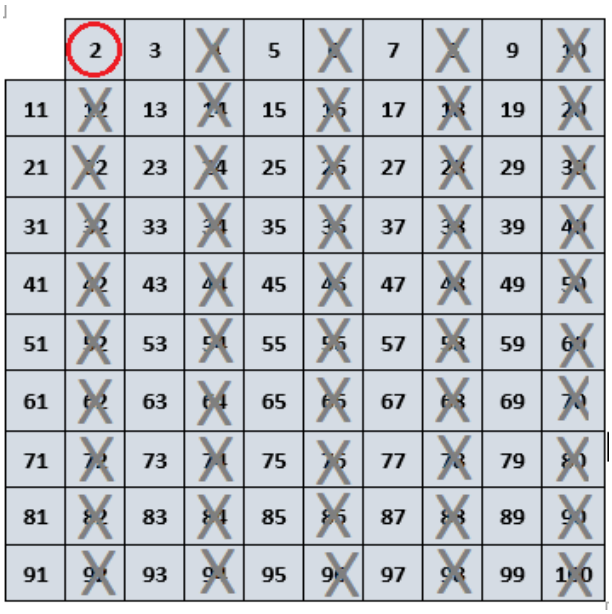
Primjer 9. *Koristeći probno dijeljenje, provjerimo je li broj* 223 *prost.*
Vrijedi $\sqrt{223} \approx 14.93$. *Lako se provjeri da ni jedan* $n \in \mathbb{N}$, $2 \leq n \leq 14$ *ne dijeli 223. Prema tome,* 223 *je prost broj.*

Iako je ova metoda neefikasna za velike n-ove, koristi se u kombinacijama s boljim metodama faktorizacije. Prethodno opisana metoda naziva se i naivna metoda faktorizacije prirodnog broja n.

2.1 Eratostenovo sito

Eratostenovo sito je postupak određivanja svih prostih brojeva koji su manji ili jednaki od zadanog prirodnog broja n. Postupak dobivanja svih prostih brojeva pomoću Eratostenovog sita prikazat ćemo na primjeru:

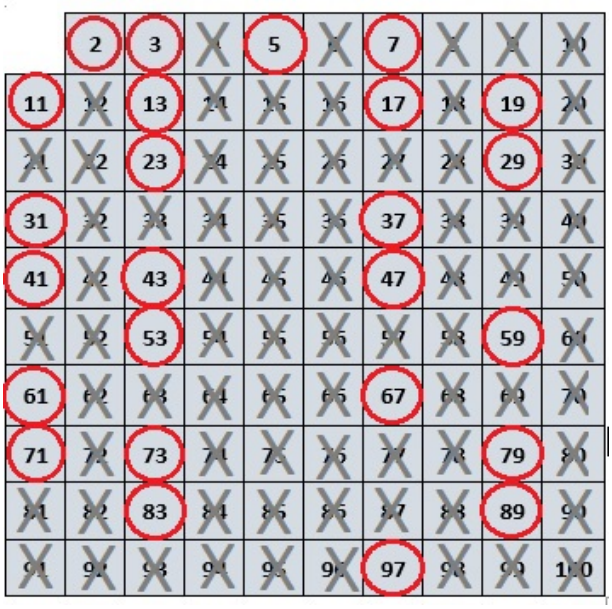
Primjer 10. *Odredimo sve proste brojeve koji su manji od 100.*
1. Ispišimo sve brojeve od 2 do 100.
2. Zaokružimo broj 2 te prekrižimo sve brojeve koji su djeljivi s 2, odnosno sve parne brojeve:



3. Zaokružimo broj 3 te prekrižimo sve brojeve koji su djeljivi s brojem 3.

4. Zaokružimo sljedeći neoznačeni broj nakon broja 3 (broj 5), a zatim prekrižimo sve neoznačene višekratnike broja 5.

5. Postupak nastavljamo dok svi brojevi ne budu označeni (prekriženi ili zaokruženi):



Svi zaokruženi brojevi su prosti, a prekriženi su složeni brojevi.
Dakle, prosti brojevi manji od 100 su: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

2.2 Fermatov test prostosti

U ovom potpoglavlju iskazat ćemo teorem koji je osnova većine testova prostosti. Neke od tih testova objasnit ćemo u nastavku ovoga rada.

Teorem 11 (Mali Fermatov teorem, vidjeti [3, Teorem 3.10.]). *Neka je p prost broj i $a \in \mathbb{Z}$. Tada je $a^p \equiv a(mod\ p)$ te ako p ne dijeli a, vrijedi i $a^{p-1} \equiv 1(mod\ p)$. Općenito, za svaki $a \in \mathbb{Z}$ vrijedi $a^p \equiv a(mod\ p)$.*

Dokaz. Dokaz se može pronaći u [3]. □

ALGORITAM ZA FERMATOV TEST PROSTOSTI:
ULAZ: neparan broj n $\geq$ 3, k (parametar koji označava broj ponavljanja)
IZLAZ: odgovor "vjerojatno prost" ili "složen"
1. Za i od 1 do k radi:
   1.1. Slučajno odaberi broj a, $2 \leq a \leq n-2$.
   1.2. Izračunaj $b = a^{n-1}(\text{mod } n)$.
   1.3. Ako je $b \neq 1$, vrati: "složen".
2. Vrati: "vjerojatno prost".

Potencije je lakše izračunati nego faktorijele iz Wilsonovog teorema, no možemo primijetiti da postoje i složeni brojevi koji zadovoljavaju izraz iz Malog Fermatovog teorema. Primjerice, za $a = 2$, broj 6 zadovoljava kongruenciju iz Teorema 12. Prema tome, ovim teoremom nije dana karakterizacija prostih brojeva. Iako pomoću Malog Fermatovog teorema ne možemo sa sigurnošću odrediti je li dani broj prost, pomoću njegovog obrata možemo odrediti je li broj složen. Odnosno, ako postoji $a \in \mathbb{N}$, $a < n-1$ takav da a^{n-1} nije kongruentan 1 modulo n, tada je n sigurno složen. Na primjer, za $a = 24$ i $n = 221$ vrijedi $24^{220} \equiv 81 \not\equiv 1(\text{mod } 221)$, prema tome je 221 složen broj.

Definicija 9. *Ako je n neparan složen broj i $a \in \mathbb{Z}$ za koji vrijedi $(n, a) = 1$ i $a^{n-1} \equiv 1(mod\ n)$, kažemo da je n pseudoprost u bazi a. Kraće pišemo n je psp(a).*

U antičkoj Kini smatrali su da je prirodan broj n prost ako i samo ako vrijedi $2^{n-1} \equiv 1(\text{mod } n)$. Ta tvrdnja opovrgnuta je 1819. godine. Primjerice, za broj 341 vrijedi $2^{340} \equiv 1(\text{mod } 341)$, odnosno zadovoljava kongruenciju $2^{n-1} \equiv 1(\text{mod } n)$, a znamo da je $341 = 11 \cdot 31$ složen broj.

Idući teorem govori o brojnosti pseudoprostih brojeva u bazi a. Iako su takvi brojevi rijetki, ima ih beskonačno mnogo.

Teorem 12 (vidjeti [4, Teorem 5.14.]). *Postoji beskonačno mnogo prirodnih brojeva koji su pseudoprosti u bazi a, $a \geq 2$.*

Dokaz. Neka je p neparan prost broj, takav da p ne dijeli $a^2 - 1$. Promotrimo broj $n = \frac{a^{2p}-1}{a^2-1}$. Iz

$$n = \frac{a^p-1}{a-1} \cdot \frac{a^p+1}{a+1}$$

zaključujemo da je n složen broj.
Iz Malog Fermatovog teorema slijedi $a^{2p} \equiv a^2(\text{mod } p)$, tj. p dijeli $a^{2p} - a^2$. Vrijedi $a^{2p} - a^2 = a^{2p} - a^2 - 1 + 1 = (a^{2p} - a^2 - 1 + 1) \cdot \frac{a^2-1}{a^2-1} = \frac{a^{2p}-1+1-a^2}{a^2-1} \cdot (a^2 - 1) = (\frac{a^{2p}-1}{a^2-1} - \frac{a^2-1}{a^2-1}) \cdot (a^2 - 1) =$

$(n-1)(a^2-1)$. Kako $p \nmid a^2-1$, slijedi $p|n-1$. Nadalje, $n-1 = a^{2p-2} + a^{2p-4} + \cdots + a^2$ je suma od $p-1$ pribrojnika iste parnosti, iz čega slijedi da je $n-1$ paran broj. Dakle, $2p$ dijeli $n-1$. Kako n dijeli $a^{2p}-1$, slijedi da n mora dijeliti i $a^{n-1}-1$. Stoga je $a^n \equiv a(\text{mod } n)$. □

Primjer 11. *Provjerimo je li broj 91 psp(2) i psp(3).*
Vrijedi:

$$3^{90} \equiv (3^6)^{15} \equiv 1(\text{mod } 91) \qquad i \qquad 2^{90} \equiv (2^{12})^7 \cdot 2^6 \equiv 64(\text{mod } 91).$$

Iz toga slijedi da je 91 pseudoprost u bazi 3, dok u bazi 2 nije.

Iz prethodnog primjera možemo zaključiti kako testiranjem sa samo jednom bazom ne možemo zaključiti da je broj prost. Zbog toga definiramo Carmichaelove brojeve:

Definicija 10. *Carmichaelov broj je složen broj n koji je pseudoprost u svakoj bazi.*

Njihovo postojanje utvrdio je R. D. Carmiachel 1912. i pretpostavio da takvih brojeva ima beskonačno mnogo. Tu tvrdnju dokazali su Alford, Granville i Pomerance 1992. godine. Svi Carmichaelovi brojevi su neparni te je svaki Carmichaelov broj produkt najmanje tri različita prosta broja. Dokazi ovih tvrdnji mogu se pronaći u [6] i [5].
Najmanji Carmichaelov broj je 561 ($561 = 3 \cdot 11 \cdot 17$).
Idući teorem daje nam vrlo jednostavan kriterij za provjeru je li prirodni broj n Carmichaelov.

Teorem 13 (Korseltov kriterij, vidjeti [6, Teorem 2.4.5])**.** *Prirodni broj n je Carmichaelov ako i samo ako je n kvadratno slobodan te za svaki prost broj p koji dijeli n vrijedi i da $p-1$ dijeli $n-1$.*

Dokaz. Dokaz se može pronaći u [6]. □

Napomena 4. *Broj $n \in \mathbb{N}$ je kvadratno slobodan ako je broj 1 najveći potpuni kvadrat koji ga dijeli, odnosno ako iz $m^2|n$, $m \in \mathbb{N}$, slijedi da je $m = 1$.*

Primjer 12. *Broj 29341 je Carmichaelov broj jer je $n = 29341 = 13 \cdot 37 \cdot 61$ te je broj $n-1 = 29340$ djeljiv s $12, 36$ i 60.*

2.3 Solovay - Strassenov test prostosti

U ovom potpoglavlju upoznat ćemo se s Eulerovim pseudoprostim brojevima te sa Solovay - Strassenovim testom prostosti koji se temelji upravo na tim brojevima.

Definicija 11. *Ako je n neparan složen broj i a cijeli broj takav da su n i a relativno prosti te ako vrijedi $a^{(n-1)/2} \equiv (\frac{a}{n})(mod\ n)$, tada n nazivamo Eulerov pseudoprost broj u bazi a.*

Primjerice, prvi Eulerov pseudoprost broj u bazi 2 je broj 341.

Napomena 5. *$(\frac{a}{n})$ je oznaka za Jacobijev simbol. Njegova definicija može se pronaći u [6].*

Napomena 6. *Ako je n Eulerov pseudoprost broj u bazi a, onda je i pseudoprost broj u bazi a. Obrat ne vrijedi (vidi [5]).*

Neka je n prirodni broj za koji želimo znati je li prost ili složen. Na slučajan način odaberemo $a,\ 0 < a < n$. Za svaki a izračunamo $a^{(n-1)/2}$, te $(\frac{a}{n})(\text{mod } n)$. Ukoliko dobiveni brojevi nisu kongruentni modulo n, zaključujemo da je broj n složen te zaustavljamo test. U suprotnom, testiramo za drugu bazu a. Ako kongruencija iz definicije Eulerovih pseudoprostih brojeva u bazi a vrijedi za k slučajno odabranih baza a, onda je vjerojatnost da je n složen, unatoč prolasku svih testova, manja ili jednaka $\frac{1}{2^k}$.

ALGORITAM ZA SOLOVAY - STRASSENOV TEST PROSTOSTI:
ULAZ: n, k (parametar koji određuje točnost testa)
IZLAZ: odgovor "složen" ili "vjerojajatno prost"
1. Za i od 1 do k radi:
   1.1. Slučajno odaberi $a,\ 0 < a < n$.
   1.2. Ako je $a^{(n-1)/2} \not\equiv (\frac{a}{n})(mod\ n)$, vrati: "složen".
2. Vrati: "vjerojatno prost".

Primjer 13. *Pokažimo da je broj $n = 91$ Eulerov pseudoprost broj u bazi 9. 91 je složen broj, $n = 91 = 7 \cdot 13$. S obzirom da vrijedi*

$$(\tfrac{91}{1}) = 1 \quad i \quad 9^{(n-1)/2} = 9^{45} \equiv (9^3)^{15} \equiv 1(\text{mod } n)$$

zaključujemo da je 91 Eulerov pseudoprost broj za bazu 9.

2.4 Miller - Rabinov test

U ovom potpoglavlju ćemo opisati Miller - Rabinov test kojemu je osnova uzastopno slučajno biranje baze za testiranje prostosti. Test se temelji na jakim pseudoprostim brojevima koje ćemo u nastavku definirati.

Definicija 12. *Neka je n neparan složen broj i neka je $n-1 = 2^t \cdot m$, pri čemu je m neparan i $t \in \mathbb{N}$. Ako za $a \in \mathbb{Z}$ vrijedi*

$$a^m \equiv 1(mod\ n)\ ili\ postoji\ r < t\ takav\ da\ je\ a^{2r \cdot m} \equiv -1(mod\ n), \tag{5}$$

onda kažemo da je n jak presudoprost broj u bazi a.

Primjerice, 121 je jak pseudoprost broj u bazi 3, jer vrijedi $120 = 2^3 \cdot 15$ te $3^{15} \equiv 1(\text{mod } n)$.

Napomena 7. *Ako je broj jak pseudoprost broj u bazi a, onda je on i Eulerov pseudoprost broj u bazi a. Obrat tvrdnje ne vrijedi.*

Ponekad se u literaturi Miller - Rabinov test naziva i Miller - Selfridge - Rabinov (MSR) test prostosti. Opisat ćemo ga u nastavku.
Neka je $n \in \mathbb{N}$ prirodni broj za koji želimo odrediti je li prost ili složen. Neka je $n-1 = 2^t m$, gdje je $m \in \mathbb{N}$ neparan i $t \in \mathbb{N}$. Na slučajan način odaberemo broj a takav da je $2 \leq a \leq n-2$ te izračunamo $a^m \text{mod } n$. Ako dobijemo ± 1, zaključujemo da je n prošao test (5) te biramo

sljedeći broj a. U suprotno, kvadriramo a^m mod n sve dok ne dobijemo -1. Ako dobijemo -1, onda kažemo da je n prošao test (5). Ako nikada ne dobijemo -1, odnosno $a^{2^{r+1}m} \equiv 1 (\text{mod } n)$, ali $a^{2^r m} \not\equiv -1 (\text{mod } n)$, onda zaključujemo da je n sigurno složen. Ako n prođe test (5) za k različitih a-ova, onda je vjerojatnost da je n složen manja ili jednaka $\frac{1}{4^k}$. Kada za neki a, $0 < a < n$, uvjet (5) nije ispunjen, broj n je složen te u tom slučaju broj a nazivamo svjedokom složenosti od n.

ALGORITAM ZA MILLER-RABINOV TEST PROSTOSTI:
ULAZ: neparan broj n $\geq$3, parametar k
IZLAZ: odgovor "složen" ili "vjerojatno prost"
1. Zapišimo n u obliku $n = 2^t m + 1$, m neparan broj.
2. Slučajno odaberi a, $2 \leq a \leq n-2$.
3. Ako je $a^m \text{mod } n = 1$ *ili* -1 vrati: "vjerojatno prost".
4. Za j od 1 do $k-1$ radi:
   4.1. Ako je $a^{2^j} \text{mod } n = -1$ vrati: "vjerojatno prost".
   4.2. Ako je $a^{2^j} \text{mod } n = 1$ vrati: "složen".
5. Vrati: "složen".

Primjer 14. *Koristeći Miller - Rabinov test prostosti, pokažimo da je broj* 577757 *vjerojatno prost te da je broj* 252601 *složen.*

- $n = 577757$, $n - 1 = 2^2 \cdot 144439$.
  Izaberimo $a = 314997 (\text{mod } n)$.

$$\begin{aligned} a^{144439} &\equiv 373220 (\text{mod } n) \\ a^{2 \cdot 144439} &\equiv 577756 \equiv -1 (\text{mod } n). \end{aligned}$$

  Prema Miller - Rabinovom testu, broj $n = 577757$ *vjerojatno je prost.*

- $n = 252601$, $n - 1 = 2^3 \cdot 31575$.
  Izaberimo $a = 85132$.

$$\begin{aligned} a^{31575} &\equiv 191102 (\text{mod } n) \\ a^{2 \cdot 31575} &\equiv 184829 (\text{mod } n) \\ a^{2^2 \cdot 31575} &\equiv 1 (\text{mod } n). \end{aligned}$$

  Prema Miller - Rabinovom testu, broj $n = 252601$ *je složen te je broj* 85132 *svjedok složenosti.*

2.5 Dokazivanje prostosti pomoću eliptičkih krivulja

U do sada opisanim testovima prostosti smo testirali je li dani prirodni broj "vjerojatno prost" ili je složen. Na osnovi tih testova ne možemo sa sigurnošću tvrditi da je dani broj prost. U ovom potpoglavlju bavit ćemo se metodama kojima se može dokazati da je broj sigurno prost.

Prije idućeg teorema definirat ćemo red od a modulo n, jer ćemo taj pojam koristiti u dokazu.

Definicija 13. *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodni broj d sa svojstvom da je $a^d \equiv 1 (mod\ n)$ nazia se* **red od** a **modulo** n**.**

Teorem 14 (Pocklington, vidjeti [7, Theorem 5.1])**.** *Neka je $n \in \mathbb{N}$. Neka je s djelitelj od $n-1$ takav da je s veći od $\sqrt{n}$. Ako postoji prirodan broj a takav da vrijedi*

$$a^{n-1} \equiv 1 (mod\ n) \tag{6}$$

$$(a^{\frac{n-1}{q}} - 1, n) = 1, \text{ za svaki prosti djelitelj } q \text{ od } s, \tag{7}$$

onda je n prost broj.

Dokaz. Ako je n složen broj, prema već objašnjenom probnom dijeljenju, postoji prost broj p, $p \leq \sqrt{n}$ koji dijeli n. Stavimo $b^s = a^{(n-1)/2}$. Tada vrijedi

$$b^s \equiv a^{n-1} \equiv 1 (\text{mod } n),$$

iz čega slijedi $b^s \equiv 1 (\text{mod } p)$. Tvrdimo da je s red od b modulo p. Pretpostavimo da za neki djelitelj q od s vrijedi $b^{s/q} \equiv 1 (\text{mod } p)$. U tom slučaju bi p dijeli n i $b^{s/q} - 1$, odnosno $a^{(n-1)/q} - 1$, što je u kontradikciji sa (7). Prema Malom Fermatovom teoremu vrijedi $b^{p-1} \equiv 1 (\text{mod } p)$. Iz toga zaključujemo da s dijeli $p-1$, što nije moguće jer je $s > \sqrt{n}$, a $p \leq \sqrt{n}$. Dakle, n je prost broj. □

Primjer 15. *Koristeći Pocklingtonov teorem, dokažimo da je broj $n = 67$ prost.*
Vrijedi $n - 1 = 66 = 2 \cdot 3 \cdot 11$. Uzmimo $s = 3 \cdot 11$ ($s = 33 > \sqrt{n} = \sqrt{67} \approx 8.19$). Prosti djelitelji od s su 3 i 11. Neka je $a = 2$. Tada vrijedi

$$2^{n-1} \equiv 2^{66} \equiv 1 (\text{mod } 67)$$

te

$$\begin{aligned} (2^{(n-1)/3} - 1, n) = (2^{22} - 1, 67) &= 1, \\ (2^{(n-1)/11} - 1, n) = (2^6 - 1, 67) &= 1, \end{aligned}$$

iz čega slijedi da je 67 prost.

Na temelju ovog primjera, možemo zaključiti da za primjenu Pocklingtonovog teorema za testiranje prostosti potrebno je poznavati barem djelomičnu faktorizaciju broja $n-1$, što u slučaju velikih brojeva može biti problem.
Iako ova metoda nije praktična za testiranje prostosti svih prirodnih brojeva, ona se koristi za testiranje prostosti brojeva specijalnog oblika.

Definicija 14. *Prothov broj je broj oblika* $n = k \cdot 2^l + 1$, *gdje je* $k \in \mathbb{Z}$ *neparan,* $l \in \mathbb{N}_0$ *i* $2^l > k$.

U nastavku ćemo vidjeti na koji način se može testirati prostost Prothovih brojeva.

Teorem 15 (Proth, vidjeti [4, Teorem 5.19.])**.** *Neka je* $l \geq 2, k \geq 1$, *takav da* $3 \nmid k$ *te* $k \leq 2^l + 1$. *Tada je prirodan broj* n, *oblika* $n = k \cdot 2^l + 1$ *prost ako i samo ako je* $3^{k \cdot 2^{l-1}} \equiv -1 (mod\ n)$.

Dokaz. Dokaz se može pronaći u [5]. □

Primjer 16. *Pokažimo da je broj* $n = 41$ *prost.*
Iz $41 = 5 \cdot 2^3 + 1$ *slijedi da je* $k = 5$ *i* $l = 3$. *Vrijedi* $3^{k \cdot 2^{3-1}} = 3486784401 \equiv -1 (mod\ 41)$.
Prema prethodnom teoremu zaključujemo da je $n = 41$ *prost broj.*

Zbog potrebe za poznavanjem barem djelomične faktorizacije broja $n-1$ prilikom korištenja Pocklingtonovog teorema, prostost ćemo testirati pomoću elipitčkih krivulja. Ovu ideju uveli su Goldwasser i Killian 1986. godine.

Definicija 15. *Neka je* K *polje.* ***Karaktristika polja*** K *je najmanji prirodni broj* n *takav da je* $1+1+...+1 = n \cdot 1 = 0$, *gdje su* 0 *i* 1 *neutralni elementi za zbrajanje, odnosno množenje u* K. *Ako je* $n \cdot \neq 0$ *za svaki prirodni broj* n, *onda se kaže da je* K *polje karakteristike 0.*

Primjerice, polja $\mathbb{N}$ i $\mathbb{C}$ su polja karatketistike 0, dok je karakteristika konačnog polja prost broj.

Definicija 16. *Neka je* K *polje karakteristike različite od 2 i 3 te neka je* $x^3 + ax + b$, $a, b \in K$ *kubični polinom bez višestrukih rješenja. Eliptička krivulja nad* K *je skup točaka* $(x, y) \in K \times K$ *koje zadovoljavaju jednadžbu*

$$y^2 = x^3 + ax + b, \tag{8}$$

zajedno s još jednim elementom kojeg označavamo s O *i nazivamo "točka u beskonačnosti".*

Napomena 8. *Ako je* K *polje karakteristike 2, onda je elitpička krivulja nad* K *skup točaka* $(x, y) \in K \times K$ *koje zadovoljavaju jednadžbu*

$$y^2 + cy = x^3 + ax + b$$

ili oblika

$$y^2 + xy = x^3 + ax^2 + b$$

zajedno s "točkom u beskonačnosti" O. *U ovom slučaju nam nije bitno imaju li ili nemaju navedene jednadžbe višestruka rješenja.*
Ako je polje K *karatkeristike 3, onda je eliptička krivulja nad* K *skup točaka* $(x, y) \in K \times K$ *koje zadovoljavaju*

$$y^2 = x^3 + ax^2 + bx + c,$$

(u ovom slučaju polinom s desne strane nema višestrukih rješenja) zajedno s "točkom u beskonačnosti" O.

Opširnije o eliptičkim krivuljama može se pronaći u [3] i [5].
Neka je E eliptička krivulja nad $\mathbb{Z}_n$. Broj $n-1$ može se shvatiti kao red grupe $\mathbb{Z}_n^*$, u slučaju kada je n prost broj. Zbog lakšeg pronalaženja eliptičke krivulje čiji se red može lako faktorizirati, grupu $\mathbb{Z}_n^*$ zamijenit ćemo grupom $E(\mathbb{Z}_n)$.
U nastavku dokazat ćemo teorem koji služi za testiranje prostosti pomoću eliptičkih krivulja.

Teorem 16 (vidjeti [3, Teorem 15.23.]). *Neka je E eliptička krivulja nad $\mathbb{Z}_n$, pri čemu je $n > 1$ i $(6, n) = 1$, dana izrazom $y^2 = x^3 + ax + b$. Neka je m prirodni broj koji ima prosti faktor $q > (n^{1/4} + 1)^2$. Ako postoji točka $P \in E(\mathbb{Z}_n)$ takva da je*

$$[m]P = O \qquad i \qquad [m/q]P \neq O,$$

onda je broj n prost.

Dokaz. Pretpostavimo da je n složen. Prema probnom dijeljenju, on ima prosti faktor $p \leq \sqrt{n}$. Neka je E' eliptička krivulja nad $\mathbb{Z}_p$ i neka ima istu jednadžbu kao i eliptička krivulja E. Neka je m' red grupe $E'(\mathbb{Z}_p)$. Prema Hasseovom teoremu[1] vrijedi

$$m' \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \leq (n^{1/4} + 1)^2 < q.$$

Stoga je $(m',\ q) = 1$ pa postoji $u \in \mathbb{Z}$ takav da je $uq \equiv 1 (\text{mod } m')$. Nadalje, neka je $P' \in E'(\mathbb{Z}_p)$ točka dobivena iz P redukcijom koordinata modulo p. Prema uvjetu teorema $[m/q]P$ je definirano te je različito od O modulo n. Istim postupkom modulo p dobivamo da je $[m/q]P' \neq O$. Ali istovremeno vrijedi i

$$[m/q]P' = [uq \cdot \frac{m}{q}]P' = [um]P' = [u]([m]P') = O,$$

čime dolazimo do kontradikcije s pretpostavkom da je n složen broj. □

Primjer 17 (vidjeti [4, Primjer 5.10.]). *Koristeći prethodni teorem, pokažimo da je broj 907 prost.*
Neka je E eliptička krivulja zadana jednadžbom $y^2 = x^3 + 10x - 2$ nad $\mathbb{Z}_n$. Red od $E(\mathbb{Z}_n)$ je $m = 923 = 71 \cdot 13$. Uzmimo $P = (56, 62)$ i $q = 71$. Tada je $[13]P = (338, 305) \neq O$ i $[923]P = [71]([13]P) = O$. Kako je $71 > (907^{1/4} + 1)^2$, slijedi da je broj 907 prost (ako je poznato da je broj 71 također prost).

2.6 Testiranje prostosti specijalnih brojeva

U Potpoglavlju 1.5. definirali smo dvije vrste specijalnih brojeva - Fermatove i Mersennove brojeve. U ovom potpoglavlju navest ćemo testove za testiranje prostosti tih brojeva.

Podsjetimo se, Fermatovi brojevi su oblika $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$.
Ranije smo rekli kako među Fermatovim brojevima ima i prostih i složenih brojeva. Idući teorem daje nam karakterizaciju prostih Fermatovih brojeva.

[1] Vidjeti [3, Teorem 15.19.].

Teorem 17 (Pepin, vidjeti [7, Theorem 5.3.]). *Za prirodan broj n, broj $F_n = 2^{2^n}+1$ je prost ako i samo ako vrijedi $5^{(F_n-1)/2} \equiv -1 (mod\ F_n)$*

Dokaz. Dokaz Pepinovog teorema može se pronaći u [7]. □

Primjer 18. *Već ranije naveli smo da je $F_4 = 65537$ za sada najveći poznati prost broj oblika $2^{2^n}+1$. Koristeći Pepinov teorem, pokazat ćemo da je zaista prost.*
Vrijedi:

$$5^{(F_n-1)/2} = 5^{65536/2} = 5^{32768} \equiv -1 (\text{mod } F_n)$$

te prema Pepinovom teoremu slijedi da je F_4 prost broj.

Idući test se koristi za testiranje prostosti Mersenneovih brojeva, odnosno brojeva oblika $M_n = 2^n - 1$, $n \in \mathbb{N}$.

Teorem 18 (Lucas - Lehmer, vidjeti [4, Teorem 5.20.]). *Neka je niz (v_k) zadan s $v_0 = 4$ i $v_{k+1} = v_k^2 - 2$. Neka je p neparan prost broj. Tada je Mersennov broj $M_p = 2^p - 1$ prost ako i samo ako $M_p | v_{p-2}$.*

Dokaz. Dokaz Lucas - Lehmerovog teorema može se pronaći u [4]. □

Primjer 19. *Koristeći Lucas-Lehmerov test, pokažimo da je broj 31 prost.*
31 je Mersennov broj za $p = 5$. Trebamo izračunati v_3. Iz $v_0 = 4$ i $v_{k+1} = v_k^2 - 2$ imamo sljedeće:

$$\begin{aligned} v_1 &= 4^2 - 2 = 14, \\ v_2 &= 14^2 - 2 = 194, \\ v_3 &= 194^2 - 2 = 37634. \end{aligned}$$

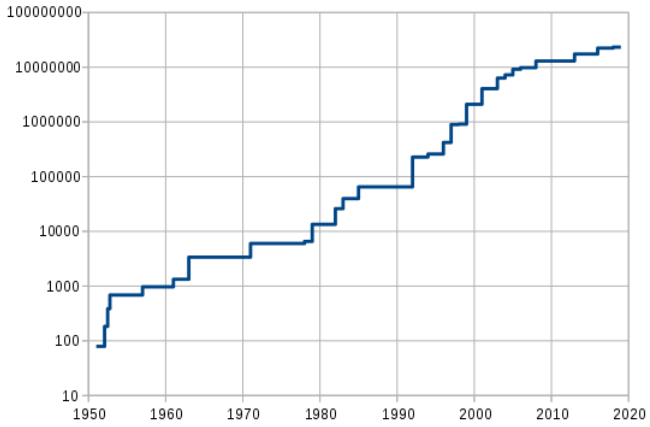
Lako vidimo da $M_5 | v_3$, $37634 = 1214 \cdot 31$. Prema tome, 31 je prost broj.

3 Zanimljivosti o prostim brojevima

U posljednjem poglavlju navest ćemo nekoliko zanimljivosti vezanih uz proste brojeve. Saznat ćemo koji je do sad najveći poznat prost broj te kako se prosti brojevi mogu vizualizirati. Konačno, navest ćemo zanimljive hipoteze o prostim brojevima koje do danas nisu dokazane.

3.1 Najveći prost broj

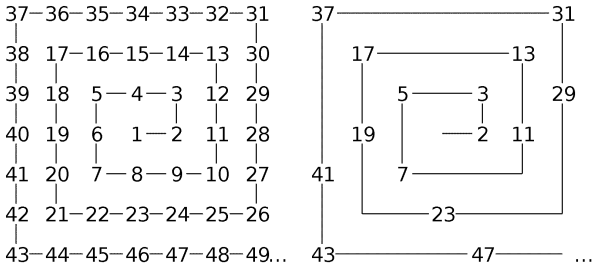
Do sada najveći poznat prost broj je broj $2^{82589933} - 1$. Otkrio ga je Patrick Laroche 2018.godine. Broj ima 24862048 znamenki. Nagrada za otkriće prostog broja s 10^7 znamenki iznosi 100000$ [8].
Na sljedećem grafu možemo vidjeti kako se broj znamenki najvećeg poznatog prostog broja mijenjao u zadnjih 70 godina:



Slika 5

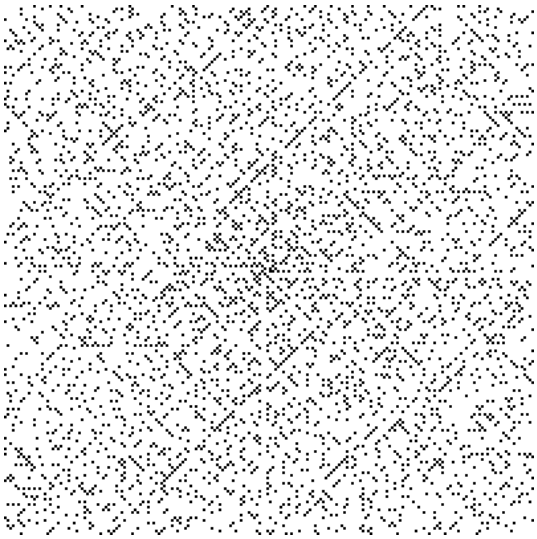
3.2 Vizualizacija prostih brojeva

Poljski matematičar Stanislaw Ulam je 1963. sasvim slučajno došao do spoznaje kako se prosti brojevi mogu jednostavno vizualizirati. Upravo po njemu je takav prikaz nazvan Ulamova spirala. Ulamova spirala dobije se tako da se najprije ispišu prirodni brojevi u obliku pravokutne spirale te se izbrišu svi brojevi koji nisu prosti.



Slika 6: Postupak dobivanja Ulamove spirale

.



Slika 7: Ulamova spirala veličine 200×200.

3.3 Nedokazane hipoteze u teoriji brojeva

U teoriji brojeva postoje mnoga otvorena pitanja te nedokazane hipoteze. Ranije je spomenuto nekoliko otvorenih pitanja vezanih uz Fermatove i Mersenneove brojeve. Najpoznatije nedokazane hipoteze u teoriji brojeva su hipoteza o parovima blizanaca te Goldbachova hipoteza [2].

Definicija 17. *Brojevi blizanci su prosti brojevi koji se razlikuju za 2.*

Primjerice, brojevi 3 i 5 te 11 i 13 su parovi blizanci.
U prvih 10 prirodnih brojeva postoji 2 para blizanaca, u prvih 100 ima njih 8, a u prvih 1000 postoji njih 35. Možemo primijetiti kako se udio takvih parova smanjuje. Jedna od najpoznatijih nedokazanih hipoteza je:

Hipoteza 1. *Parova blizanaca ima beskonačno mnogo.*

Do danas najveći poznati par blizanaca je $2996863034895 \cdot 2^{1290000} \pm 1$ (vidi [8]).

Druga nedokazana hipoteza je Goldbachova hipoteza:

Hipoteza 2. *Svaki parni prirodni broj veći od 2 može se prikazati kao suma dva prosta broja.*

Hipotezu je postavio ruski matematičar Christian Goldbach 1742. godine, po kome je hipoteza i dobila ime. 2013. godine dokazana je tzv. neparna Goldbachova slutnja da se svaki neparni prirodni broj $n \geq 7$ može prikazati kao suma tri prosta broja. Slutnju je dokazao peruanski matematičat Helfgott (vidjeti [3]).

Literatura

[1] F. M. Brückler, *Povijest matematike I,* Odjel za matematiku, Sveučilište u Osijeku, Osijek, 2014.

[2] F. M. Brückler, *Povijest matematike II,* Odjel za matematiku, Sveučilište u Osijeku, Osijek, 2009.

[3] A. Dujella, *Teorija brojeva,* Školska knjiga, Zagreb, 2019.

[4] A. Dujella, M. Maretić, *Kriptografija,* Element, Zagreb, 2007.

[5] N. Koblitz, *A Course in Number Theory and Cryptography,* Springer, New York, 1994.

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

[7] R. A. Mollin, *An introduction to cryptography* (2. izdanje), Chapman & Hall/CRC, Boca Raton, 2007.

[8] *The largest known primes,* dostupno na `https://primes.utm.edu/largest.html`, `02. lipnja 2020.`

[9] *Why are Prime Numbers called Primes*?, dostupno na `https://primes.utm.edu/notes/faq/WhyCalledPrimes.html, 05. lipnja 2020.`

[10] J. Barthel, P. Sgobba, F. Zhu, *Visualing the distribution of primes,* dostupno na `http://math.uni.lu/eml/projects/reports/prime-distribution.pdf`.