Testiranje i dokazivanje prostosti i primjene rezultata u kriptografiji

Kokotec-Lovrek, Alen

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Alen Kokotec-Lovrek

TESTIRANJE I DOKAZIVANJE PROSTOSTI I PRIMJENE REZULTATA U KRIPTOGRAFIJI

ZAVRŠNI RAD

Varaždin, 2018.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Alen Kokotec-Lovrek

Matični broj: 43373/14–R

Studij: Informacijski sustavi

TESTIRANJE I DOKAZIVANJE PROSTOSTI I PRIMJENE REZULTATA U KRIPTOGRAFIJI

ZAVRŠNI RAD

Mentor:

doc. dr. sc. Marcel Maretić

Varaždin, rujan 2018.

Alen Kokotec-Lovrek

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada i da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada korištene su etički prikladne i prihvatljive metode i tehnike rada.

Autor potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Tema ovog rada je testiranje prostosti. Dovoljna je pseudoprostost, tj. da znamo da je broj vrlo vjerojatno prost. Faktorizacija većih brojeva na proste faktore nije jednostavna. Objašnjeni su pojmovi prostih brojeva, same pseudoprostosti u bazi i jake pseudoprostosti u bazi, kongruencije, Eulerove funkcije, modularnog potenciranja. Obrađeni su Legendreov i Jacobijev simbol za potrebe testova prostosti. Središnji dio rada su probabilistički testovi prostosti kojima se ispituje prostost broja zadovoljavajućom točnošću. Radi se o Fermatovom testu, Solovay-Strassenovom testu i Miller-Rabinovom testu. Testovi su objašnjeni i algoritamski, također su potkrijepljeni primjerima izračuna. Naposlijetku, veliki pseudoprosti ili prosti brojevi nalaze primjenu u kriptografiji kako bi se poruke prenosile na što sigurniji način.

Ključne riječi: teorija brojeva; prosti brojevi; pseudoprosti brojevi; testovi prostosti; kriptografija;

Sadržaj

1. Predgovor

Tema ovog rada je testiranje prostosti. Radi se o području teorije brojeva, a smisao je u provjeri velikih brojeva. U prvom dijelu rada objašnjeno je sve potrebno za testove prostosti. Radi se o prostim brojevima, modularnom potenciranju, Legendreovom i Jacobijevom simbolu. Središnji dio rada su probabilistički testovi prostosti: Fermatov test, Solovay-Strassenov test i Miller-Rabinov test. Naposljetku, veliki brojevi povezani su s kriptografijom radi teže faktorizacije ukoliko je uopće moguća, što implicira sigurnost prenošene poruke.

Svrha rada je sustavnim proučavanjem literature objasniti predmet rada, kao i potrebno predznanje za razumijevanje testova. Sve to zajedno je uobličeno u jednu cjelinu zajedno s primjerima ili dodatnim objašnjavanjem i konkretnom implementacijom u programskom kodu.

1.1. Metode i tehnike rada

Kod obrade sadržaja korištene su knjige kao literatura. Tri izvora (jedna knjiga, dvije skripte) su na hrvatskom jeziku, sve ostalo (knjige) je na engleskom jeziku. Za implementaciju korišten je programski jezik Python. Rad je strukturiran tako da su za neku metodu objašnjeni potrebni pojmovi, činjenice i pretpostavke. Većina teorema je preuzeta bez dokaza, a za sve važnije tvrdnje dan je dokaz. Metode su potkrijepljene primjerima izračuna.

Rad je podijeljen u 6 poglavlja, gdje je ovo uvodno poglavlje. U drugom poglavlju objašnjeni su prosti brojevi, osnovni teorem aritmetike, problem faktorizacije broja na proste faktore i Eratostenovo sito. Dani su primjeri velikih brojeva i predočen broj prostih brojeva. Nadalje su obrađeni pseudoprosti brojevi u bazi i jaki pseudoprosti brojevi u bazi, Eulerova funkcija, kongruencije, kvadratni ostaci. Obrađeni su Legendreov i Jacobijev simbol kao potrebno za same testove prostosti koje rad obuhvaća, zajedno s detaljnim primjerom izračuna Jacobijevog simbola. U trećem poglavlju objašnjeno je algoritamsko računanje modularnog potenciranja uz jedan primjer izračuna.

Kod četvrtog, središnjeg poglavlja rada objašnjeni su Fermatov test, Solovay-Strassenov test, Miller-Rabinov test kao probabilistički testovi prostosti, spomenuti su brojevi specijalnog oblika. Svaka metoda je opisana i iznešena algoritamski. Dani su primjeri provjere prostosti broja. Nadalje je ukratko objašnjeno generiranje prostih brojeva i vjerojatnost zadovoljavajućeg odabira. Mali Fermatov teorem je iz 17. stoljeća, dok su druge dvije metode iz 20. stoljeća.

U petom poglavlju nalaze se implementacije testova, modularnog potenciranja i izračuna Jacobijevog simbola. Na kraju u šestom poglavlju, dan je zaključak s kratkim osvrtom na kriptografiju i sigurnost prijenosa poruke u vezi s faktorizacijom velikih brojeva.

Na kraju rada je navedena korištena literatura.

2. Prosti brojevi

Prost ili prim broj $p > 1$ je onaj koji je djeljiv s 1 i sa samim sobom, dok je broj složen ako nije prost i može se rastaviti na proste faktore. Broj 1 nije ni prost ni složen broj. Relativno prosti brojevi su oni koji nemaju zajedničkih djelitelja, to jest najveći zajednički djelitelj im je 1.

Teorem 1. Svaki $n > 1, n \in \mathbb{N}$ može se prikazati kao produkt prostih brojeva.

Teorem 2 (Osnovni teorem aritmetike). Faktorizacija prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Ako grubom silom ispitujemo prostost, dovoljno je provjeriti brojeve do drugog korijena broja za koji želimo saznati status, odnosno prosti faktori broja su manji ili jednaki od njegovog drugog korijena.

Teorem 3. Složeni prirodni broj b ima prosti faktor $p \leq \sqrt{b}$.

Dokaz. Neka je $b > 1, b \in \mathbb{N}$ složen broj: $b = mn,\ 1 < m, n < b,\ m, n \in \mathbb{N}$. Ako pretpostavimo suprotno da je $m, n > \sqrt{b}$ tada je $mn > \sqrt{b}\sqrt{b}$. Kako $b \not> b$ pretpostavka ne vrijedi i mora biti suprotno, to jest prosti faktor broja je manji ili jednak $\sqrt{b}$. □

Teorem 4 (Teorem o prostim brojevima). Neka je π broj prostih brojeva manjih ili jednakih x. Aproksimacija za broj prostih brojeva je $\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$, to jest $\pi(x) \sim \frac{x}{\ln x}$.

Vjerojatnost da je broj manji od n prost, obrnuto je proporcionalna broju znamenaka od n.

Primjer 1. Želimo li ispitati prostost broja 119, potrebno je provjeriti je li broj djeljiv kojim prirodnim brojem iz $[2, \sqrt{119} \approx 10]$. Možemo krenuti redom i zaključiti da je broj složen jer je djeljiv s brojem 7.

Eratostenovo sito

Jedan jednostavan, ali ne previše efikasan način pronalaženja prostih brojeva do željenog broja je Eratostenovo sito. Ispišu se svi brojevi do željenog broja i ponavlja se postupak zaokruživanja prvog prostog broja (zapravo prvo neprecrtani broj) i precrtavanja njegovih

višekratnika, sve dok se ne dođe do korijena tog zadanog broja. Zaokruženi i neprecrtani brojevi nakon obavljenog postupka su prosti brojevi.

U Tablici 1 je prikazan broj prostih brojeva do određenog 10^k. Najveća izračunata vrijednost spomenute funkcije je za 10^{20}.

Tablica 1: Broj prostih brojeva (prema: Rosen et al., 2000)

k	$\pi(10^k)$
1	4
2	25
3	168
4	1 229
5	9 592
⋮	⋮
11	4 118 054 813
12	37 607 912 018
13	346 065 536 839
⋮	⋮
18	24 739 954 287 740 860
19	234 057 667 276 344 607
20	2 220 819 602 560 918 840

2.1. Veliki brojevi

Ljudi općenito imaju lošu percepciju o duljini broja, odnosno vrijednosti koju on predstavlja. U Tablici 2 su primjeri velikih brojeva koji ugrubo predstavljaju veličine.

Tablica 2: Veliki brojevi (prema: Schneier, 1996)

veličina	**baza 10**	**baza 2**
visina čovjeka (metara)	$10^{1/3}$	2^1
starost planeta (godina)	10^9	2^{30}
starost Sunca (godina)	10^{10}	2^{34}
broj atoma na Zemlji	10^{51}	2^{170}
broj atoma Sunca	10^{57}	2^{190}

Primjer 2. Uzmimo da imamo računalo konfiguracije takve da može grubom silom provjeravati prostost broja provjerom milijun brojeva u sekundi. Recimo da taj broj ima 128 bita, odnosno onda je n toliko dug, a $n \approx 2^{128}$. Prema tome, potrebno je u najgorem slučaju ispitati brojeve do $\sqrt{2^{128}} = 2^{64}$ ili samo neparne brojeve, pa ih je $2^{64} : 2 = 2^{63}$. Vrijeme potrebno za završetak posla je $\frac{2^{63}b}{10^6 b/s} \approx 9{,}22 \cdot 10^{12} s$. Možemo reći da će se raditi o približno $292\,364$ godina. Iz toga se može zaključiti da korištenje velikih prostih brojeva daje određenu sigurnost kod neželjenog napada.

2.2. Kongruencije. Kvadratni ostaci

Definicija 1. Ako vrijedi $m|(a-b)$ za $m \in \mathbb{Z}, m \neq 0$, onda je a kongruentan b modulo m **(▲)** i tada pišemo $a \equiv b (\mathrm{mod}\, m)$. U protivnom ako ne vrijedi, tada a nije kongruentan b modulo m i označava se s $a \not\equiv b (\mathrm{mod}\, m)$.

Relacija **(▲)** je relacija ekvivalencije na skupu $\mathbb{Z}$ (vrijedi refleksivnost, simetričnost i tranzitivnost).

Označimo najveću zajedničku mjeru brojeva m i n s $M(m,n)$. Teorem o dijeljenju kongruencija naveden je bez dokaza:

Teorem 5. Za brojeve $a, x, y, n \in \mathbb{N}$ vrijedi $ax \equiv ay (\mathrm{mod}\, n) \Leftrightarrow x \equiv y (\mathrm{mod}\, \frac{n}{M(a,n)})$.

Definicija 2. Neka su cijeli brojevi a i m takvi da je $M(a,m) = 1$. Ako vrijedi

$$x^2 \equiv a (\mathrm{mod}\, m),$$

tada se a naziva **kvadratnim ostatkom** modulo m, u suprotnom radi se o **kvadratnom neostatku**.

Teorem 6. Ukoliko je p neki neparan prost broj, reducirani sustav ostataka modulo p sastoji se od $\frac{p-1}{2}$ kvadratnih ostataka i također $\frac{p-1}{2}$ kvadratnih neostataka (Dujella, 2018a).

Dokaz. Svaki kvadratni ostatak modulo p kongruentan je nekom od $-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}$, to jest nekom od $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Pretpostavimo da je $k^2 \equiv l^2 (\mathrm{mod}\, p), 1 \leq k < l \leq \frac{p-1}{2}$, pa je tada $(l-k)(l+k) \equiv 0 (\mathrm{mod}\, p)$; $l - k \equiv 0 (\mathrm{mod}\, p)$ ili $l + k \equiv 0 (\mathrm{mod}\, p)$

što je suprotno od pretpostavljenog jer je $0 < l - k < p,\ 0 < l + k < p$. □

2.3. Pseudoprostost

U nekim slučajevima dovoljno je pokazati da je broj pseudoprost odnosno vrlo vjerojatno prost. Sam taj pristup ubrzava ispitivanje za razliku od nekog konkretnog testa koji će reći da je broj sigurno prost. Kod kriptiranja ako su recimo brojevi tajni i velikog broja znamenki, dovoljna je pseudoprostost. Ako broj zadovolji provjere prostosti onda je vjerojatno prost i to s onolikom vjerojatnošću koliko je test intenzivno proveden, odnosno koliko je puta ispitivano ili ugrubo rečeno, ako smo nešto više puta provjerili za različit izbor parametara, sigurno je vjerojatnost istinitog zaključka veća. Dakle, povećavanjem broja ispitivanja povećava se vjerojatnost točnosti, a ukoliko test ne prolazi za samo jedan izbor parametara, radi se o složenom broju. Ovdje se onda dalje otvara problem faktorizacije tog broja na proste faktore.

Definicija 3. Složen broj n je **pseudoprost** u bazi b ako je $b^n \equiv b (\mathrm{mod}\, n)$.

Propozicija 1. Pseudoprostih brojeva u bazi b ima beskonačno za svaki prirodni broj $b > 2$.

Dokaz. Neka je p neparan prost broj, takav da $p \nmid b^2 - 1$ i složen broj $n = \frac{b^{2p}-1}{b^2-1}$.

$n = \frac{b^p-1}{b-1} \cdot \frac{b^p+1}{b+1}$, iz Malog Fermatovog teorema slijedi $b^{2p} \equiv b^2 (\mathrm{mod}\, p) \Rightarrow p | b^{2p} - b^2 = (b^p - b)(b^p + b)$.

$$b^{2p} - b^2 = b^{2p} - b^2 + 1 - 1 = (b^{2p} - 1) - (b^2 - 1)$$

$$= \frac{(b^{2p} - 1)(b^2 - 1) - (b^2 - 1)(b^2 - 1)}{b^2 - 1}$$

$$= \frac{b^2(b^{2p} - 1) - (b^{2p} - 1) - b^2(b^2 - 1) + b^2 - 1}{b^2 - 1}$$

$$= b^2 \cdot \frac{b^{2p} - 1}{b^2 - 1} - \frac{b^{2p} - 1}{b^2 - 1} - b^2 + 1$$

$$= \left(\frac{b^{2p} - 1}{b^2 - 1} - 1\right)(b^2 - 1)$$

$$= (n - 1)(b^2 - 1)$$

Iz pretpostavke slijedi da je $p | n - 1$. $n - 1$ je suma $p - 1$ pribrojnika iste parnosti, pa je $n - 1$ paran, znači $2p | n - 1;\ n | b^{2p} - 1 \Rightarrow n | b^{n-1} - 1 \Rightarrow b^n \equiv b (\mathrm{mod}\, n)$ što je i zahtjev pseudoprostog broja u bazi b. □

Primjer 3. Broj 91 je pseudoprost u bazi 3 jer je

$$3^{90} \equiv 27^{30} \equiv (-1)^{30} \equiv 1 (\mathrm{mod}\ 7),$$

$$3^{90} \equiv 27^{30} \equiv 1^{30} \equiv 1 (\mathrm{mod}\ 13).$$

Stoga je $3^{91-1} \equiv 1 (\mathrm{mod}\ 91), 3^{90} \equiv 1 (\mathrm{mod}\ 91)$. Također vrijedi $3^{91} \equiv 3 (\mathrm{mod}\ 91)$.

Definicija 4. Neka je n neparan složen broj takav da je $n - 1 = 2^s t$ gdje je t neparan. Broj n je **jak pseudoprost** broj u bazi b, ako za $b \in \mathbb{Z}$ vrijedi $b^t \equiv 1 \ (\mathrm{mod}\ n)$ ili $\exists\, r, 0 \leq r < s,\ b^{2^r t} \equiv -1 (\mathrm{mod}\ n)$.

Ako disjunkcija ne daje pozitivan odgovor za neku bazu $0 < b < n$, onda je ispitivani broj sigurno složen, a ta baza (broj) svjedok složenosti. Nije moguće da složen broj bude jak pseudoprost broj u svakoj bazi (Koblitz, 1994).

2.4. Legendreov i Jacobijev simbol

Definicija 5. Neka je $x \in \mathbb{N}$ i prost broj $p > 2$. Za Legendreov simbol $\left(\frac{x}{p}\right)$ vrijedi:

$$\left(\frac{x}{p}\right) = \begin{cases} 0, & x \equiv 0 (\mathrm{mod}\ p) \\ 1, & \exists y: x \equiv y^2 (\mathrm{mod}\ p) \\ -1, & \text{ostali slučajevi} \end{cases}$$

Drugim riječima, Legendreov simbol je 0 ako je broj x djeljiv brojem p. U drugom slučaju je 1 ako je x kvadratni ostatak modulo p, dok je -1 za ostale slučajeve, odnosno za x kvadratni neostatak modulo p.

Definicija 6. Neka je $n \in \mathbb{N}$ neparan broj čija je faktorizacija na proste faktore $n = \prod_{i=1}^{k} {p_i}^{\alpha_i}$. Jacobijev simbol je

$$\left(\frac{x}{n}\right) = \prod_{i=1}^{k} \left(\frac{x}{p_i}\right)^{\alpha_i},$$

gdje $\left(\frac{x}{p_i}\right)$ predstavlja Legendreov simbol.

Ako je broj n prost, Legendreov i Jacobijev simbol se podudaraju. Ako je $M(x, n) > 1$ tada je $\left(\frac{x}{n}\right) = 0$, a inače je Jacobijev simbol iz skupa $\{-1, 1\}$ (Buchmann, Müller, 1992).

Svojstva za računanje Jacobijevog simbola navedena su bez dokaza:

Propozicija 2. Svojstva za računanje Jacobijevog simbola (Dujella, 2018b):

1) $a \equiv b (\mathrm{mod}\, p) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),\ \left(\frac{a}{pq}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$

3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & p \equiv 1 (\mathrm{mod}\, 4) \\ -1, & p \equiv 3 (\mathrm{mod}\, 4) \end{cases}$

4) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & p \equiv 1,7 (\mathrm{mod}\, 8) \\ -1, & p \equiv 3,5 (\mathrm{mod}\, 8) \end{cases}$

Teorem 7 (Gaussov kvadratni zakon reciprociteta). Ako su p i q, $p \neq q$ neparni prosti brojevi, onda vrijedi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Primjer 4. Izračunajmo Jacobijev simbol $\left(\frac{51}{71}\right)$.

$J = \left(\frac{51}{71}\right) = -\left(\frac{71}{51}\right)$ prema Gaussovom zakonu reciprociteta.

$-\left(\frac{71}{51}\right) = -\left(\frac{20}{51}\right)$ jer je $71 \equiv 20 (\mathrm{mod}\, 51)$.

$-\left(\frac{20}{51}\right) = -\left(\frac{2}{51}\right)\left(\frac{10}{51}\right)$ prema Propoziciji 2.2.

Nadalje $J = 1 \cdot \left(\frac{10}{51}\right)$ prema Propoziciji 2.4.

Slično dalje $J = \left(\frac{2}{51}\right)\left(\frac{5}{51}\right) = -1 \cdot \left(\frac{5}{51}\right) = -\left(\frac{51}{5}\right)$.

$J = -\left(\frac{1}{5}\right)$ jer je $51 \equiv 1 (\mathrm{mod}\, 5)$.

$-\left(\frac{1}{5}\right) = -\left(\frac{-1}{5}\right)\left(\frac{-1}{5}\right)$.

Konačno je prema Propoziciji 2.3: $J = -1 \cdot 1 \cdot 1 = -1$.

2.5. Eulerova funkcija. Eulerov kriterij

Definicija 7 (Eulerova funkcija). Funkcija $\varphi: \mathbb{N} \to \mathbb{N}$ predstavlja broj prostih brojeva u nizu do n koji su relativno prosti s n.

Definicija 8. Reducirani sustav ostataka modulo n je skup brojeva $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$, $r_i \in \mathbb{Z}$ takvih da su r_i i n relativno prosti i $r_i \not\equiv r_j (\mathrm{mod}\, n)$ za $i \neq j$, također za svaki $x \in \mathbb{Z}$ relativno prost s n postoji r_i takav da je $x \equiv r_i (\mathrm{mod}\, n)$.

Reducirani sustav ostataka modulo n dobije se tako da se izbace iz niza svi brojevi (ostaci) koji nisu relativno prosti s n.

Propozicija 3 (Eulerov kriterij). Neka je n neparan prost broj. Ako za broj $b \in \mathbb{Z}$ vrijedi da je $M(b,n) = 1$, tada je

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n.$$

Dokaz.

1° Ako je Jacobijev simbol $\left(\frac{b}{n}\right) = 0$, tada $n|b$ i kriterij je zadovoljen.

2° Ako je $\left(\frac{b}{n}\right) = 1$, onda $\exists x \in \mathbb{Z}: x^2 \equiv b (\bmod n)$. Iz Malog Fermatovog teorema slijedi da je $b^{\frac{n-1}{2}} \equiv x^{n-1} \equiv 1 \equiv \left(\frac{b}{n}\right) (\bmod n)$.

3° Pretpostavimo da je $\left(\frac{b}{n}\right) = -1$. $b^{n-1} - 1 \equiv \left(b^{\frac{n-1}{2}} - 1\right)\left(b^{\frac{n-1}{2}} + 1\right) \bmod n$, pa je vrijednost od $b^{\frac{n-1}{2}} \bmod n$ jednaka -1. □

Teorem 8 (Eulerov teorem). Ako je najveća zajednička mjera dvaju brojeva jednaka 1, to jest ako su oni relativno prosti, tada za $a, n \in \mathbb{N}$ vrijedi:

$$a^{\varphi(n)} = 1 (\bmod n).$$

Dokaz. Neka je $\{r_1, r_2, \dots, r_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. $\{ar_1, ar_2, \dots, ar_{\varphi(n)}\}$ je također reducirani sustav ostataka modulo n i vrijedi da je $M(a,n) = 1$, slijedi da je

$$\prod_{j=1}^{\varphi(n)} ar_j \equiv \prod_{i=1}^{\varphi(n)} r_i (\bmod n)$$

$$a^{\varphi(n)} \prod_{j=1}^{\varphi(n)} r_j \equiv \prod_{i=1}^{\varphi(n)} r_i (\bmod n).$$

Prema $M(r_i, n) = 1 \Rightarrow M\left(\prod_i^{\varphi(n)} r_i, n\right) = 1$ i Teoremu 5 slijedi da je

$$a^{\varphi(n)} \equiv 1 \left(\bmod \frac{n}{M\left(\prod_i^{\varphi(n)} r_i, n\right)} \right),$$

$$a^{\varphi(n)} \equiv 1 (\bmod n).$$ □

Korolar 1. Ako je broj $p \in \mathbb{N}$ prost, tada je $\varphi(p) = p - 1$.

2.5.1. Eulerovi pseudoprosti brojevi u bazi

Definicija 9. Eulerov pseudoprost broj u bazi b je neparan složen broj n takav da je $M(b,n) = 1$ i koji zadovoljava Eulerov kriterij $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n$.

Propozicija 4. Ako je broj Eulerov pseudoprost u bazi b, tada je broj i pseudoprost u bazi b.

Dokaz. Lako je vidljivo dok se pokaže da iz Eulerovog kriterija slijedi Mali Fermatov teorem.

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

$b^{n-1} \equiv 1 (\bmod n)$ □

3. Modularno potenciranje

Definicija 10. Ako je $r = a^k \bmod n$, tada vrijedi $a^k \cdot s + r = n$, gdje je r ostatak pri dijeljenju a^k brojem n.

Potrebno je izračunati vrijednost $a^k \bmod n, a \in \mathbb{Z}_n$, $0 \leq k < n$ tako da je $k = \sum_{i=0}^{t} k_i 2^i$ binarna reprezentacija eksponenta. Efikasan način za to provesti je polinomijalan algoritam (Menezes et al., 1996):

Algoritam 1. Modularno potenciranje

1. $b \leftarrow 1$
2. *ako* $k = 0$ *vrati* (b)
3. $A \leftarrow a$
4. *ako* $k_0 = 1 : b \leftarrow a$
5. *za* i *od* 1 *do* t *radi:*
   5.1. $A \leftarrow A^2 \ mod \ n$
   5.2. *ako* $k_i = 1$ *tada* $b \leftarrow A \cdot b \ mod \ n$
6. *vrati* (b)

Primjer 5. Recimo da želimo izračunati $7^{712} \bmod 1234 = 1183$. U Tablici 3 je prikazano stanje u varijablama nakon određene iteracije. Rezultat je sama vrijednost ključne varijable u zadnjem stupcu tablice.

Tablica 3: Prikaz rezultata za primjer modularnog potenciranja

i	0	1	2	3	4	5	6	7	8	9
k_i	0	0	0	1	0	0	1	1	0	1
A	7	49	1167	787	1135	1163	105	1153	391	1099
b	1	1	1	787	787	787	1191	1015	1015	**1183**

4. Probabilistički testovi prostosti

Probabilističkim testovima prostosti zaključuje se prostost broja s određenom vjerojatnošću. Ima smisla provjeravati prostost neparnih brojeva. Ako razmišljamo algoritamski, postavljamo pitanje je li broj prost. Tada testiranje može dati samo pozitivan ili negativan odgovor. Ukoliko je odgovor pozitivan, broj je vjerojatno prost odnosno pseudoprost. Ukoliko je odgovor negativan, broj je sigurno složen odnosno sigurno nije prost. Takvi testovi se temelje na iteriranju tako da se za svaku iteraciju provjerava neka relacija za nasumično odabrani broj poštujući ograničenja. Povećavanjem broja iteracija povećava se vjerojatnost prostosti.

4.1. Brojevi specijalnog oblika

Definicija 11. Neka je n složen broj. Broj n je **Carmichaelov broj** ako zadovoljava relaciju

$$b^{n-1} \equiv 1 (\mathrm{mod}\ n)$$

za svaki broj b relativno prost s n.

Teorem 9 (Korseltov kriterij). Broj n je Carmichaelov broj ako i samo ako je složen, kvadratno slobodan i za svaki njegov prosti faktor p vrijedi $p-1|n-1$.

Propozicija 5. Carmichaelov broj se može prikazati kao umnožak najmanje tri prosta faktora.

Najmanji Carmichaelov broj je $561 = 3 \cdot 11 \cdot 17$.

Primjer 6. Pokažimo da je broj 6601 Carmichaelov broj. Spomenuti broj je kvadratno slobodan i složen s faktorizacijom na proste faktore $6601 = 7 \cdot 23 \cdot 41$. Vrijedi dakle Korseltov kriterij jer je:

$$7-1|6601-1,$$
$$23-1|6601-1,$$
$$41-1|6601-1.$$

Definicija 12. Brojevi oblika $2^{2^{n-1}}+1$ nazivaju se **Fermatovim brojevima**. Oni koji su prosti takvog oblika su Fermatovi prosti brojevi.

Prvih nekoliko Fermatovih brojeva je $3, 5, 17, 257, 65\,537, 4\,294\,967\,297$. Već za $n = 6$ broj $4\,294\,967\,297$ je složen.

4.2. Fermatov[1] test prostosti

Teorem 10 (Mali Fermatov teorem). Neka je $n \in \mathbb{N}$ prost broj. Vrijedi $b^{n-1} \equiv 1 (\mathrm{mod}\, n)$ za svaki broj $b \in \mathbb{Z}$.

Dokaz. Prema Eulerovom teoremu je $b^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$, a kako se radi prostom broju n, vrijedi iz Korolara 1 da je $\varphi(n) = n - 1$. Stoga slijedi da je $b^{n-1} \equiv 1 (\mathrm{mod}\, n)$. □

Ako je n neparan složen broj, vrijedi Mali Fermatov teorem i najveća zajednička mjera $M(b, n)$ je jednaka 1 (relativno prosti brojevi), onda je taj broj pseudoprost u bazi b.
Ispitivanje se vrši slučajnim odabirom baze $0 < b < n$, i $d = M(n, b)$. Sada se mogu pojaviti dvije mogućnosti. Prva je da je $d > 1$ i onda znači da je ispitivani broj sigurno složen i nema potrebe za daljnjim ispitivanjem. Druga je da je $d = 1$, i tada se b potencira na $(n - 1)$. Ukoliko test nije zadovoljen, ispitivani broj je sigurno složen, a ukoliko je zadovoljen, može se prijeći na sljedeću slučajno odabranu bazu po spomenutom ograničenju. Što se postupak više puta ponavlja, smanjuje se vjerojatnost da je broj složen, odnosno povećava vjerojatnost da je broj prost (Crandall, Pomerance, 2001).

Algoritam 2. Fermatov test prostosti

1. *za i od 1 do t radi:*
   - *1.1. slučajno odabrati $a, 2 \leq a \leq n - 2$*
   - *1.2. $r \leftarrow a^{n-1} \bmod n$*
   - *1.3. ako $r \neq 1$ vrati „složen“*
2. *vrati „prost“*

Iteracija se provodi do željenog broja baza za testiranje i za svaku se generira slučajan broj iz zadanog intervala.

Propozicija 6. Ako Fermatov test prostosti ne daje pozitivan odgovor za neku bazu b, tada testirani broj ne prolazi test za najmanje polovicu mogućih baza.

Dokaz. Neka je skup $\{b_1, b_2, \dots, b_k\}$ skup baza za koje je testirani broj n pseudoprost. Ako je b baza za koji broj ne prolazi test i n pseudoprost za baze bb_i, tada je i pseudoprost za $b \equiv (bb_i){b_i}^{-1} \bmod n$ što nije istina. Prema tome onda broj ne prolazi test za $\{bb_1, bb_2, \dots, bb_k\}$. Za isti broj baza testiranje daje pozitivan odgovor, za isti broj baza ispitivanje daje negativan

[1] Pierre de Fermat, francuski pravnik i matematičar, 17. stoljeće

odgovor, pa je vjerojatnost pada testa odnosno da je broj složen 50% do trenutnog slučaja (što se kasnije potencira na željeni broj testiranja) (Koblitz, 1994). □

Primjer 7. Provjerimo Fermatovim testom prostosti je li broj 2553 prost. Prvo slučajno odabiremo broj $a, 2 \leq a \leq n-2, a = 158$. Računamo

$$r = 158^{2552} \bmod 2553 = 2209.$$

Kako prema tome ne vrijedi $a^{n-1} \equiv 1 (\bmod n)$, odnosno $r \neq 1$, zaključak je da je broj sigurno složen. Sada je broj 158 svjedok složenosti ispitivanog broja. Sam test ne daje faktorizaciju broja $2553 = 3 \cdot 23 \cdot 37$.

Primjer 8. Provjerimo Fermatovim testom prostosti je li broj 2557 prost pretpostavljajući da ne znamo da se sigurno radi o prostom broju. Slučajno odabiremo broj $a, 2 \leq a \leq n-2, a = 158$. Računamo

$$r = 158^{2556} \bmod 2557 = 1.$$

Kako vrijedi $a^{n-1} \equiv 1 (\bmod n)$, može se prijeći na sljedeći slučajno odabrani a. Recimo, dalje je također za $a = 1375$,

$$r = 1375^{2556} \bmod 2557 = 1.$$

Za sada je zaključak da je broj pseudoprost, a analogno dalje ponavljanjem testa povećava se vjerojatnost da je ispitivani broj prost.

Primjer 9. Kako je vjerojatnost da je ispitivani broj složen (u slučaju k uspješnih prolazaka testova) $\frac{1}{2^k}$ odnosno da je prost $1 - \frac{1}{2^k}$, za 10 uspješno testiranih baza, vjerojatnost da je broj prost je

$$\left(1 - \frac{1}{2^{10}}\right) \cdot 100\% \approx 99{,}9023\%.$$

4.3. Solovay[2]-Strassenov[3] test prostosti

Solovay-Strassenov test prostosti zasnovan je na Eulerovim pseudoprostim brojevima. Neka je $n \in \mathbb{N}$ neparni broj. Treba slučajno odabrati bazu $0 < b < n$ i računati obje strane od $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \bmod n$. Ako je uvjet zadovoljen, može se prijeći na sljedeću slučajno odabranu bazu, ako nije zadovoljen, tada je n sigurno složen.

[2] Robert Martin Solovay, američki matematičar;
[3] Volker Strassen, njemački matematičar;

Propozicija 7. Vjerojatnost za da je broj složen za k uspješno ispitanih baza je $\frac{1}{2^k}$ (Stinson, 2006).

Algoritam 3. Solovay-Strassenov test prostosti

1. *za* i *od* 1 *do* t *radi:*
   - 1.1. *slučajno odabrati* $a, 2 \leq a \leq n-2$
   - 1.2. $r \leftarrow a^{\frac{n-1}{2}} \bmod n$
   - 1.3. *ako* $r \neq 1$ *i* $r \neq n-1$ *vrati „složen“*
   - 1.4. $s = \left(\frac{a}{n}\right)$
   - 1.5. *ako* $r \not\equiv s \pmod n$ *vrati „složen“*
2. *vrati „prost“*

Iteracija se provodi do željenog broja baza za testiranje i za svaku se slučajno generira broj iz zadanog intervala. s predstavlja Jacobijev simbol.

Primjer 10. Ispitajmo Solovay-Strassenovim testom prostosti je li broj 221 prost. Slučajno odabiremo $a = 174$, pa prvo računamo

$$r = 174^{\frac{221-1}{2}} \bmod 221 = -1 \bmod 221.$$

Dalje računamo Jacobijev simbol

$$\left(\frac{174}{221}\right) = \left(\frac{2}{221}\right)\left(\frac{87}{221}\right) = -\left(\frac{87}{221}\right) = -\left(\frac{29}{221}\right)\left(\frac{3}{221}\right) = -\left(\frac{221}{29}\right)\left(\frac{221}{3}\right) = -1.$$

Kako znamo da su 29 i 3 prosti brojevi, Jacobijev i Legendreov simbol se podudaraju pa je opet

$$\left(\frac{174}{221}\right) \bmod 221 = -1 \bmod 221.$$

Za sada tvrdimo pseudoprostost ispitivanog broja. Nadalje, slučajno odaberimo $a = 38$. Računamo

$$r = 38^{\frac{221-1}{2}} \bmod 221 = 118\ (\bullet).$$

Dalje računamo Jacobijev simbol

$$\left(\frac{38}{221}\right) = \left(\frac{2}{221}\right)\left(\frac{19}{221}\right) = -\left(\frac{221}{19}\right) = -(-1) = 1,$$

pa je

$$\left(\frac{38}{221}\right) \bmod 221 = 1 \bmod 221\ (\circ).$$

Zbog (●) i (○) zaključak je da je ispitivani broj složen i da je broj 38 svjedok složenosti. Test ne daje faktorizaciju broja $221 = 13 \cdot 17$.

4.4. Miller[4]-Rabinov[5] test prostosti

Miller-Rabinov test prostosti temelji se na jakim pseudoprostim brojevima. Neka je $n \in \mathbb{N}$ neparan broj koji se ispituje. Potrebno je zapisati $n - 1 = 2^s t$, gdje je t neparan. Nadalje treba slučajno izabrati bazu $0 < b < n$ i računati $b^t \bmod n$.
Ako je $b^t \bmod n = 1$ ili $b^t \bmod n = n - 1$, tada test prolazi i može se prijeći ne sljedeću bazu. Ukoliko nije zadovoljen prethodni zahtjev, treba kvadrirati $b^t \bmod n$, pa tako dalje kvadrirati do kada se ne dobije -1. Ako se dakle uspije dobiti -1, tada test prolazi i može se prijeći na odabir sljedeće baze, ukoliko se ne dobije -1, $b^{2^{r+1}} \equiv 1 (\bmod n)$ dok također vrijedi $b^{2^r} \not\equiv -1 (\bmod n), 0 \leq r < s$, tada je ispitivani broj sigurno složen. Povećavanjem broja ispitanih baza povećava se vjerojatnost da je broj prost (Crandall, Pomerance, 2001).

Algoritam 4. Miller-Rabinov test prostosti

1. *neka je* $n - 1 = 2^s r,\ r$ *neparan*
2. *za* i *od* 1 *do* t *radi:*
   - 2.1. *slučajno odabrati* $a, 2 \leq a \leq n - 2$
   - 2.2. $y \leftarrow a^r \bmod n$
   - 2.3. *ako* $y \neq 1$ *i* $y \neq n - 1$ *radi:*
     - 2.3.1. $j \leftarrow 1$
     - 2.3.2. *dok je* $j \leq s - 1$ *i* $y \neq n - 1$*:*
       - 2.3.2.1. $y \leftarrow y^2 \bmod n$
       - 2.3.2.2. *ako* $y = 1$ *vrati „složen“*
       - 2.3.2.3. $j \leftarrow j + 1$
     - 2.3.3. *ako* $y \neq n - 1$ *vrati „složen“*
3. *vrati „prost“*

Iteracija se provodi do željenog broja baza za testiranje i za svaku se generira varijabla slučajnog broja a u zadanom intervalu.

[4] Gary Lee Miller, američki računalni znanstvenik;
[5] Michael Oser Rabin, izraelski matematičar

Primjer 11. Ispitajmo Miller-Rabinovim testom prostosti je li broj $252\,601$ prost. Broj je traženog oblika $252\,601 - 1 = 2^3 \cdot 31\,575$. Računamo za slučajno odabrani $a = 85\,132$,

$$a^{31\,575} \bmod 252\,601 = 191\,102 \neq 1 \neq 252\,600.$$

Sljedeći korak je računanje

$$(a^{31\,575})^2 \bmod 252\,601 = 184\,829,$$

pa je opet dalje

$$(a^{31\,575})^{2^2} \bmod 252\,601 = 1.$$

Zaključak je da je ispitivani broj složen jer je $(85\,132^{31\,575})^{2^2} \equiv 1 (\bmod 252\,601)$.

Primjer 12. Ispitajmo Miller-Rabinovim testom prostosti je li broj $6\,553$ prost. Broj je traženog oblika $6\,553 - 1 = 2^3 \cdot 819$. Računamo za slučajno odabrani $a = 123$,

$$a^{819} \bmod 6\,553 = 2\,672 \neq 1 \neq 6552.$$

Sljedeći korak je računanje

$$(a^{819})^2 \bmod 6\,553 = 3\,367,$$

pa je opet dalje

$$(a^{819})^{2^2} \bmod 6\,553 = 6\,552.$$

Zaključak je da je broj jak pseudoprost u bazi 123 jer je $(123^{819})^{2^2} \equiv -1 (\bmod 6\,553)$. Analogno dalje se ispituje za željeni broj baza.

Direktno navodimo potrebno za dokaz da je složen broj jak pseudoprost u bazi za najviše $\frac{1}{4}$ svih baza.

Lema 1. Neka je $d = M(k, m)$. Tada je točno d elemenata u grupi $\{g, g^2, g^3, \ldots, g^m = 1\}$ za koje vrijedi da je $x^k = 1$.

Lema 2. Neka je p neparan prost broj i $p - 1 = 2^{s'} t'$, gdje je t' neparan. Tada je broj brojeva $x \in (\boldsymbol{Z}/p\boldsymbol{Z})^*$ takvih da je $x^{2^r t} \equiv -1 (\bmod p)$, gdje je t neparan jednak:

$$\begin{cases} 2^r M(t, t'), & r < s' \\ 0, & r \geq s'. \end{cases}$$

Propozicija 8. Neka je n je složeni neparni broj. n je jak pseudoprost broj u bazi b za najviše 25% od svih $0 < b < n$.

Dokaz.

1° Neka je $p^\alpha | n,\ \alpha \geq 2$, gdje je p prost broj. Svakako treba biti $b^{n-1} \equiv 1 \pmod n$, pa je $b^{n-1} \equiv 1 (\bmod p^2)$ **(►)**. Kako je ciklička grupa $(\boldsymbol{Z}/p^2\boldsymbol{Z})^* = \{g, g^2, g^3, \ldots, g^{p(p-1)}\}, g \in \mathbb{N}$, prema Lemi 1 kongruencija **(►)** ima $d = M(p(p-1), n-1)$ rješenja. Budući da $p|n$, znači da vrijedi $p \nmid n - 1$

i $p \nmid d$, prema tome $d \leq p-1$. Dakle, broj baza b, $0 < b < n$ koje zadovoljavaju kongruenciju **(►)** je

$$\frac{p-1}{p^2-1} = \frac{1}{p+1} \leq \frac{1}{4}.$$

2° Neka je $n = p \cdot q, p \neq q$, umnožak prostih brojeva. Neka može vrijediti $\begin{cases} p-1 = 2^{s_1}t_1 \\ q-1 = 2^{s_2}t_2 \end{cases}$, tako da su t_1 i t_2 neparni. Bez smanjenja općenitosti pretpostavimo da je $s_1 \leq s_2$. Jedno od sljedećega mora vrijediti: $\begin{cases} b^t \equiv 1 \pmod p \\ b^t \equiv 1 \pmod q \end{cases}$ ili $\begin{cases} b^{2^r t} \equiv -1 \pmod p \\ b^{2^r t} \equiv -1 \pmod q \end{cases}$ za neki $r, 0 \leq r < s$. Prema Lemi 1 broj baza za koje potonja tvrdnja vrijedi je $M(t,t_1) \cdot M(t,t_2) \leq t_1 t_2$. Prema Lemi 2, $b^{2^r t} \equiv -1 \pmod n$ ima rješenja ako je $2^r M(t,t_1) \cdot 2^r M(t,t_2) < 4^r t_1 t_2$. Kako je $n-1 > \varphi(n) = 2^{s_1+s_2} \cdot t_1 t_2$ slijedi da je najveći broj brojeva $b, 0 < b < n$ gdje je n jaki pseudoprost

$$\frac{t_1t_2 + t_1t_2 + 4t_1t_2 + 4^2t_1t_2 + \cdots + 4^{s_1-1}t_1t_2}{2^{s_1s_2}t_1t_2} = \frac{1+1+4+\cdots+4^{s_1-1}}{2^{s_1s_2}} = 2^{-s_1-s_2}\left(1 + \frac{4^{s_1}-1}{4-1}\right).$$

Ako je $s_1 < s_2$ tada je

$$2^{-2s_1-1}\left(\frac{4^{s_1}+2}{3}\right) \leq \frac{1}{2^{2s_1}} \cdot \frac{1}{2} \cdot \frac{2^{2s_1}}{3} + \frac{1}{2^3} \cdot \frac{2}{3} = \frac{1}{6} + \frac{1}{12} = \frac{1}{4}.$$

Nadalje, ako je $s_1 = s_2$ **(◊)**, barem jedna od nejednakosti $M(t,t_1) \leq t_1$, $M(t,t_2) \leq t_2$ mora biti stroga nejednakost jer ako je $t_1 | t$ i $t_2 | t$, tada bi bilo $n-1 = 2^s t = pq - 1 \equiv q-1 \pmod{t_1}$. Prema tome, iz $t_1 | q-1 = 2^{s_2}t_2$ slijedi da vrijedi $t_1 | t_2$ i analogno $t_2 | t_1$, što znači da je $t_1 = t_2$, odnosno $p = q$ ⇒⇐.

Kako radimo s neparnim brojevima i vrijedi stroga nejednakost barem za jednu od spomenutih najmanjih zajedničkih mjera, mora postojati faktor 3, pa mijenjajući t_1t_2 s $\frac{1}{3}t_1t_2$ dobivamo ocjenu $\frac{1}{3}2^{-s_1-s_2}\left(\frac{4^{s_1}+2}{3}\right)$. Uvrštavajući uvjet **(◊)**, dobivamo gornju granicu za koju je n pseudoprost:

$$\frac{1}{3}2^{-2s_1}\left(\frac{4^{s_1}+2}{3}\right) \leq \frac{1}{3} \cdot \frac{1}{2^{2s_1}} \cdot \frac{2^{2s_1}}{3} + \frac{1}{3} \cdot \frac{1}{2^2} \cdot \frac{2}{3} = \frac{1}{9} + \frac{1}{18} = \frac{1}{6} < \frac{1}{4}.$$

3° Neka je $n = p_1p_2 \cdots p_k,\ p_1 \neq p_2 \neq p_k,\ k \geq 3$ umnožak prostih brojeva i $p_j - 1 = 2^{s_j}t_j$ gdje je t_j neparan. Bez smanjenja općenitosti označimo $s_1 \leq s_j$ kao najmanji od s_j. Tada je najveći broj baza $b, 0 < b < n$ za koje je n pseudoprost:

$$2^{-s_1-s_2-\cdots-s_j}\left(1 + \frac{2^{ks_1}-1}{2^k-1}\right) \leq 2^{-ks_1}\left(\frac{2^k-1}{2^k-1} + \frac{2^{ks_1}}{2^k-1} + \frac{-1}{2^k-1}\right) =$$

$$= 2^{-ks_1}\left(\frac{2^k-2}{2^k-1} + \frac{2^{ks_1}}{2^k-1}\right) = 2^{-ks_1} \cdot \frac{2^k-2}{2^k-1} + \frac{1}{2^k-1}$$

$$\leq 2^{-k} \cdot \frac{2^k-2}{2^k-1} + \frac{1}{2^k-1} = \frac{2-2^{1-k}}{2^k-1} = \frac{2^{1-k+k}-2^{1-k}}{2^k-1} = \frac{2^{1-k} \cdot 2^k - 2^{1-k}}{2^k-1} = \frac{2^{1-k}\left(2^k-1\right)}{2^k-1} = 2^{1-k}$$

i kako je $k \geq 3$, slijedi da je $2^{1-k} \leq \frac{1}{4}$ (Koblitz, 1994). □

Primjer 13. Kako je vjerojatnost da je broj složen je $\frac{1}{4^k}$ za k baza za koje test daje pozitivan odgovor odnosno vjerojatnost da je prost $1 - \frac{1}{4^k}$, za 10 uspješno testiranih baza, vjerojatnost da je broj prost je

$$\left(1 - \frac{1}{4^{10}}\right) \cdot 100\% \approx 99{,}999905\%.$$

Također se može zaključiti da se postiže veća vjerojatnost prostosti za isti broj ispitivanih baza u odnosu na test preko Malog Fermatovog teorema.

4.4.1. Generiranje prostih brojeva

Jedan jednostavan način za generiranje prostog broja je kroz sljedeća dva koraka:

1. generiranje slučajnog broja n i odabir sigurnosnog parametra (broj baza za provjeru),
2. ako provjera za prostost daje pozitivan odgovor, generiran broj je dobar, a ako daje negativan odgovor, potrebno je vratiti se prethodni korak.

Neka je X događaj da je odabrani broj n složen, a Y_v događaj gdje Miller-Rabinov test prostosti daje odgovor da je n prost. Prema Propoziciji 8, vjerojatnost događaja uz uvjet je

$$P(X|Y_v) \leq \left(\frac{1}{4}\right)^v.$$

Neka je $0 \leq p \leq 1$ sama vjerojatnost da je broj n prost. Prema Bayesovoj formuli[6] je

$$P(X|Y_v) = \frac{P(X)P(Y_v|X)}{P(Y_v)} \leq \frac{P(Y_v|X)}{P(Y_v)} \leq \frac{1}{p}\left(\frac{1}{4}\right)^v.$$

Ako je slučajno odabran broj iz intervala neparnih brojeva $[3, x]$, tada vrijedi da je $P(X|Y_v) \leq \left(\frac{1}{4}\right)^v$ za svaki $x \geq 10^{60}$. (Menezes et al., 1996)

Neuspješnost generiranja prostog broja $p_{k,v}$ ovisi o broju bitova k i broju baza b za testiranje. Ako generirani broj ima manje bitova, tada broj baza za testiranje treba biti veći kako bi se zadovoljila određena postavljena granica prihvatljivosti da se odabere složeni broj.

[6] *Bayesova formula koristi se za računanje uvjetnih vjerojatnosti koje se nazivaju aposteriorne vjerojatnosti pojedinih hipoteza; prije početka pokusa, svaka hipoteza ima svoju vjerojatnost realizacije,* $P(H_i|A) = \frac{P(H_i)P(A|H_i)}{\sum_{j=1}^{n} P(H_j)P(A|H_j)}$;

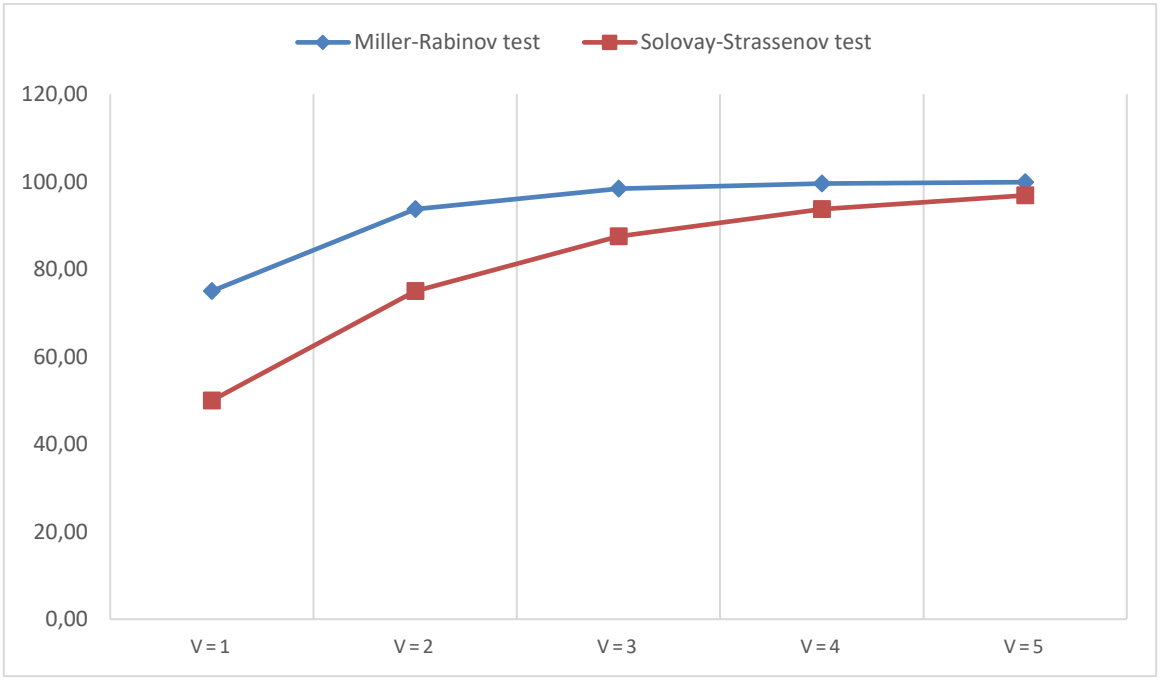
Tablica 4: Primjeri zadovoljavajućih broja bitova i broja baza (prema Menezes et al., 1996)

k	v
100	27
250	12
550	5
1050	3
1300	2

U Tablici 4 prikazani primjeri kombinacija brojeva k i v tako da vrijedi $p_{k,v} \leq \left(\frac{1}{2}\right)^{80}$.

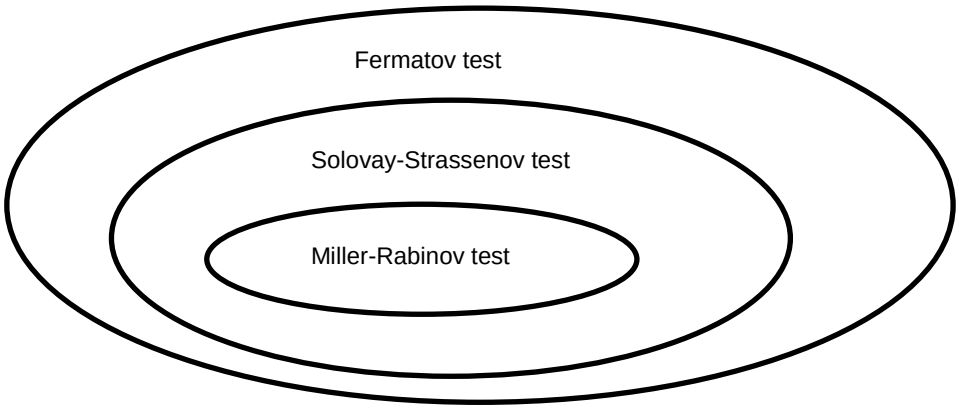
4.5. Usporedba testova

Ako uzmemo v kao broj baza za koje testovi prolaze, može se iscrtati graf za Solovay-Strassenov test i Miller-Rabinov test prostosti. Miller-Rabinov test dolazi do vjerojatnosti veće od 99% da je broj prost, dok drugom treba nešto više baza.



Slika 1: Usporedba vjerojatnosti kod testova prostosti

S obzirom na gornje testove, složeni brojevi imaju različiti broj brojeva za koje test prostosti daje pozitivan odgovor[7]. Imamo neki složeni broj za koji ispitujemo prostost s Fermatovim, Solovay-Strassenovim i Miller-Rabinovim testom prostosti. Ako za neki broj Miller-Rabinov test prostosti daje pozitivan odogovor, tada taj broj daje pozitivan odgovor i na ispitivanje Solovay-Strassenovim testom. Ako za neki broj Solovay-Strassenov test prostosti daje pozitivan odgovor, tada taj broj daje pozitivan odgovor i na ispitivanje Fermatovim testom. Odnos broja takvih brojeva prikazan je i grafički.



Slika 2: Odnos broja brojeva koji lažno potvrđuju prostost (prema: Menezes et al., 1996)

Primjer 14. Pokažimo broj za koji je testiranje prostosti sigurno složenog broja pozitivno. Krenimo ispitivati prostost broja $65 = 5 \cdot 13$ Fermatovim testom. Za nasumično odabran broj 18 vidimo da vrijedi

$$18^{64} \equiv 1 (\mathrm{mod}\ 65)$$

iako znamo da je broj 65 složen.

[7] eng. *(strong) liar number* ;

5. Prilozi koda

Kod 1. Implementacija modularnog potenciranja

```
def modularnoPotenciranje (a, k, n):
    binK=""
    brojac=0
    brojK=k
    while brojK!=0:
        binK=str(brojK%2)+binK
        brojK //=2
        brojac=brojac+1
    K=binK[::-1]

    b=1
    if k==0: return b
    A=a
    if K[0]=="1": b=a

    for i in range (1,brojac):
        A=(A*A)%n
        if K[i]=="1": b=A*b%n

    return b
```

Funkcija `modularnoPotenciranje (a, k, n)` iz Koda 1 vraća vrijednost $a^k \pmod n$. Prvo se računa binarna reprezentacija eksponenta i sprema u polje. Nadalje se računa rezultat na način koji je prikazan u Primjeru 4.

Implementacija izračuna Jacobijevog simbola koja se koristi u testovima prostosti dana je rekurzivno, koristeći sljedeće[8]:

- $J(0,n) = 0$
- $J(1,n) = 1$
- $J(ab,n) = J(a,n) \cdot J(b,n)$
- ako je $\frac{n^2-1}{8}$ parno $J(2,n) = 1$, inače $J(2,n) = -1$
- $J(a,n) = J(a \bmod n, n)$
- $J(a,pq) = J(a,p) \cdot J(a,q)$
- ako je $\frac{(a-1)(b-1)}{4}$ parno onda je $J(a,b) = J(b,a)$, ako je neparno onda je $J(a,b) = -J(b,a)$

[8] $J(x,y) = \left(\frac{x}{y}\right)$;

Kod 2. Implementacija izračuna Jacobijevog simbola (prema Schneier, 1996)

```
def Jacobi(a,b):
    if a>=b: a=a%b
    if a==0: return 0
    if a==1: return 1

    if a<0:
        if((b-1)/2)%2==0: return Jacobi(-a,b)
        else: return -Jacobi(-a,b)

    if a%2==0:
        if((b*b-1)/8)%2==0: return Jacobi(a/2,b)
        else: return -Jacobi(a/2,b)

    m=nzm(a,b)

    if m==a: return 0
    elif m!=1: return Jacobi(m,b)*Jacobi(a/m,b)
    elif (((a-1)*(b-1))/4)%2==0: return Jacobi(b,a)
    else: return -Jacobi(b,a)
```

Kod 3. Implementacija Fermatovog testa prostosti

```
def testFermat(n,v):
    for i in range (1,v+1):
        a=random.randint(2,n-2)
        r=modularnoPotenciranje(a,n-1,n)
        if r!=1: return "Broj je složen"
    return "Broj je pseudoprost"
```

Kod 4. Implementacija Solovay-Strassenovog testa prostosti

```
def testSolovayStrassen(n,v):
    for i in range (1,v+1):
        a=random.randint(2,n-2)
        s=Jacobi(a,n)
        if s==0: return "Broj je složen"
        eks=(n-1)/2
        r=modularnoPotenciranje(a,eks,n)
        if r%n == s: return "Broj je složen"
    return "Broj je pseudoprost"
```

Kod 5. Implementacija Miller-Rabinovog testa prostosti

```
def testMillerRabin(v,s,r):
    n=(2**s)*r+1
    for i in range (1,v+1):
        a=random.randint(2,n-2)
        y=modularnoPotenciranje(a,r,n)
        if y!=1 and y!=n-1:
            j=1
            while j<=s-1 and y!=n-1:
                y=(y*y)%n
                if y==1: return "Broj je složen"
                j=j+1
            if y!=n-1: return "Broj je složen"
    return "Broj je pseudoprost"
```

Primjer 15. Nađimo jedan pseudoprost broj izvršavanjem Miller-Rabinovog algoritma.

Možemo kao primjer ispisati:

45 844 312 962 604 026 618 177 901 144 864 622 755 302 133 071 773 251 723 287 429 121.

Izvršavanjem algoritma ne znamo faktorizaciju niti je li broj zasigurno prost.

6. Zaključak

Prost broj je onaj koji nema drugih djelitelja osim broja 1 i sebe samog. Faktorizacija složenog broja na proste faktore otežava se povećavanjem broja znamenki. Jednostavnim dijeljenjem nije moguće ispitivati prostost ili rastavljati na proste faktore u razumnom vremenu. Za ispitivanje prostosti postoje različiti testovi i složena znanja, a u ovom radu su opisana tri probabilistička testa. Ovisno o potrebama, dovoljno je znati da je veliki broj pseudoprost (vrlo vjerojatno prost).

Probabilistički testovi (Monte Carlo - orijentirani prema pozitivnom odgovoru), nakon željenog broja iteracija, mogu dati dva odgovora:

1. broj nije složen, odnosno prost je (moguće da nije točna tvrdnja),
2. broj je složen (sigurno je točna tvrdnja).

Ima smisla ispitivati samo neparne brojeve. Povećavanjem broja iteracija, odnosno baza za koje ispitujemo je li broj pseudoprost ili jak pseudoprost broj, smanjuje se vjerojatnost da je ispitivani broj složen. Za broj iteracija i, kod Fermatovog i Solovay-Strassenovog testa prostosti, vjerojatnost da je broj složen je $\frac{1}{2^i}$, dok kod Miller-Rabinovog testa $\frac{1}{4^i}$. Napomenimo da složen broj može zadovoljavati uvjete testa na prostost. Razumijevanjem spomenutih testova uz znanje opisano u prvom dijelu rada, moguće je generirati veće pseudoproste brojeve. Spomenuto se sve zbiva u razumnom vremenu. Veliki prosti odnosno pseudoprosti brojevi nalaze primjenu u kriptografiji.

Kriptografija je znanstvena disciplina koja se bavi načinima prijenosa poruke. Sam sadržaj poruke je nerazumljiv putujući kroz nesigurni kanal. Otvoreni tekst pretvara se u šifrat po nekom ključu, i opet po nekom ključu na drugoj strani šifrat treba postati otvoreni razumljiv tekst. Kriptosustav je uređeni sustav konačnog skupa mogućeg otvorenog teksta, mogućih elemenata šifrata, mogućih ključeva i funkcija enkripcije i dekripcije. Prema Kerckhoffsovom principu, kriptosustav mora biti siguran i kada su sve informacije o njemu poznate, osim naravno tajnog ključa. Kriptosustav postiže savršenu tajnost ako poruka koja se prenosi ne daje nikakve informacije o svojem značenju, odnosno otvorenom tekstu. Sigurnost prijenosa leži u teškoj faktorizaciji velikih brojeva.

Jedan od poznatijih kriptosustava je RSA kriptosustav (Rivest, Shamir, Adleman). Ovaj asimetrični kriptosustav (postoje javni i tajni ključ) je iz 1977. godine. Prvo se odabiru dva različita prosta broja p i q. Zatim se računa $n = pq$ i $\varphi(n) = (p-1)(q-1)$. Nadalje treba

postaviti d tako da je $de \equiv 1 (\mathrm{mod}\ \varphi(n))$, za odabrani $e < \varphi(n)$, $M\big(e, \varphi(n)\big) = 1$. Sada su javni ključ za šifriranje (n, e) i tajni ključ za dešifriranje (d, e). Djelovanjem javnim pa tajnim ključem na otvoreni tekst, ponovno se dobiva taj otvoreni tekst.

Popis literature

[1] Buchmann, J., i Müller, V. (1992). *Primality testing.* Saarbrücken: Universität des Saarlandes.

[2] Crandall, R., i Pomerance, C. (2001). *Prime Numbers: A Computational Perspective (2. izdanje).* New York: Springer-Verlag.

[3] Dujella, A. (2018a). *Diskretna matematika* [skripta - bilješke s predavanja]. preuzeto 15.06.2018. s https://web.math.pmf.unizg.hr/~duje/diskretna/diskretna.pdf

[4] Dujella, A. (2018b). *Uvod u teoriju brojeva* [skripta]. preuzeto 15.06.2018. s https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf

[5] Dujella, A., i Maretić, M. (2007). *Kriptografija.* Zagreb: Element.

[6] Koblitz, N. (1994). *A Course in Number Theory and Cryptography.* New York: Springer-Verlag.

[7] Kurose, J., i Ross, K. (2013). *Computer networking : a top-down approach (6. izdanje).* Boston: Pearson.

[8] Menezes, A. J., i Oorschot, P. C., i Vanstone, S. A. (1996). *Handbook of Applied Cryptography.* Boca Raton: CRC Press.

[9] Rosen, K., et al. (2000). *Handbook of Discrete and Combinatorial Mathematics.* Boca Raton: CRC Press.

[10] Schneier, B. (1996). *Applied Cryptography (2. izdanje).* Somerset, New Jersey: John Wiley & Sons.

[11] Smart, N. (2002). *Cryptography: An Introduction (3. izdanje).* New York: McGraw-Hill.

[12] Stallings, W. (2005). *Cryptography and Network Security - Principles and Practice.* Upper Sadle River: Prentice Hall.

[13] Stinson, D. R. (2006). *Discrete Mathematics and its Applications: Cryptography - Theory and Practice (3. izdanje).* Boca Raton: Chapman&Hall/CRC Press.

Popis slika

Popis tablica