Osječki matematički list 25 (2025), 161–178

Testovi prostosti

Bernadin Ibrahimpašić*, Sajra Kasić†

Sažetak

U članku se opisuju testovi prostosti s posebnim naglaskom na vjerojatnosne testove prostosti. To su kriteriji za koje vrijedi da ako ih prirodni broj n zadovolji tada je n vjerojatno prost i u tom slučaju kažemo da je broj n možda prost. Međutim, ako ih broj n ne zadovolji onda je n sigurno složen. Opisat ćemo Fermatov, Solovay – Strassenov i Miller – Rabinov test.

Ključne riječi: *prosti brojevi, pseudoprosti brojevi, testovi prostosti*

Primality tests

Abstract

In this paper we describe some primality tests with emphasis on probabilistic algorithms. A primality test is an algorithm for determining whether an input number is prime. A probabilistic primality test is a primality test that outputs "probable prime" or "composite" and has certain of error if the output is "probable prime". We will describe Fermat, Solovay – Strassen and Miller – Rabin primality test.

Keywords: *primes, pseudoprimes, primality tests*

*Pedagoški fakultet, Univerzitet u Bihaću, email: bernadin@bih.net.ba
†Pedagoški fakultet, Univerzitet u Bihaću, email: sajra.kasic@gmail.com

1 Prosti brojevi

Teorija brojeva, kao jedna od najstarijih grana matematike, prvenstveno se bavi proučavanjem svojstava cijelih brojeva, kao što su djeljivost, prostost, parnost, aditivnost, multiplikativnost, jedinstvenost faktorizacije, itd. Djeljivost se proučava najmanje tri tisuće godina. Prije vremena Pitagore, Grci su razmatrali pitanja o parnim i neparnim brojevima, savršenim i prijateljskim brojevima te i među mnogim drugima i o prostim brojevima. Ni danas na neka od tih pitanja još uvijek nema odgovora. Inače, jedna od karakteristika teorije brojeva je da se u njoj dosta problema može lako iskazati, ali istovremeno i teško riješiti.

Prosti brojevi, za koje se također koristi i naziv prim brojevi, pripadaju ekskluzivnom svijetu intelektualnih koncepcija. Prosti brojevi imaju mnoga posebna i lijepa svojstva i igraju vrlo važnu ulogu u teoriji brojeva. Jedna od najvažnijih činjenica o prostim brojevima, koja kaže da prostih brojeva ima beskonačno mnogo, veže se uz Euklida. Također treba istaknuti činjenicu da se svaki prirodan broj veći od 1 može na jedinstven način prikazati kao produkt prostih brojeva.

Gauss, koji je matematiku nazvao kraljicom znanosti a teoriju brojeva kraljicom matematike, je kao dva temeljna problema i dva najvažnija istraživačka polja u teoriji brojeva istakao testiranje prostosti i faktorizaciju prirodnih brojeva. Istaknimo da su ta dva problema, pojavom modernih računala, našli veliku primjenu u kriptografiji s javnim ključem i informacijskoj sigurnosti.

Definicija 1.1. *Neka su $m \neq 0$ i a cijeli brojevi. Kažemo da je a **djeljiv** s m, odnosno da m **dijeli** a, ako postoji cijeli broj q takav da je $a = mq$. To zapisujemo s $m|a$. Ako a nije djeljiv s m, onda pišemo $m \nmid a$.*

*Ako $m|a$, onda još kažemo da je m **djelitelj** ili **faktor** od a te da je a **višekratnik** od m.*

Za prirodan broj n brojevi 1 i n nazivaju se **trivijalni djelitelji** broja n, dok se njegov djelitelj d, takav da je $1 < d < n$, naziva **netrivijalan djelitelj** broja n. Pozitivni djelitelj broja n, koji je različit od n, naziva se **pravi djelitelj** broja n.

Definicija 1.2. *Za prirodan broj $p > 1$ kažemo da je **prost** ako nema nijednog djelitelja d takvog da je $1 < d < p$, tj. ako su njegovi jedini pozitivni djelitelji 1 i p. Za prirodan broj $n > 1$ koji nije prost kažemo da je **složen**.*

Navedimo sada neke tvrdnje o prostim brojevima čiji se dokazi mogu pronaći u [1].

- Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva s jednim ili više faktora. Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora (Osnovni teorem aritmetike, [1, Teorem 2.12]).
- Ako je p prost i $p|ab$ onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1a_2 \cdot \ldots \cdot a_k$ onda p dijeli bar jedan faktor a_i.
- Svaki složeni broj n ima prost faktor $p \leq \sqrt{n}$.

Napomenimo da analogon Osnovnog teorema aritmetike ne vrijedi za cijele brojeve u nekim kvadratnim poljima. Tako u $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ možemo navesti sljedeće tri faktorizacije broja 7

$$7 = 1 \cdot 7 = -1 \cdot (-7) = (5 + 3\sqrt{2})(5 - 3\sqrt{2}).$$

Iz Osnovnog teorema aritmetike slijedi da svaki prirodan broj $n > 1$ možemo na jedinstven način prikazati u obliku

$$n = {p_1}^{k_1} \cdot {p_2}^{k_2} \cdot \ldots \cdot {p_r}^{k_r},$$

gdje su $p_1, \ldots, p_r$ različiti prosti brojevi a $k_1, \ldots, k_r$ prirodni brojevi. Ovakav prikaz broja n zove se **kanonski rastav** broja n na proste faktore.

Metoda prosijavanja u teoriji brojeva je metoda ili postupak za pronalaženje brojeva sa željenim svojstvom, gdje se iz popisa brojeva do neke određene granice, uzastopnim uklanjanjem kandidata koji ne zadovoljavaju neko svojstvo, na kraju dolazi do samo onih brojeva koji imaju traženo svojstvo. Želimo li generirati tablicu prostih brojeva manjih ili jednakih danom prirodnom broju n, što je prije razvoja računala bilo skoro pa neophodno, to možemo uraditi tzv. **Eratostenovim sitom**.

Eratosten iz Cirene bio je starogrčki kartograf, geograf, filozof, matematičar i astronom (Cirena, Libija, oko 276. god. pr.n.e. – Aleksandrija, Egipat, oko 194. god. pr.n.e.) je, osim razvoja postupka za generiranje prostih brojeva, opisao postupak za određivanje opsega Zemlje, približno točno odredio nagib ekliptike prema nebeskom ekvatoru, dužinu dana i trajanje godine.

Ako želimo pronaći sve proste brojeve manje ili jednake od n onda zapišemo sve prirodne brojeve od 2 do n. Zaokružimo broj 2 a zatim prekrižimo sve višekratnike broja 2 koji su veći od 2. Nakon toga zaokružimo najmanji preostali broj koji nije ni zaokružen ni prekrižen te prekrižimo sve njegove višekratnike koji su veći od njega. Postupak ponavljamo dok ima nezaokruženih ili neprekriženih brojeva a zaustavljamo se kada najmanji nezaokruženi ili neprekriženi broj bude veći od $\sqrt{n}$. Nakon konačno mnogo koraka će preostati samo prosti (zaokruženi i neprekriženi) brojevi.

Pogledajmo kako to izgleda ako želimo generirati proste brojeve manje ili jednake od 50.

Slika 1. Eratostenovo sito

Dobili smo da su prosti brojevi manji ili jednaki 50: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$ i 47.

Na slici 1 također je vidljivo da postoje susjedni brojevi koji su prosti. To su brojevi 2 i 3 i to je jedini par susjednih prostih brojeva. Međutim vidimo da i među prvih 50 prirodnih brojeva ima dosta susjednih neparnih brojeva koji su prosti (5 i 7, 11 i 13, 17 i 19, 29 i 31, te 41 i 43). Takva dva broja se nazivaju **prosti brojevi blizanci**. Postoji slutnja da prostih brojeva blizanaca ima beskonačno mnogo. S druge strane uzastopni prosti brojevi mogu biti prilično udaljeni o čemu svjedoči tvrdnja (za dokaz vidjeti [1]) koja kaže da za svaki prirodan broj n postoji bar n uzastopnih složenih brojeva. Rečeno nas ne navodi na očekivanje pravilnosti u pojavljivanju prostih brojeva. Također, činjenice da u intervalima $(1, 100)$, $(100, 200)$, $(10^7, 10^7 + 100)$, $(10^8 - 100, 10^8)$, $(10^8, 10^8 + 100)$, $(10^9 - 100, 10^9)$ i $(10^9, 10^9 + 100)$ imamo redom $25, 21, 2, 5, 6, 2$ i 7 prostih brojeva, smanjuju nam nadu u pravilnost njihovog pojavljivanja. Ipak postoji izvjesna pravilnost u pojavljivanju prostih brojeva. Tako imamo da je osnovni rezultat o distribuciji prostih brojeva **Teorem o prostim brojevima** (PNT – Prime Number Theorem, vidjeti [1]) koji kaže da se za $x > 0$ broj prostih brojeva manjih ili jednakih x, u oznaci $\pi(x)$, može aproksimirati kvocijentom $x/\ln x$, tj. da vrijedi

$$\pi(x) \sim \frac{x}{\ln x}.$$

Ovu tvrdnju naslutio je Gauss a dokazali su je, neovisno jedan od drugog, Hadamard i de la Vallée Poussin 1896. godine. Strategija, kao i sam dokaz PNT–a može se vidjeti primjerice u [3, Chapter 9].

Pogledajmo jednu grublju, ali jednostavniju za računanje, aproksimaciju broja $\pi(x)$. Kako je broj znamenki broja $\lfloor x \rfloor$ (najveće cijelo $\lfloor x \rfloor$ od x je

najveći cijeli broj koji nije veći od x) u bazi 10 jednak najmanjem cijelom broju strogo većem od $\log\lfloor x\rfloor$ te kako je $\ln x = \ln 10 \cdot \log x$ to se broj $\pi(x)$ ugrubo može aproksimirati funkcijom

$$f(x) = \frac{x}{2 \cdot (\text{broj znamenki od } \lfloor x\rfloor)}.$$

Još bolja aproksimacija funkcije $\pi(x)$ je tzv. **logaritamsko–integralna funkcija**

$$\mathrm{li}(x) = \int_2^x \frac{1}{\ln t} dt.$$

Iako su prosti brojevi predmet proučavanja još od samih početaka matematike, ipak je nagli razvoj računarstva u 20. stoljeću dao prostim brojevima novi značaj. Našli su veliku primjenu u kriptosustavima s javnim ključem i bez njih bi kriptografija javnog ključa bila skoro pa nezamisliva kao i općenito kompletna informacijska sigurnost. Potreba za pronalaženjem velikih prostih brojeva razvila je potrebu za postojanjem algoritama za ispitivanje je li dani broj prost ili ne.

Ispitivanje je li (neparan) prirodan broj n prost vrši se pomoću testova prostosti. Možemo ih podijeliti u dvije klase. U jednu klasu spadaju deterministički testovi koji daju točan odgovor je li testirani broj prost ili ne. Međutim, njihova primjena nije efikasna za velike prirodne brojeve. U drugu klasu spadaju vjerojatnosni testovi. To su kriteriji za koje vrijedi da ako ih prirodan broj n zadovolji tada je n vjerojatno (s nekom vjerojatnošću) prost. U tom slučaju kažemo da je broj n možda prost. Međutim, ako ih broj n ne zadovolji onda je n sigurno složen. Što više takvih testova broj n prođe (zadovolji) to je veća vjerojatnost da je broj n prost. Vjerojatnost uspjeha, tj. dobivanja točnog odgovora, povećava se kako raste raspoloživo vrijeme za algoritam. Osnovna manjkavost ovakvih algoritama je da se ne može potpuno sigurno vidjeti je li dobiveni odgovor točan.

Također treba napraviti razliku između testova prostosti i metoda za dokazivanje prostosti. Vjerojatnosni testovi prostosti su puno brži od poznatih metoda za dokazivanje prostosti. Metode za dokazivanje prostosti koriste tvrdnje koje karakteriziraju proste brojeve, ali one nisu jednostavne za provjeru. S druge strane, vjerojatnosni testovi prostosti koriste neka važna svojstva prostih brojeva, ali ta svojstva ne karakteriziraju proste brojeve jer postoje i neki složeni brojevi koji imaju to svojstvo.

2 Deterministički testovi prostosti

Jedan način za provjeru prostosti broja n je da ga dijelimo sa svim prostim brojevima manjim ili jednakim $\sqrt{n}$. Ako n nije djeljiv ni s jednim od njih

onda je n sigurno prost.

Primjer 2.1. *Dijeljenjem s prostim brojevima provjerimo jesu li brojevi* 825 *i* 373 *prosti.*

Rješenje. Kako je

$$28 < \sqrt{825} < 29 \qquad \text{i} \qquad 19 < \sqrt{373} < 20$$

to broj 825 pokušavamo dijeliti s prostim brojevima manjim ili jednakim 28 $(2, 3, 5, 7, 11, 13, 17, 19, 23)$ a broj 373 pokušavamo dijeliti prostim brojevima manjim ili jednakim 19 $(2, 3, 5, 7, 11, 13, 17, 19)$. Dobivamo da je

$$825 = 3 \cdot 5 \cdot 5 \cdot 11 = 3 \cdot 5^2 \cdot 11$$

pa je složen, a kako broj 373 nije djeljiv s navedenim prostim brojevima to zaključujemo da je prost. ◀

Istaknimo da ovaj test nije praktičan za velike prirodne brojeve n jer traje predugo. Pretpostavimo li da je $n > 10^{100}$ tada je $\sqrt{n} > 10^{50}$ pa je u slučaju da je n prost potrebno provesti više od 10^{50} dijeljenja sa svim brojevima manjim od 10^{50}. Ako posjedujemo računalo koje izvodi 10^{10} dijeljenja u sekundi jednostavno se pokazuje da je za to potrebno više od 10^{31} godina. Čak ni u situaciji da znamo sve proste brojeve manje od 10^{50} ne bismo imali puno "bolje" vrijeme.

Jedna od relacija koja se često koristi u testiranju prostosti je relacija biti kongruentan modulo m koja je relacija ekvivalencije na skupu cijelih brojeva.

Definicija 2.1. *Ako cijeli broj* $m \neq 0$ *dijeli razliku* $a - b$ *onda kažemo da je* a ***kongruentan*** b ***modulo*** m *i pišemo* $a \equiv b \pmod{m}$. *U protivnom kažemo da a* ***nije kongruentan*** b ***modulo*** m *i pišemo* $a \not\equiv b \pmod{m}$.

Kako je $a - b$ djeljivo s m ako i samo ako je djeljivo s $-m$, to možemo razmatrati samo slučajeve kada je m pozitivan cijeli broj, tj. kada je m prirodan broj. Očigledno je da ako je $a \equiv b \pmod{m}$ da tada postoji cijeli broj k takav da je $a = km + b$.

Sljedeći teorem karakterizira proste brojeve.

Teorem 2.1 (Mali Fermatov teorem, vidjeti [1]). *Neka je b prirodan broj i p prost broj takav da* $p \nmid b$. *Tada je*

$$b^{p-1} \equiv 1 \pmod{p}.$$

Za svaki cijeli broj b vrijedi da je $b^p \equiv b \pmod{p}$.

Napomenimo da obrat Malog Fermatovog teorema ne vrijedi, jer n može biti i složen a da ipak za neki prirodan broj b vrijedi da je $b^{n-1} \equiv 1 \pmod{n}$. Kao primjer koji to potvrđuje možemo uzeti $b = 2$ i $n = 341$. Dobivamo da je $2^{340} \equiv 1 \pmod{341}$ ali broj $341 = 11 \cdot 31$ nije prost.

Međutim ako se uvjet $b^{n-1} \equiv 1 \pmod{n}$ proširi s odgovarajućim dodatnim uvjetom mogu se dobiti tzv. obrati Teorema 2.1. Jedan od njih je tzv. Lucasov obrat.

Teorem 2.2 (Lucasov obrat Malog Fermatovog teorema, [8]). *Neka je $n > 1$ prirodan broj. Ako postoji cijeli broj b takav da je*

1. $b^{n-1} \equiv 1 \pmod{n}$ *i*
2. $b^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$, *za svaki prost p takav da $p|(n-1)$,*

tada je n prost broj.

Primjer 2.2. *Primjenom Teorema* 2.2 *pokažimo da je* 991 *prost broj.*

Rješenje. Imamo da je $n = 991$ pa je $n - 1 = 990 = 2 \cdot 3^2 \cdot 5 \cdot 11$. Kako je

$$2^{990/2} \equiv 3^{990/3} \equiv 4^{990/2} \equiv 5^{990/2} \equiv 1 \pmod{991},$$

to za $b \in \{2, 3, 4, 5\}$ još ne možemo zaključiti je li 991 prost broj, jer nije ispunjen uvjet 2 iz Teorema 2.2. Međutim kako je

$$6^{990} \equiv 1,\ 6^{990/2} \equiv 990,\ 6^{990/3} \equiv 113,\ 6^{990/5} \equiv 825,\ 6^{990/11} \equiv 118 \pmod{991}$$

to prema Teoremu 2.2 zaključujemo da je broj 991 prost broj. ◄

Napomenimo da je nedostatak ovog testa taj što se zahtijeva poznavanje faktorizacije broja $n - 1$ što je slične težine kao i faktorizacija od n pa je samim tim problem teži nego testiranje prostosti broja n.

Navedimo još jedan teorem, također tzv. obrat Teorema 2.1, koji može poslužiti kao osnova za testiranje prostosti.

Teorem 2.3 (Pocklington, vidjeti [1]). *Neka je s djelitelj od $n - 1$ koji je veći od $\sqrt{n}$. Ako postoji prirodan broj b takav da je*

1. $b^{n-1} \equiv 1 \pmod{n}$ *i*
2. $\operatorname{nzd}\left(b^{(n-1)/q} - 1, n\right) = 1$ *za svaki prost faktor q od s,*

onda je n prost broj.

Problem računanja najvećeg zajedničkog djelitelja $y = \text{nzd}\left(b^{(n-1)/q} - 1, n\right)$ rješavamo tako da najprije pomoću algoritma "kvadriraj i množi" (vidjeti [4]) izračunamo $z = b^{(n-1)/q} \bmod n$ a zatim pomoću Euklidovog algoritma izračunamo $y = \text{nzd}(z-1, n)$.

Primjer 2.3. *Primjenom Teorema* 2.3 *pokažimo da je broj* 147353 *prost broj.*

Rješenje. Imamo da je

$$n = 147353,\ 383 < \sqrt{147353} < 384,\ n - 1 = 147352 = 2^3 \cdot 113 \cdot 163,$$

pa možemo uzeti da je

$$s = 2^2 \cdot 113 = 452 > \sqrt{147353}.$$

Prosti faktori od s su $q_1 = 2$ i $q_2 = 113$. Uzmemo li da je $b = 3$ imamo da je

$$3^{n-1} \equiv 1 \pmod{n},\ \text{nzd}\left(3^{(n-1)/2} - 1, n\right) = 1,\ \text{nzd}\left(3^{(n-1)/113} - 1, n\right) = 1$$

pa na osnovu Teorema 2.3 zaključujemo da je broj $n = 147353$ prost broj.◄

Napomenimo da smo ovdje koristili činjenicu da je 113 prost broj. Da bismo dokazali da je broj 113 prost možemo koristiti istu ili neku drugu metodu. Kako je $113 - 1 = 112 = 2^4 \cdot 7$ to možemo uzeti da je $s = 2^4 = 16 > \sqrt{113}$ i $q = 2$. Kako je $5^{112} \equiv 1 \pmod{113}$ i $\text{nzd}(5^{112/2} - 1, 113) = 1$ to možemo zaključiti da je 113 prost.

U prethodnom primjeru vidjeli smo da se prilikom primjene Pocklingtonova teorema pitanje prostosti jednog broja svodi na pitanje prostosti jednog ili više manjih brojeva. Taj postupak nastavljamo sve dok brojevi ne postanu dovoljno maleni.

Često se testovi koji koriste navedene tvrdnje nazivaju "$n-1$ testovi", jer se u njihovoj implementaciji koristi faktorizacija broja $n-1$. Kako je faktorizacija velikih prirodnih brojeva općenito težak problem to su $n-1$ testovi neprilagođeni za upotrebu s velikim prirodnim brojevima. Ipak oni su prikladni u slučajevima brojeva n specijalnog oblika kod kojih je faktorizacija broja $n-1$ jednostavna ili kod kojih je poznata faktorizacija dovoljno velikog djelitelja od $n-1$.

Sljedeći teorem je ekvivalentan Teoremu 2.2 te i on može biti korišten u testiranju prostosti. Prije samog iskaza teorema navedimo dvije definicije.

Definicija 2.2. *Neka su a i n relativno prosti prirodni brojevi. Najmanji prirodan broj d sa svojstvom da je $a^d \equiv 1 \pmod{n}$ naziva se* ***red*** *od a modulo n i označava s $\text{ord}_n(a)$.*

Definicija 2.3. *Funkcija* $\varphi\colon \mathbb{N} \to \mathbb{N}$ *koja prirodnom broju* m *pridružuje broj prirodnih brojeva manjih ili jednakih* m *koji su relativno prosti s* m *naziva se* ***Eulerova funkcija****.*

Eulerova funkcija je multiplikativna, tj. $\varphi(1) = 1$ te ako su m i n relativno prosti prirodni brojevi onda vrijedi $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. Ako je $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ kanonski rastav prirodnog broja $n > 1$ na proste faktore onda vrijedi

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_r}\right).$$

Specijalno imamo da za prost broj p vrijedi $\varphi(p) = p - 1$.

Teorem 2.4 (vidjeti [8]). *Neka su* a *i* n *relativno prosti prirodni brojevi. Ako je*

$$\operatorname{ord}_n(a) = \varphi(n) = n - 1$$

onda je n *prost broj.*

Primjer 2.4. *Primjenom Teorema* 2.4 *pokažimo da je* 3457 *prost.*

Rješenje. Kako je $\operatorname{ord}_{3457}(2) = 576$, $\operatorname{ord}_{3457}(3) = 1728$, $\operatorname{ord}_{3457}(4) = 288$, $\operatorname{ord}_{3457}(5) = 1152$ i $\operatorname{ord}_{3457}(6) = 432$, brojevi $2, 3, 4, 5$ i 6 nisu dobri kandidati za broj a. Međutim, za $a = 7$ vrijedi

$$\operatorname{nzd}(7, 3457) = 1, \;\; \operatorname{ord}_{3457}(7) = 3456 \;\text{ i }\; \varphi(3457) = 3456,$$

pa zaključujemo da je broj 3457 prost. ◀

3 Vjerojatnosni testovi prostosti

Ponovimo već opisanu karakteristiku vjerojatnosnih testova prostosti. To su kriteriji za koje vrijedi da ako ih broj n prođe (zadovolji), tada je n možda (vjerojatno) prost, a u slučaju da ih n ne prođe (ne zadovolji), onda je n sigurno složen. Vidimo da u slučaju kada n prođe vjerojatnosni test prostosti, to ne mora uvijek značiti da je takav n zaista prost broj. U takvim slučajevima, kada želimo potpunu sigurnost da je n zaista prost, rezultat testa je potrebno potvrditi nekom od algebarskih metoda ispitivanja prostosti brojeva, poput same faktorizacije ili nekog od deterministčkih testova prostosti (primjerice vidjeti [2, poglavlje 4]).

3.1 Fermatov test

Činjenica da ne vrijedi obrat Malog Fermatovog teorema nas dovodi do koncepta **pseudoprostih brojeva**.

Definicija 3.1. *Ako je n neparan složen broj i b cijeli broj relativno prost s n koji zadovoljava kongruenciju*

$$b^{n-1} \equiv 1 \pmod{n} \tag{1}$$

*onda kažemo da je n **pseudoprost broj u bazi** b u oznaci* $\mathrm{psp}(b)$.

Teorem 3.1 (vidjeti [2]). *Neka je n neparan složen broj. Tada vrijedi:*

1. *n je pseudoprost broj u bazi b, gdje je* $\mathrm{nzd}(b,n) = 1$, *ako i samo ako* $\mathrm{ord}_n(b) | (n-1)$;
2. *Ako je n pseudoprost u bazama b_1 i b_2, onda je n pseudoprost i u bazama $b_1 \cdot b_2$ i $b_1 \cdot b_2^{-1}$;*
3. *Ako n ne zadovoljava relaciju (1) za neku bazu b, onda n ne zadovoljava relaciju (1) za bar pola mogućih baza b (brojeva između 1 i n koji su relativno prosti s n).*

Kako je definicija pseudoprostog broja u direktnoj vezi s Malim Fermatovim teoremom to se za pseudoprost broj u bazi b koristi i naziv **Fermatov pseudoprost broj u bazi** b.

Pseudoprosti brojevi u bazi b ponašaju se kao prosti brojevi, tj. oni prolaze test prostosti. Za svaki prirodan broj $b \geq 2$ postoji beskonačno mnogo pseudoprostih brojeva u bazi b (vidjeti [1]). Njihovo postojanje pokazuje da nije dovoljno testirati prostost nekog broja n samo u jednoj bazi kako bismo zaključili je li on prost. Tako imamo da je

$$2^{340} \equiv 1 \pmod{341} \qquad \text{i} \qquad 3^{340} \equiv 56 \not\equiv 1$$

pa je složeni broj $341 = 11 \cdot 31$ $\mathrm{psp}(2)$, ali nije $\mathrm{psp}(3)$. Slično tome imamo da je

$$2^{90} \equiv 64 \not\equiv 1 \pmod{91} \qquad \text{i} \qquad 3^{90} \equiv 1,$$

pa je složeni broj $91 = 7 \cdot 13$ $\mathrm{psp}(3)$ ali nije $\mathrm{psp}(2)$.

Teorem 3.1 može se iskoristiti kao osnova za vjerojatnosni test prostosti. Na slučajan način izaberemo b, $0 < b < n$. Ako je relacija (1) ispunjena, zaključujemo da je n prošao test i biramo sljedeći b. Ako relacija (1) nije ispunjena, onda znamo da je n sigurno složen. Kako je vjerojatnost da složeni broj n prođe test manja od $1/2$ ako n prođe test za k slučajno i neovisno odabranih b–ova, onda je vjerojatnost da je n složen manja od $1/2^k$.

Primjer 3.1. *Odredimo najmanji broj k različitih baza b za koje n zadovoljava relaciju* (1) *da bismo tvrdili* (*smatrali*) *da je n prost s vjerojatnošću većom od p, $0 < p < 1$.*

Rješenje. Kako znamo da vjerojatnost da je n složen je manja ili jednaka $1/2^k$ to mora biti

$$1 - \frac{1}{2^k} > p$$

iz čega se dobiva

$$k > \log_2 \frac{1}{1-p}.$$

Sada zaključujemo da nam je potrebno barem

$$k = \left\lfloor \log_2 \frac{1}{1-p} \right\rfloor + 1$$

različitih baza. ◀

Primjer 3.2. *Ispitajmo s vjerojatnošću većom od* $0,95$ *jesu li brojevi* $31, 341$ *i* 561 *prosti.*

Rješenje. Imamo da nam treba najmanje

$$k = \left\lfloor \log_2 \frac{1}{1-0,95} \right\rfloor + 1 = 4 + 1 = 5$$

različitih baza. Najlakše nam je uzeti prvih 5 odgovarajućih prostih brojeva.

Kako vrijedi

$$2^{30} \equiv 3^{30} \equiv 5^{30} \equiv 7^{30} \equiv 11^{30} \equiv 1 \pmod{31}$$

to zaključujemo s vjerojatnošću većom od $0,95$ da je broj 31 prost što on zaista i jeste.

Kako vrijedi

$$2^{340} \equiv 1 \qquad \text{i} \qquad 3^{340} \equiv 56 \not\equiv 1 \pmod{341}$$

to zaključujemo da je broj 341 složen, što on zaista i jeste, jer je $341 = 11 \cdot 31$.

Kako vrijedi

$$2^{560} \equiv 5^{560} \equiv 7^{560} \equiv 13^{560} \equiv 19^{560} \equiv 1 \pmod{561}$$

to zaključujemo s vjerojatnošću većom od $0,95$ da je broj 561 prost, iako je broj $561 = 3 \cdot 11 \cdot 17$ složen. ◀

Vidjeli smo da je broj 561 prošao svih 5 testova, iako je složen. To predstavlja nedostatak ovog testa jer postoje složeni brojevi koji zadovoljavaju relaciju (1) za svaki cijeli broj b, tj. koji su pseudoprosti u svim bazama. Ti brojevi nazivaju se **Carmichaelovi brojevi**, ima ih beskonačno mnogo a najmanji od njih je 561.

Definicija 3.2. *Složeni broj n za kojeg je $b^{n-1} \equiv 1 \pmod{n}$ za svaki cijeli broj b, gdje je $\mathrm{nzd}(b,n) = 1$, zove se **Carmichaelov broj**.*

3.2 Solovay–Strassenov test

Problem postojanja Carmichaelovih brojeva možemo izbjeći testom koji koristi jedan drugi uvjet. To je Solovay–Strassenov test za koji ne postoje analogoni Carmichaelovih brojeva, tj. ne postoje složeni brojevi koji će proći test za sve baze. U njegovoj implementaciji koristi se pojam Jacobijevog simbola pa ga definirajmo.

Definicija 3.3. *Neka je m prirodan i a cijeli broj, gdje je $\mathrm{nzd}(a,m) = 1$. Ako kongruencija $x^2 \equiv a \pmod{m}$ ima rješenja onda kažemo da je a **kvadratni ostatak** modulo m. Ako navedena kongruencija nema rješenja onda kažemo da je a **kvadratni neostatak** modulo m.*

Napomenimo da su kvadratni ostaci i neostaci definirani samo kada je ispunjen uvjet $\mathrm{nzd}(a,m) = 1$.

Definicija 3.4. *Neka je p neparan prost broj i a cijeli broj. **Legendreov simbol** $\left(\frac{a}{p}\right)$ definira se na sljedeći način:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0\,, & \text{ako } p|a, \text{ tj. ako je } a \equiv 0 \pmod{p}, \\ 1\,, & \text{ako je } a \text{ kvadratni ostatak modulo } p, \\ -1\,, & \text{ako je } a \text{ kvadratni neostatak modulo } p. \end{cases}$$

Teorem 3.2 (Eulerov kriterij, vidjeti [1]). *Neka je p neparan prost broj i a cijeli broj. Tada je a kvadratni ostatak modulo p ako i samo ako je*

$$a^{(p-1)/2} \equiv 1 \pmod{p},$$

što je ekvivalentno s

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Definicija 3.5. *Neka je* $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$ *neparan prirodan broj i* a *cijeli broj. Tada se* ***Jacobijev simbol*** $\left(\frac{a}{n}\right)$ *definira kao*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \cdot \left(\frac{a}{p_2}\right)^{k_2} \cdot \ldots \cdot \left(\frac{a}{p_r}\right)^{k_r},$$

gdje su $\left(\frac{a}{p_i}\right)$, $i = 1, 2, \ldots, r$, *Legendreovi simboli.*

Definicija 3.6. *Ako je* n *neparan složen broj i* b *cijeli broj relativno prost s* n *te ako Jacobijev simbol* $\left(\frac{b}{n}\right)$ *zadovoljava relaciju*

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod{n} \tag{2}$$

onda kažemo da je n ***Eulerov pseudoprost broj u bazi*** b *u oznaci* $\mathrm{epsp}(b)$.

Kvadriranjem relacije (2) dobivamo relaciju (1) pa zaključujemo da je svaki Eulerov pseudoprost u bazi b ujedno i pseudoprost u istoj bazi. Obrat ne vrijedi. Kako smo vidjeli, 91 je $\mathrm{psp}(3)$, međutim kako je $3^{45} \equiv 27 \pmod{91}$ to 91 nije $\mathrm{epsp}(3)$.

Teorem 3.3 (vidjeti [2]). *Neka je* n *neparan složen broj. Tada je* n *Eulerov pseudoprost broj za najviše polovinu mogućih baza* b, $0 < b < n$.

Ovaj teorem nam daje osnovu za još jedan vjerojatnosni test, ali za koji ne postoje analogoni Carmichaelovih brojeva, jer za svaki složeni broj n relacija (2) nije zadovoljena za bar polovinu mogućih baza. I ovdje kao i u Fermatovom testu slučajno biramo k različitih baza b, $0 < b < n$ te računamo obje strane kongruencije (2). Ako za neku bazu b dobijemo dva nekongruentna broja, onda se test zaustavlja i tada smo sigurni da je n složen broj. Ako n prođe test za svih k odabranih baza b, onda je vjerojatnost da je n složen manja od $1/2^k$. Iz toga kao i kod Fermatovog testa zaključujemo da za broj k, koji predstavlja najmanji potreban broj različitih baza za koje n treba proći test da bismo s vjerojatnošću većom od p, $0 < p < 1$, tvrdili da je n prost, vrijedi

$$k = \left\lfloor \log_2 \frac{1}{1-p} \right\rfloor + 1.$$

Primjer 3.3. *Ispitajmo s vjerojatnošću većom od* 0,9 *jesu li brojevi* 101 *i* 1729 *prosti.*

Rješenje. Vrijedi

$$k = \left\lfloor \log_2 \frac{1}{1-0,9} \right\rfloor + 1 = 3 + 1 = 4$$

pa su nam potrebne najmanje 4 različite baze.

a) Uzmemo li za baze prva 4 prosta broja, tj. $2, 3, 5$ i 7, dobivamo:

$$\left(\frac{2}{101}\right) = -1, \qquad 2^{(101-1)/2} \equiv -1 \pmod{101},$$

$$\left(\frac{3}{101}\right) = -1, \qquad 3^{(101-1)/2} \equiv -1 \pmod{101},$$

$$\left(\frac{5}{101}\right) = 1, \qquad 5^{(101-1)/2} \equiv 1 \pmod{101},$$

$$\left(\frac{7}{101}\right) = -1, \qquad 7^{(101-1)/2} \equiv -1 \pmod{101}.$$

Zaključujemo s vjerojatnošću većom od $0,9$ da je broj 101 prost, što on i jeste.

b) Ako za baze uzmemo brojeve $2, 3, 5$ i 11 onda imamo:

$$\left(\frac{2}{1729}\right) = 1, \qquad 2^{(1729-1)/2} \equiv 1 \pmod{1729},$$

$$\left(\frac{3}{1729}\right) = 1, \qquad 3^{(1729-1)/2} \equiv 1 \pmod{1729},$$

$$\left(\frac{5}{1729}\right) = 1, \qquad 5^{(1729-1)/2} \equiv 1 \pmod{1729},$$

$$\left(\frac{11}{1729}\right) = -1, \qquad 11^{(1729-1)/2} \equiv 1 \pmod{1729}.$$

Zaključujemo da je broj 1729 složen, što on zaista i jeste, jer vrijedi da je $1729 = 7 \cdot 13 \cdot 19$. ◀

3.3 Miller – Rabinov test

Kombinirajući Mali Fermatov teorem i svojstvo kongruencije $x^2 \equiv 1 \pmod{p}$ (vidjeti [8], Teorem 2.2.9) dobivamo jači zahtjev od zahtjeva iz definicije pseudoprostih brojeva. Uzmimo da je n neparan prirodan broj i neka je b takav da je $\text{nzd}(b, n) = 1$ i $b^{n-1} \equiv 1 \pmod{n}$. Zbog parnosti od $n-1$ možemo pokušavati računati druge korijene iz navedene kongruencije, tj. potencirati b redom s $(n-1)/2, (n-1)/4, \ldots, (n-1)/2^s$ gdje je $t = (n-1)/2^s$ neparan.

Pretpostavimo da u i–tom koraku prvi put na desnoj strani dobijemo nešto različito od 1, tj. da je $b^{(n-1)/2^i} \equiv a \pmod{n}$. Ako je n prost tada je $a \equiv -1 \pmod{n}$, jer je $b^{(n-1)/2^{i-1}} \equiv 1 \pmod{n}$ a jedina rješenja kongruencije $x^2 \equiv 1 \pmod{p}$ su $x \equiv \pm 1 \pmod{p}$.

Definicija 3.7. *Neka je n neparan složen broj i neka je $n - 1 = 2^s \cdot t$ gdje je t neparan. Neka je b cijeli broj takav da je* $\text{nzd}(b, n) = 1$. *Ako vrijedi*

$$b^t \equiv 1 \pmod{n} \tag{3}$$

ili

$$\exists r,\ 0 \leq r < s,\ \text{takav da je } b^{2^r \cdot t} \equiv -1 \pmod{n} \tag{4}$$

onda kažemo da je n ***jaki pseudoprost broj u bazi*** *b u oznaci $spsp(b)$.*

Ako je $n = p$ prost onda on zadovoljava (3) ili (4) za svaki b, $1 < b < p$ za koji je $\text{nzd}(b, p) = 1$.

Ako je n jak pseudoprost broj u bazi b onda je on i Eulerov pseudoprost broj u bazi b (pa samim tim i pseudoprost u bazi b). Obrat ne vrijedi. Broj 1105 je epsp(2), ali nije spsp(2).

Teorem 3.4 (vidjeti [1]). *Neka je n neparan složen broj. Tada je n jak pseudoprost broj u bazi b za najviše $(n-1)/4$ mogućih baza b, gdje je $0 < b < n$.*

Ovaj teorem nam pokazuje da ni u slučaju jakih pseudoprostih brojeva ne postoji analogon Carmichaelovih brojeva jer je nemoguće da složen broj bude jak pseudoprost broj u svakoj bazi.

Neka je n veliki neparan pozitivan broj za kojeg želimo odrediti je li prost ili ne. Zapišemo $n - 1 = 2^s t$ gdje je t neparan i izaberemo slučajno b, $(0 < b < n)$. Najprije izračunamo $b^t \bmod n$ i ako dobijemo da je $b^t \equiv \pm 1 \pmod{n}$ onda zaključujemo da je n prošao test i na isti način biramo sljedeći b.

Ako je $b^t \not\equiv \pm 1 \pmod{n}$ onda kvadriramo b^t modulo n sve dok ne dobijemo rezultat -1. Ako dobijemo da je za neki r, $b^{2^r \cdot t} \equiv -1 \pmod{n}$, onda

je n prošao test i biramo sljedeći b. Međutim, ako nikad ne dobijemo $-1 \pmod{n}$ kao rezultat, tj. ako dobijemo da je $b^{2^{r+1}\cdot t} \equiv 1 \pmod{n}$, gdje je $b^{2^r \cdot t} \not\equiv -1 \pmod{n}$, onda smo sigurni da je n složen.

Ako n prođe test za svih k odabranih baza b, onda je vjerojatnost da je n složen manja od $1/4^k$. Iz toga, na sličan način kao i prije, zaključujemo da za broj k, koji predstavlja najmanji potreban broj različitih baza za koje n treba proći test da bismo s vjerojatnošću većom od p, $0 < p < 1$, tvrdili da je n prost, vrijedi

$$k = \left\lfloor \frac{\log_2 \frac{1}{1-p}}{2} \right\rfloor + 1.$$

Vidimo da nam je ovdje potrebno skoro 2 puta manje baza za postizanje iste vjerojatnosti kao kod prethodnih testova.

Primjer 3.4. *Ispitajmo s vjerojatnošću većom od* $0,9$ *jesu li brojevi* $1033, 1153$ *i* 1233 *prosti.*

Rješenje. Kako je

$$k = \left\lfloor \frac{\log_2 \frac{1}{1-0,9}}{2} \right\rfloor + 1 = 1 + 1 = 2$$

to imamo da su nam potrebne najmanje 2 različite baze.

a) Za baze uzmimo prva 2 prosta broja, tj. 2 i 3. Sada je

$$1033 - 1 = 1032 = 2^3 \cdot 129 \qquad \Rightarrow \qquad s = 3,\ t = 129.$$

Dobivamo da je

$$2^{129} \equiv 1032 \equiv -1 \pmod{1033}.$$

Imamo da je 1033 $\mathrm{spsp}(2)$.

Provjerimo li za bazu 3, dobivamo

$$3^{129} \equiv 355 \not\equiv \pm 1 \pmod{1033},$$

$$3^{2^1 \cdot 129} \equiv 1032 \equiv -1 \pmod{1033}.$$

Imamo da je 1033 također $\mathrm{spsp}(3)$ i zaključujemo s vjerojatnošću većom od $0,9$ da je broj 1033 prost, što on i jeste.

b) Za baze ponovo uzmimo prva 2 prosta broja, tj. 2 i 3. Sada imamo

$$1153 - 1 = 1152 = 2^7 \cdot 9 \qquad \Rightarrow \qquad s = 7,\ t = 9.$$

Dobivamo

$$\begin{aligned} 2^9 &\equiv 512 \not\equiv \pm 1 \pmod{1153}, \\ \\ 2^{2^1 \cdot 9} &\equiv 413 \not\equiv -1 \pmod{1153}, \\ 2^{2^2 \cdot 9} &\equiv 1078 \not\equiv -1 \pmod{1153}, \\ 2^{2^3 \cdot 9} &\equiv 1013 \not\equiv -1 \pmod{1153}, \\ 2^{2^4 \cdot 9} &\equiv 1152 \equiv -1 \pmod{1153}. \end{aligned}$$

Pokazali smo da je 1153 $\mathrm{spsp}(2)$. Provjerimo je li 1153 $\mathrm{spsp}(3)$. Kao i u prethodnom imamo

$$\begin{aligned} 3^9 &\equiv 82 \not\equiv \pm 1 \pmod{1153}, \\ \\ 3^{2^1 \cdot 9} &\equiv 959 \not\equiv -1 \pmod{1153}, \\ 3^{2^2 \cdot 9} &\equiv 740 \not\equiv -1 \pmod{1153}, \\ 3^{2^3 \cdot 9} &\equiv 1078 \not\equiv -1 \pmod{1153}, \\ 3^{2^4 \cdot 9} &\equiv 1013 \not\equiv -1 \pmod{1153}, \\ 3^{2^5 \cdot 9} &\equiv 1152 \equiv -1 \pmod{1153}. \end{aligned}$$

Imamo da je 1153 također $\mathrm{spsp}(3)$ i zaključujemo s vjerojatnošću većom od $0,9$ da je broj 1153 prost, što on i jeste.

c) Za baze ponovo uzmimo prva 2 prosta broja, tj. 2 i 3. Sada je

$$1233 - 1 = 1232 = 2^4 \cdot 77 \qquad \Rightarrow \qquad s = 4,\ t = 77.$$

Analogno prethodnom slijedi da je

$$\begin{aligned} 2^{77} &\equiv 923 \not\equiv \pm 1 \pmod{1233}, \\ \\ 2^{2^1 \cdot 77} &\equiv 1159 \not\equiv -1 \pmod{1233}, \\ 2^{2^2 \cdot 77} &\equiv 544 \not\equiv -1 \pmod{1233}, \\ 2^{2^3 \cdot 77} &\equiv 16 \not\equiv -1 \pmod{1233}. \end{aligned}$$

Imamo da 1233 u bazi $b = 2$ ne zadovoljava (3). Također ne postoji $0 \leq r < 4 = s$ tako da je za $b = 2$ zadovoljena relacija (4). Zaključujemo da broj 1233 nije prošao test u bazi $b = 2$ pa nije spsp(2). Sada smo sigurni da je 1233 složen broj. Vrijedi $1233 = 3^2 \cdot 137$. ◀

Literatura

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

[2] A. Dujella, *Kriptografija*, Skripta, `web.math.pmf.unizg.hr/$\sim$duje/kript/kriptografija.html`

[3] L. K. Hua, *Introduction to Number Theory* (translated by P. Shiu), Springer–Verlag, Berlin–Heidelberg–New York, 1982.

[4] B. Ibrahimpašić, *Uvod u teoriju brojeva*, Pedagoški fakultet, Bihać, 2014.

[5] B. Ibrahimpašić, *Kongruencije oblika* $x^n \equiv 0 \pmod{m}$, Osječki matematički list, Vol 15 $(1)(2015)$, 33–40.

[6] B. Ibrahimpašić, S. Ibrahimpašić, D. Kovačević, A. Šehanović, *Pravila djeljivosti*, Osječki matematički list, Vol 11 $(2)(2011)$, 107–112.

[7] R. Solovay, V. Strassen, *A Fast Monte–Carlo Test for Primality*, SIAM Journal for Computing, **6**(1) (1977), 84–85.

[8] S.Y. Yan, *Number Theory for Computing*, Springer–Verlag, Berlin, Heidelberg, 2002.

[9] S. Y. Yan, *Primality Testing and Integer Factorization in Public–Key Cryptography*, Springer–Verlag, New York, 2009.