Pseudoprosti brojevi

Fišer, Maja

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:296452

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-12**

Repository / Repozitorij:

Repository of School of Applied Mathematics and Computer Science

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij matematike
Financijska matematika i statistika

Maja Fišer

Pseudoprosti brojevi

Diplomski rad

Osijek, 2022.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij matematike
Financijska matematika i statistika

Maja Fišer

Pseudoprosti brojevi

Diplomski rad

Voditelj: izv. prof. dr. sc. Mirela Jukić Bokun

Osijek, 2022.

Sadržaj

Uvod **1**

1. Osnovni pojmovi i tvrdnje **2**

2. Pseudoprosti brojevi **5**

2.1. Pseudoprosti brojevi 5

2.2. Carmichaelovi brojevi 6

2.3. Eulerovi pseudoprosti brojevi 9

2.4. Jaki pseudoprosti brojevi 9

2.5. Lucasovi pseudoprosti brojevi 13

2.6. Superpseudoprosti brojevi 14

3. Testiranje prostosti **18**

3.1. Fermatov test prostosti 18

3.2. Miller - Rabinov test prostosti 19

3.3. Pocklington - Lehmerov test prostosti 20

3.4. Solovay - Strassenov test prostosti 21

Literatura **24**

Sažetak **25**

Summary **26**

Životopis **27**

Uvod

U ovom diplomskom radu pokušat ćemo približiti pojam pseudoprostih brojeva. Pseudoprosti brojevi su ušli u svijet matematike kroz teoriju brojeva koja je jedna od grana matematike. Kako bi mogli dobro upoznati pseudoproste brojeve, potrebno je dobro poznavanje djeljivosti i svojstava prostih brojeva što nas baš sama teorija brojeva uči. Prisjetimo se da su prosti brojevi prirodni brojevi koji imaju točno dva pozitivna djelitelja.

Teorija brojeva je igra inspiracije.

Michael Sean Mahoney

Pseudoprost broj je složeni broj koji prolazi test ili niz testova koji ne uspijevaju za većinu složenih brojeva. "Pseudoprost" korišten bez obilježja znači Fermatov pseudoprost, tj. složeni broj koji unatoč tome zadovoljava Fermatov mali teorem za neku bazu ili skup baza.

U prvom dijelu rada ćemo se prisjetiti svih važnih definicija i teorema kako bi lakše pratili ostatak rada. U nastavku ćemo imati fokus na pseudoprostim brojevima, njegovim oblicima te svojstvima koji sami pseudoprosti brojevi te kasnije i njegovi oblici, imaju. Iskazat ćemo u čemu se oni međusobno razlikuju i što ih povezuje.

Testiranje prostosti će biti sljedeća cjelina u kojoj ćemo opisati načine kako otkriti je li neki broj prost ili nije te ćemo na primjerima pokazati njihovu primjenu.

1. Osnovni pojmovi i tvrdnje

Prije nego što se upoznamo s pseudoprostim brojevima, prisjetimo se tvrdnji iz teorije brojeva koje će nam olakšati razumijevanje samih pseudoprostih brojeva i kasnije testiranje prostosti. Ovaj dio gradiva će se bazirati na [5] i [13].

Definicija 1.1. ***Fermatovi brojevi*** *su brojevi oblika* $F_n = 2^{2^n} + 1$, *gdje je* n *nenegativan cijeli broj dok su* ***Mersennovi brojevi*** *brojevi oblika* $M_n = 2^n - 1, n \in \mathbb{N}$.

Teorem 1.1 (Kineski teorem o ostacima, vidi [13]). *Neka su* $n_1, n_2, \ldots, n_k$ *u parovima relativno prosti prirodni brojevi te neka su* $a_1, a_2, \ldots, a_k$ *cijeli brojevi. Tada sustava kongruencija*

$$x \equiv a_1 \pmod{n_1}, x \equiv a_2 \pmod{n_2}, \ldots, x \equiv a_k \pmod{n_k}$$

ima rješenja. Ako je x_0 *jedno rješenje, tada su sva rješenja dana s* $x \equiv x_0 \pmod{n_1 n_2 \cdots n_k}$, *tj. rješenje je jedinstveno modulo* $n_1 n_2 \cdots n_k$.

Definicija 1.2. *Neka je* n *prirodan broj. Broj prirodnih brojeva u nizu* $1, 2, \ldots, n$ *koji su relativno prosti s* n *se označava s* $\varphi(n)$; *ovim je definirana funkcija* $\varphi : \mathbb{N} \to \mathbb{N}$ *koja se naziva* ***Eulerova funkcija***.

Teorem 1.2 (vidi [5]). *Eulerova funkcija* φ *je multiplikativna. Neka je* $n > 1$ *prirodan broj,* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. *Tada je*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Teorem 1.3 (Eulerov teorem, vidi [5]). *Neka je* $a \in \mathbb{Z}$, $n \in \mathbb{N}$. *Ako je* $(a, n) = 1$, *onda je*

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

Dokaz: Neka je $S = \{a_1, a_2, \ldots, a_{\varphi(n)}\}$ reducirani sustav ostataka modulo n. Tada je i skup $\{aa_1, aa_2, \ldots, aa_{\varphi(n)}\}$ reducirani sustav ostataka modulo n (iz $aa_i \equiv aa_j \pmod{n}$ slijedi $a_i \equiv a_j \pmod{n}$, jer je $(a, n) = 1$, pa je $i = j$ jer je S reducirani sustav ostataka modulo n). Stoga za svaki $i \in \{1, \ldots, \varphi(n)\}$ postoji jedinstveni $j \in \{1, \ldots, \varphi(n)\}$ takav da je $a_i \equiv aa_j \pmod{n}$. Prema tome je

$$\prod_{j=1}^{\varphi(n)} (aa_j) \equiv \prod_{i=1}^{\varphi(n)} a_i \pmod{n},$$

odnosno

$$a^{\varphi(n)} \prod_{j=1}^{\varphi(n)} a_j \equiv \prod_{i=1}^{\varphi(n)} a_i \pmod{n}.$$

Pošto znamo da je $(a_i, n) = 1$, zbog svojstava kongruencije dobivamo $a^{\varphi(n)} \equiv 1 \pmod{n}$. $\square$

Teorem 1.4 (Mali Fermatov teorem, vidi [13]). *Neka je* p *prost broj i* $a \in \mathbb{Z}$. *Tada je*

$$a^p \equiv a \pmod{p},$$

a ako $p \nmid a$ *onda je*

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

Dokaz: Iz Eulerovog teorema slijedi $a^{p-1} \equiv 1 \pmod{p}$ ako $p \nmid a$. Množenjem ove jednakosti s a, dobije se jednakost $a^p \equiv a \pmod{p}$ za koju se lako vidi da vrijedi i ako $p \mid a$. $\square$

Obrat Malog Fermatovog teorema ne vrijedi, te ćemo to pokazati primjerom.

Primjer 1.1. *Neka je $a = 2$ i $p = 341 = 31 \cdot 11$. Iz*

$$2^{10} \equiv 1 \pmod{341}$$

slijedi da je

$$2^{340} \equiv 1 \pmod{341}.$$

No, broj 341 je složen.

Definicija 1.3. *Neka je $n \in \mathbb{N}, a \in \mathbb{Z}$ i $(a, n) = 1$. Najmanji prirodni broj d sa svojstvom da je*

$$a^d \equiv 1 \pmod{n}$$

naziva se ***red od a modulo n*** *te ćemo ga označavati sa $\mathrm{ord}_d a$.*

Definicija 1.4. *Ako je red od a modulo n jednak $\varphi(n)$, onda se a naziva* ***primitivni korijen modulo n****.*

Teorem 1.5 (vidi [12])**.** *Neka je $n \in \mathbb{N}$, neka je a cijeli broj sa svojstvom $(a, n) = 1$ te neka je m cijeli broj. Tada vrijedi*

$$a^m \equiv 1 \pmod{n} \Longleftrightarrow \mathrm{ord}_n(a) \mid m.$$

Definicija 1.5. *Neka je $n \in \mathbb{N}$. Za svaki $a \in \mathbb{Z}$ takav da je $(a, n) = 1$ postoji jedinstveni $l \in \{0, 1, \ldots, \varphi(n) - 1\}$ takav da je $g^l \equiv a \pmod{n}$. Eksponent l se naziva* ***indeks (ili diskretni logaritam) od a u odnosu na g*** *i označava se s $\mathrm{ind}_g a$ ili $\mathrm{ind} a$.*

Teorem 1.6 (vidi [5])**.** *Vrijedi sljedeće:*

$$\begin{aligned}
&(1)\ \mathrm{ind} a + \mathrm{ind} b \equiv \mathrm{ind}(ab) \pmod{\varphi(n)},\\
&(2)\ \mathrm{ind} 1 = 0, \mathrm{ind}_g g = 1,\\
&(3)\ \mathrm{ind}(a^m) \equiv m \cdot \mathrm{ind} a \pmod{\varphi(n)} \text{ za } m \in \mathbb{N},\\
&(4)\ \mathrm{ind}(-1) = \frac{1}{2}\varphi(n) \text{ za } n \geq 3.
\end{aligned}$$

Dokaz: Svojstva (1)-(3) proizlaze direktno iz definicije indeksa te množenja i potenciranja potencija. Također su analogna svojstvima logaritamske funkcije. Svojstvo (4) slijedi iz $g^{2\mathrm{ind}(-1)} \equiv (-1)^2 \equiv 1 \pmod{n}$ i $2\mathrm{ind}(-1) < 2\varphi(n)$. $\square$

Sada ćemo definirati Legrendreov i Jacobijev simbol koje ćemo koristiti u definiranju Eulerovih pseudoprostih brojeva i u Solovay-Strassenovom testu prostosti.

Definicija 1.6. *Neka je p neparni prosti broj i $a \in \mathbb{Z}$.* ***Legendreov simbol*** $\left(\frac{a}{p}\right)$ *je jednak 1 ako je a kvadratni ostatak modulo p, jednak je -1 ako je a kvadratni neostatak modulo p, a jednak je 0 ako $p \mid a$.*

Teorem 1.7 (Eulerov kriterij, vidi [13]). *Neka je p neparan prost broj i $a \in \mathbb{Z}$. Tada je*

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

Definicija 1.7. *Neka je P neparan prirodan broj te neka je $P = p_1 \cdots p_s$, gdje su p_i neparni prosti brojevi, ne nužno različiti. Tada se* ***Jacobijev simbol*** $\left(\frac{a}{P}\right)$ *definira s*

$$\left(\frac{a}{P}\right) = \prod_{j=1}^{s} \left(\frac{a}{p_i}\right),$$

gdje je $\left(\frac{a}{p_i}\right)$ *Legrendreov simbol.*

Svojstva Jacobijevog simbola ćemo koristiti u Solovay-Strassenovom testu prostosti pa ćemo ih ovdje odmah iskazati.

Propozicija 1.1 (vidi [13]). *Neka su $a, b \in \mathbb{Z}$ te P_1 i P_2 neparni prirodni brojevi. Tada vrijedi:*

(1) $\left(\frac{a}{P_1 P_2}\right) = \left(\frac{a}{P_1}\right)\left(\frac{a}{P_2}\right)$,

(2) $\left(\frac{ab}{P_1}\right) = \left(\frac{a}{P_1}\right)\left(\frac{b}{P_1}\right)$,

(3) ako je $a \equiv b \pmod{P_1}$, *tada vrijedi* $\left(\frac{a}{P_1}\right) = \left(\frac{b}{P_1}\right)$,

(4) ako je $(a, P_1) = 1$, *tada vrijedi* $\left(\frac{a^2}{P_1}\right) = \left(\frac{a}{P_1^2}\right) = 1$,

(5) $\left(\frac{-1}{P_1}\right) = (-1)^{\frac{P_1-1}{2}}, \left(\frac{2}{P_1}\right) = (-1)^{\frac{P_1^2-1}{8}}$,

(6) ako je $(P_1, P_2) = 1$, *tada vrijedi* $\left(\frac{P_1}{P_2}\right)\left(\frac{P_2}{P_1}\right) = (-1)^{\frac{P_1-1}{2} \cdot \frac{P_2-1}{2}}$.

2. Pseudoprosti brojevi

Nakon što smo se prisjetili bitnih pojmova i izraza, prijeđimo sada na pseudoproste brojeve i njihova obilježja kako bi se kasnije mogli upoznati s njihovim oblicima.

2.1. Pseudoprosti brojevi

Definicija 2.1. *Neparan složen broj n koji zadovoljava*

$$a^{n-1} \equiv 1 \pmod{n}, \tag{1}$$

gdje je $a \in \mathbb{Z}, (a, n) = 1$, zovemo ***pseudoprost broj u bazi a*** *(kraće psp(a)).*

Za pseudoproste brojeve u bazi a još se koriste i nazivi *Pouletovi brojevi, Sarrusovi brojevi ili Fermateovi brojevi* ([9]).

Primjer 2.1. *U Primjeru 1.1 je pokazano kako je broj* 341 psp(2). *Još neki primjeri pseudoprostih brojeva su: 561, 645, 1105, 1729, 1905.*

Teorem 2.1 (vidi [12])**.** *Ako je n neparan pseudoprost broj, tada je $n' = 2^n - 1$ također neparan pseudoprost broj.*

Dokaz: Kako je n neparan psp broj, tada prema Malom Fermatovom teoremu $n \mid 2^{n-1} - 1$ te vrijedi $n \mid 2^n - 2$. Ako primijenimo oznaku iz iskaza Teorema 2.1 dobivamo $n \mid n' - 1$. Po definiciji djeljivosti slijedi, $n' - 1 = kn$, gdje je $k \in \mathbb{Z}$. Sada imamo:

$$2^{n'-1} - 1 = 2^{kn} - 1 = (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1).$$

Dakle, $n' = 2^n - 1 \mid 2^{n'-1} - 1$, pa je n' psp broj. □

Prethodni teorem nam govori da za svaki psp broj možemo naći jedan veći. U sljedećem teoremu pokazat ćemo da postoji beskonačno mnogo psp brojeva u svakoj bazi.

Teorem 2.2 (vidi [5])**.** *Za svaki $a \in \mathbb{N}$ i $a \geq 2$ postoji beskonačno mnogo pseudoprostih brojeva u bazi a.*

Dokaz: Neka je p proizvoljan neparan prost broj za koji vrijedi $p \nmid a^2 - 1$. Promatramo $n \in \mathbb{N}$ takav da je $n = \frac{a^{2p}-1}{a^2-1}$. Zbog razlike kvadrata vrijedi

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

iz čega slijedi da je n složen broj.
Iz Malog Fermatovog teorema slijedi da je $a^{2p} \equiv a^2 \pmod{p}$. Dakle, $p \mid a^{2p} - a^2 = (n-1)(a^2 - 1)$. Pošto smo pretpostavili da $p \nmid a^2 - 1$, znači da $p \mid n - 1$. Osim toga, $n - 1 = a^{2p-2} + a^{2p-4} + \cdots + a^2$ je zbroj od $p - 1$ pribrojnika iste parnosti, pa je $n - 1$ paran broj.
Dakle, $2p \mid n - 1$, pa kako je $a^{2p} \equiv 1 \pmod{n}$, vrijedi i $a^{n-1} \equiv 1 \pmod{n}$, što povlači da je n psp broj u bazi a. Kako ima beskonačno mnogo prostih brojeva, također ima i beskonačno mnogo pseudoprostih brojeva u bazi a. □

Gornjim teoremom smo pokazali da psp brojeva ima beskonačno mnogo kao i prostih, ali su oni rjeđi od prostih brojeva. Rijetkost psp brojeva sa fiksnom bazom a, u usporedbi

s prostim brojevima, daje objašnjenje za korištenje Malog Fermatovog teorema kao baze za test prostosti.

Postojanje psp brojeva u bazi a pokazuje nam da testiranje samo s jednom bazom nije dovoljno da bi zaključili da je broj prost što ćemo pokazati sljedećim primjerom.

Primjer 2.2 (vidi [9]). *Pogledajmo kongruenciju*

$$4^{14} \equiv 1 \pmod{15}$$

iz koje je vidljivo da zadovoljava (1), *ali* 15 *nije prost broj. U takvim slučajevima možemo pokušati kombinirati više baza. U Primjeru 1.1 smo pokazali da je* 341 psp(2). *Kako vrijedi:*

$$3^{340} \not\equiv 1 \pmod{341},$$

341 *nije* psp(2).
Vrijedi

$$3^{90} \equiv 1 \pmod{91},$$

ali

$$2^{90} \not\equiv 1 \pmod{91},$$

pa je 91 psp(3), *a nije* psp(2).

Pseudoprosti brojevi u bazi a ponašaju se kao prosti, tj. prolaze test prostosti.

Pitamo se sljedeće: ako je prirodan broj n pseudoprost u bazi a za svaki $2 \leq a \leq n, (n, a) = 1$, je li tada n prost? Ili, obratno, ako je prirodan broj n složen, postoji li nužno a takav da je $(n, a) = 1$ i $a^{n-1} \not\equiv 1 \pmod{n}$? Nažalost, kao što ćemo vidjeti u nastavku, odgovor je ne. Navedenim testom se ne mogu s potpunom sigurnošću određivati prosti brojevi (iako se na taj način mogu određivati s velikom vjerojatnošću) ([13]).

2.2. Carmichaelovi brojevi

Prva podvrsta pseudoprostih brojeva koju ćemo upoznati su Carmichaelovi brojevi. Nazvani su po Robertu Carmichaelu koji je bio američki matematičar. Pronašao je najmanji Carmichaelov broj, 561, a preko 50 godina kasnije dokazano je da ih ima beskonačno mnogo.

Definicija 2.2. *Složen broj n nazivamo* ***Carmichaelovim brojem*** *ako za svaki $a \in \mathbb{Z}$, takav da je $1 < a < n$ i $(a, n) = 1$, vrijedi:*

$$a^{n-1} \equiv 1 \pmod{n}.$$

Zanimljivo je da ako je poznata faktorizacija od n, onda se može lako ustanoviti je li broj n Carmichaelov broj.

Primjer 2.3. *Malim Fermatovim teoremom pokažimo da je broj* 561 *Carmichaelov broj. Faktorizirajmo prvo broj* $561 = 3 \cdot 11 \cdot 17$. *Fermatov teorem nam kaže da ako vrijedi* $b \not\equiv 0 \pmod{17}$, *onda je* $b^{16} \equiv 1 \pmod{17}$. *Tada je*

$$b^{560} \equiv (b^{16})^{35} \equiv 1^{35} \equiv 1 \pmod{17}.$$

Slično, kada $b \not\equiv 0 \pmod{11}$, *Fermatov teorem nam daje* $b^{10} \equiv 1 \pmod{11}$, *pa je*

$$b^{560} \equiv (b^{10})^{56} \equiv 1^{56} \equiv 1 \pmod{11}.$$

Na kraju, za $b \not\equiv 0 \pmod 3$, *Fermatov teorem nam daje* $b^2 \equiv 1 \pmod 3$, *odakle slijedi* $b^{560} \equiv 1 \pmod 3$. *Zaključujemo da je*

$$b^{560} \equiv 1 \pmod{561},$$

za svaki cijeli broj b *za koji vrijedi* $(b, 561) = 1$, *pa je* 561 *Carmichaelov broj.*

Lema 2.1 (vidi [13]). *Svaki Carmichaelov broj je neparan.*

Dokaz: Ako je $n > 2$ paran broj, tada je $(n-1)^{n-1} \equiv (-1)^{n-1} \equiv -1 \pmod n$ pa n nije pseudoprost u bazi $n-1$, a dva uzastopna broja su uvijek relativno prosta. □

Pomoću definicije kvadratno slobodnog broja i Kineskog teorema o ostacima, iskažimo i dokažimo bitni kriterij za određivanje Carmichaelovih brojeva.

Propozicija 2.1 (Korseltov kriterij, vidi [1]). *Cijeli složeni broj* $n > 2$ *je Carmichaelov broj ako i samo ako je*

(a) n *kvadratno slobodan i*

(b) za svaki prosti broj p *koji dijeli* n, *također* $p - 1 \mid n - 1$.

Dokaz: Neka je n Carmichaelov broj. Prvo ćemo pokazati da je n kvadratno slobodan. Ako prost broj p dijeli n više puta, označimo $n = p^k n'$ i neka vrijedi $(p, n') = 1$. Želimo pokazati da je $k = 1$ i to ćemo postići pomoću Kineskog teorema o ostacima (Teorem 1.1). Pretpostavimo suprotno, neka je $k \geq 2$, pa je n djeljiv sa p^2. Po Kineskom teoremu o ostacima, postoji $a \in \mathbb{Z}$ tako da vrijedi $a \equiv 1+p \pmod{p^k}$ i $a \equiv 1 \pmod{n'}$. Iz definicije Carmichaelovog broja, $(a, n) = 1$ i $a^{n-1} \equiv 1 \pmod n$. Skraćivanjem gornje kongruencije modulo p^2, dobivamo $(1+p)^{n-1} \equiv 1 \pmod{p^2}$. Zbog Binomnog teorema imamo $(1+p)^{n-1} \equiv 1+(n-1)p \pmod{p^2}$. Pošto je n djeljiv sa p, $1 + (n-1)p \equiv 1 - p \pmod{p^2} \equiv 1 \pmod{p^2}$. Dobivamo kontradikciju pa je $k = 1$.
U nastavku pokažimo da $(p-1) \mid (n-1)$ za svaki p koji dijeli n. Pošto je n kvadratno slobodan, p i n/p su relativno prosti. Izaberemo bilo koji $b \in \mathbb{Z}$ tako da $b \mod n$ ima red veličine $p-1$ (postoji primitivni korijen modulo bilo koji prost broj). Po Kineskom teoremu o ostacima, postoji $a \in \mathbb{Z}$ takav da je $a \equiv b \pmod p$ i $a \equiv 1 \pmod{n/p}$, pa je $(a, n) = 1$. Tada vrijedi $a^{n-1} \equiv 1 \pmod n$. Skraćivanjem obje strane modulo p, dobije se $b^{n-1} \equiv 1 \pmod p$. Ovo implicira, po izboru od b, da $(p-1) \mid (n-1)$.
Sada pretpostavimo da je n kvadratno slobodan i vrijedi $(p-1) \mid (n-1)$ za svaki prost broj p koji dijeli n. Želimo pokazati da je n Carmichaelov broj. Ako $a \in \mathbb{Z}$ zadovoljava $(a, n) = 1$, tada za svaki prosti broj p koji dijeli n, vrijedi da je $(a, p) = 1$, pa je $a^{p-1} \equiv 1 \pmod p$. Kako je $p-1$ faktor od $n-1$ dobivamo $a^{n-1} \equiv 1 \pmod n$. Također, n je složen, pa je n Carmichaelov broj. □

Sljedeći primjer nam pokazuje primjenu Korseltovog kriterija.

Primjer 2.4. *Primjenimo Korseltov kriterij na broj* 1105. *Faktorizirajmo prvo broj,* $1105 = 5 \cdot 13 \cdot 17$. *Vidimo da je broj kvadratno slobodan, moramo još pokazati da svaki* $p - 1$ *mora dijeliti* $n - 1$. *Provjerimo:*

$$4 \mid 1104, 12 \mid 1104 \ i \ 16 \mid 1104.$$

Oba uvjeta su zadovoljena, prema tome broj 1105 *je Carmichaelov broj.*

Teorem 2.3 (vidi [10]). *Svaki Carmichaelov broj je produkt najmanje tri međusobno različita prosta broja.*

Dokaz: Iz Propozicije 2.1 (a) znamo da Carmichaelov broj mora biti produkt različitih prostih brojeva. Preostaje nam odbaciti mogućnost da je $n = pq$ produkt dva različita prosta broja. Pretpostavimo da je $p < q$. Ako je n Carmichaelov broj imali bi $n-1 \equiv 0 \pmod{q-1}$ zbog Propozicije 2.1 (b). Slijedi $n - 1 = p(q - 1 + 1) - 1 \equiv p - 1 \pmod{q - 1}$ što nije $\equiv 0 \pmod{q - 1}$ jer je $0 < p - 1 < q - 1$. □

Primijetimo da je složen broj n Carmichaelov ako i samo ako je pseudoprost u svakoj bazi koja je relativno prosta s n.

Primjer 2.5. *Carmichaelov broj je* 1729. *Vidimo da je* $1729 = 7 \cdot 13 \cdot 19$. *Neka je a prirodan broj koji je relativno prost s* 1729, *pa a ne smije biti djeljiv s* $7, 13$ *i* 19. *Tada vrijedi* $a^{m-1} \equiv 1 \pmod{m}$ *za* $m \in \{7, 13, 19\}$. *Kako je* $1728 = 6 \cdot 288 = 12 \cdot 144 = 18 \cdot 96$, *dobivamo da je* $a^{1728} \equiv 1 \pmod{m}, m \in \{7, 13, 19\}$, *odakle je* $a^{1728} \equiv 1 \pmod{1729}$.

Neka je $C(x)$ broj Carmichaelovih brojeva koji su manji ili jednaki x. Tada za svaki dovoljno veliki x vrijedi: $C(x) > x^{\frac{2}{7}}$. Iz toga slijedi da Carmichaelovih brojeva ima beskonačno mnogo (vidi [9]). Kako brojevi postaju sve veći, Carmichaelovi brojevi postaju sve rjeđi. Zanimljivo je da postoji 20138200 Carmichaelovih brojeva između 1 i 10^{21}.

Postojanje Carmichaelovih brojeva pokazuje važan nedostatak testiranja prostosti na osnovi Malog Fermatova teorema. U sljedećem poglavlju ćemo pokazati kako se malim promjenama na testu se taj nedostatak može ukloniti.

Teorem 2.4 (vidi [9]). *Neka je n neparan složen broj i $a \in \mathbb{Z}$. Tada vrijedi:*

> *(1) n je pseudoprost broj u bazi a ako i samo ako red od a modulo n dijeli $n - 1$.*
> *(2) Ako je n pseudoprost u bazama a_1 i a_2, onda je n pseudoprost i u bazama $a_1 \cdot a_2$ i $a_1 \cdot a_2^{-1}$.*
> *(3) Ako n ne zadovoljava* (1) *za neki a, $(a, n) = 1$, onda n ne zadovoljava* (1) *za barem pola mogućih baza a (tj. cijelih brojeva između* 1 *i n koji su relativno prosti s n).*

Dokaz: (1) Neka je d red od a modulo n i neka je n pseudoprost broj u bazi a iz Teorema 1.4 slijedi da $d \mid n - 1$.

(2) Iz $a_1^{n-1} \equiv a_2^{n-1} \equiv 1 \pmod{n}$, slijedi $(a_1a_2)^{n-1} \equiv 1 \pmod{n}$ i $(a_1a_2^{-1})^{n-1} \equiv a_1^{n-1}(a_2^{n-1})^{-1} \equiv 1 \pmod{n}$. Dakle, tvrdnja vrijedi.

(3) Neka su $a_1, a_2, \ldots, a_s$ baze u kojima n jest, a neka je a' baza u kojima n nije psudoprost broj. Kongruencija (1) ne vrijedi za $a = a'a_i$, gdje je $i \in \{1, \ldots, s\}$, jer bi onda vrijedilo i za $a' = (a'a_i)a_i^{-1}$. Dakle, postoji barem s baza u kojima n nije pseudoprost. □

Teorem 2.4 se može iskoristiti kao osnova za vjerojatnosni test prostosti. Naime, ako pretpostavimo da postoji baza a za koju ne vrijedi (1), te ako uzmemo k slučajno odabranih baza i n zadovolji test (1) za sve njih, onda je po Teoremu 2.4 (3) vjerojatnost da je n složen $\leq 1/2^k$. Nažalost, nedostatak ovog testa jest u tome što postoje složeni brojevi koji su pseudoprosti za sve baze a.

2.3. Eulerovi pseudoprosti brojevi

Sljedeći na redu su nam Eulerovi pseudoprosti brojevi i opišimo njihovu vezu s pseudoprostim brojevima. Ovaj oblik pseudoprostih brojeva dobio je ime po Leonhardu Euleru koji je bio švicarski matematičar, fizičar i astronom. Ovaj dio izlaganja baziran je na [7].

Definicija 2.3. *Neka je $b \in \mathbb{Z}$. Neparan pozitivan složen broj n koji je relativno prost sa b nazivamo* ***Eulerov pseudoprost broj u bazi b*** *ako vrijedi*

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

gdje $\left(\frac{b}{n}\right)$ označava Jacobijev simbol.

Kako je $\left(\frac{b}{n}\right) = \pm 1$ slijedi da Eulerov pseudoprost broj u bazi b mora biti i pseudoprost broj u bazi b. Obrat ne vrijedi: postoje pseudoprosti brojevi u bazi b koji nisu Eulerovi pseudoprosti brojevi u toj bazi.

Primjer 2.6. *Pokažimo da pseudoprost broj $n = 91$ nije Eulerov pseudoprost broj u bazi 3. Dakle, $3^{90} \equiv 1 \pmod{91}$, ali također $3^{45} \equiv 27 \pmod{91}$, pa 91 nije Eulerov pseudoprost broj u bazi 3. Iako 91 je Eulerov pseudoprost broj u bazi 10 jer je*

$$10^{45} \equiv 1000^{15} \equiv (-1)^{15} \equiv -1 \pmod{91}, \left(\frac{10}{91}\right) = -1.$$

Ako bazu b slučajno izaberemo, vjerojatnost da je složeni neparan cijeli broj n Eulerov pseudobroj u bazi b je manja ili jednaka $1/2$. To je osnova za stvaranje Solovay - Strassenovog testa prostosti s kojim ćemo se upoznati u sljedećem poglavlju.

2.4. Jaki pseudoprosti brojevi

Pojam jakog pseudoprostog broja uveo je Selfridge 1974. godine, a izlaganje ćemo bazirati na [6].

Definicija 2.4. *Neka je n neparan složen broj. Definiramo n kao $n = 2^s t + 1$, gdje je t neparan. Ako za $b \in \mathbb{Z}$ vrijedi:*

$$b^t \equiv 1 \pmod{n}, \text{ ili postoji } r < s \text{ takav da je } b^{2^r t} \equiv -1 \pmod{n}, \tag{3}$$

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

Primjer 2.7. *Jaki pseudoprost broj je 91 u bazi 10 jer je $10^{45} \equiv -1 \pmod{91}$.*

Ako uvjet (3) nije ispunjen za neki $b, 0 < b < n$, tada je broj n složen. U tom slučaju broj b zovemo *svjedok složenosti od n.*

Svaki spsp(b) je ujedno i psp(b). Obrat ne vrijedi. To ćemo pokazati sljedećim primjerom.

Primjer 2.8. *Broj $n = 341$ je* psp(2), *ali nije* spsp(2). *Zaista,*

$$340 = 2^2 \cdot 85,$$

dok je

$$\begin{aligned} 2^{85} &\equiv 32 \pmod{341}, \\ 2^{170} &\equiv 1 \pmod{341}. \end{aligned}$$

Propozicije i teorem koji nam slijede, govore nam o povezanosti Eulerovih pseudoprostih brojeva i spsp.

Propozicija 2.2 (vidi [10]). *Neka je n neparan prirodan broj i $b < n$ prirodan broj koji je relativno prost sa n. Ako je $n \equiv 3 \pmod 4$, onda je n jaki pseudoprost broj u bazi b ako i samo ako je n Eulerov pseudoprost broj u bazi b.*

Dokaz: Ako je $n \equiv 3 \pmod 4$, po (3) s mora biti 1. Tada je n jaki pseudoprost broj u bazi b ako i samo ako vrijedi

$$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod n. \tag{4}$$

Pokažimo prvo nužnost.
Ako je n Eulerov pseudoprost broj u bazi b, onda je

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

tj. vrijedi (4) i n je jaki pseudoprost broj u bazi b.
Nužnost ćemo dokazati na sljedeći način. Neka je n jaki pseudoprost broj u bazi b. Iz pretpostavke da je $n \equiv 3 \pmod 4$ slijedi

$$\left(\frac{\pm 1}{n}\right) = \pm 1,$$

pa je

$$\left(\frac{b}{n}\right) = \left(\frac{b \cdot (b^2)^{(n-3)/4}}{n}\right) = \left(\frac{b^{(n-1)/2}}{n}\right) = \left(\frac{\pm 1}{n}\right) = \pm 1 \equiv b^{\frac{n-1}{2}} \pmod n,$$

iz čega slijedi da je n Eulerov pseudoprost broj u bazi b. □

Propozicija 2.3 (vidi [10]). *Neka je n neparan prirodan broj i $b < n$ pozitivan broj koji je relativno prost s n. Ako je n jaki pseudoprost broj u bazi b, tada je n i Eulerov pseudoprost broj u bazi b.*

Teorem 2.5 (vidi [12]). *Neka je F_m složen Fermatov broj i neka je $M_p = 2^p - 1$ složen Mersenneov broj, gdje je p prost. Tada su i F_m i M_p Eulerovi pseudoprosti i jaki pseudoprosti brojevi.*

Dokaz: Poznato je da je $m \geq 5$ i $p \geq 11$. Tada je $\left(\frac{2}{F_m}\right) = 1$ i $\left(\frac{2}{M_p}\right) = 1$.
Prvo ćemo gledati Fermatove brojeve F_m. Jasno je da je

$$2^{2^m} \equiv -1 \pmod{F_m} \tag{5}$$

i dakle, F_m je jaki pseudoprost broj. Dalje, za $m \geq 5$

$$\frac{F_m - 1}{2} = 2^{2^m - 1} > 2^m.$$

Neka je k takav da vrijedi

$$\frac{(F_m - 1)/2}{2^m} = 2^k.$$

Tada po (5) slijedi

$$2^{(F_m-1)/2} = (2^{2^m})^{2^k} \equiv (-1)^{2^k} \equiv 1 \equiv \left(\frac{2}{F_m}\right) \pmod{F_m},$$

i tako je F_m Eulerov pseudoprost broj.
Sada gledamo Mersenneov broj M_p. Zapišemo $\frac{M_p-1}{2} = 2^{p-1} - 1$ koji je neparan cijeli broj. Prema Malom Fermatovom teoremu slijedi

$$\frac{M_p - 1}{2} \equiv 0 \pmod{p}.$$

Stoga je $\frac{M_p-1}{2} = kp$ za neki $k \in \mathbb{N}$. Kako $M_p = 2^p - 1 \mid 2^{kp} - 1$, slijedi

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

Tada je M_p i Eulerov i jaki pseudoprost broj. □

Sljedeći teorem nam omogućuje stvaranje beskonačno mnogo jakih pseudoprostih brojeva te zbog Propozicije 2.3 stvaranje beskonačno mnogo Eulerovih pseudoprostih brojeva.

Teorem 2.6 (vidi [12]). *Ako je n pseudoprost, tada je $n' = 2^n - 1$ jaki pseudoprost broj.*

Dokaz: Uočimo da je $\frac{2^n-2}{2} = 2^{n-1} - 1$ neparan cijeli broj. Iz dokaza Teorema 2.1 imamo

$$2^{(2^n-2)/2} \equiv 1 \pmod{n'}$$

i stoga je n' jaki pseudoprost broj. □

Slijede nam svojstva jakih pseudoprostih brojeva koja će nam biti bitna za testove prostosti koje ćemo kasnije iskazati (preuzeto iz [6]).

Teorem 2.7 (vidi [6]). *Neka je n neparni složeni broj. Tada je n jaki pseudoprosti broj u bazi b za najviše $(n-1)/4$ baza $b, 0 < b < n$.*

Teorem 2.7 nam pokazuje da u slučaju jakih pseudoprostih brojeva ne postoji analogon Carmichaelovih brojeva. Dakle, nemoguće je da složen broj bude jaki pseudoprosti broj u svakoj bazi.

Prije dokaza Teorema 2.7, dokazat ćemo lemu koja će nam dati potrebne informacije o kongruencijama oblika $x^m \equiv \pm 1 \pmod{n}$. S $\nu_m(t)$ ćemo označavati najveći cijeli broj k takav da $m^k \mid t$.

Lema 2.2 (vidi [6]). *Neka je $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ neparan broj te neka je*

$$\nu = \min\{\nu_2(p_i - 1) : i = 1, \ldots, r\} \text{ i } S = \prod_{i=1}^{r} (m, \varphi(p_i^{\alpha_i})).$$

Tada vrijedi:

(1) Kongruencija $x^m \equiv 1 \pmod{n}$ ima točno S rješenja.
(2) Kongruencija $x^m \equiv -1 \pmod{n}$ ima rješenja ako i samo ako je $\nu_2(m) < \nu$.
(3) Ako kongruencija $x^m \equiv -1 \pmod{n}$ ima rješenja, onda ih ima točno S.

Dokaz: Neka je g_i primitivni korijen modulo $p_i^{\alpha_i}$. Neka je $j = \text{ind}_{g_i} x$. Koristit ćemo svojstva indeksa navedena u prvom poglavlju. Kongruencija $x^m \equiv c \pmod{n}$ je ekvivalentna sustavu kongruencija

$$m \cdot \text{ind}_{g_i} x \equiv \text{ind}_{g_i} c \pmod{\varphi(p_i^{\alpha_i})}, i = 1, \ldots, r.$$

Za $c = 1$ je $\text{ind}_{g_i} 1 = 0$, pa sustav postaje

$$m \cdot \text{ind}_{g_i} x \equiv 0 \pmod{\varphi(p_i^{\alpha_i})}, \quad i = 1, \ldots, r.$$

Ovo su linearne kongruencije kojih imamo i, pa je broj rješenja $(m, \varphi(p_i^{\alpha_i}))$. Ukupan broj rješenja sustava je umnožak svih najmanjih zajedničkih djelitelja što je jednako S.
Za $c = -1$ je $\text{ind}_{g_i}(-1) = \frac{\varphi(p_i^{\alpha_i})}{2}$, pa gornji sustav postaje

$$m \cdot \text{ind}_{g_i} x \equiv \frac{\varphi(p_i^{\alpha_i})}{2} \pmod{\varphi(p_i^{\alpha_i})}, \quad i = 1, \ldots, r.$$

Kao i u slučaju kada je $c = 1$, iz sustava linearnih kongruencija zaključujemo da ako ovaj sustav ima rješenja, onda ih ima S, a nužan i dovoljan uvjet za postojanje rješenja je da za svaki i broj $(m, \varphi(p_i^{\alpha_i}))$ dijeli $\frac{\varphi(p_i^{\alpha_i})}{2}$. Odavde imamo da $(2^{\nu_2(m)} m_1, p_i^{\alpha_i - 1} \cdot 2^{\nu_2(p_i - 1)} \cdot q_i)$ dijeli $p_i^{\alpha_i - 1} \cdot 2^{\nu_2(p_i - 1) - 1} \cdot q_i$, gdje su m_1 i q_i neparni brojevi. No ovo je očito ekvivalentno s $\nu_2(m) < \nu_2(p_i - 1)$ za $i = 1, \ldots, r$, tj. s $\nu_2(m) < \nu$. □

Dokaz Teorema 2.7:

1. slučaj: n nije kvadratno slobodan

Neka je $n = p^2 q$, gdje je p prost. Ako je n spsp(b), onda je $b^{n-1} \equiv 1 \pmod{n}$. Tada je i $b^{n-1} \equiv 1 \pmod{p^2}$. Prema Lemi 2.2 je $\varphi(p^2) = p(p-1)$, pa ova kongruencija ima $d = (p(p-1), n-1)$ rješenja. Budući da $p \mid n$, to p ne dijeli $n - 1$. Zato je $d \leq p - 1$. Stoga je broj baza b za koje je n psp(b)

$$\leq dq \leq (p-1)q = \frac{(p^2-1)q}{p+1} = \frac{p^2 q - q}{p+1} \leq \frac{p^2 q - 1}{p+1} \leq \frac{n-1}{4}.$$

Pošto smo pretpostavili da n nije kvadratno slobodan, jednakost vrijedi samo za $n = 9$.

2. slučaj: $n = pq$, gdje su p i q različiti prosti brojevi.

Neka je $p - 1 = 2^u \cdot v, q - 1 = 2^w \cdot z$, gdje su v i z neparni te $u \leq w$, $n - 1 = 2^s t$, tj. $u = \nu_2(p-1), w = \nu_2(q-1), s = \nu_2(n-1)$. Pretpostavimo da je $b^t \equiv 1 \pmod{n}$. Prema Lemi 2.2, takvih baza ima $(t, v) \cdot (t, z) \leq vz$. Pretpostavimo sada da je $b^{2^r t} \equiv -1 \pmod{n})$ za neki $r, 0 \leq r < s$. Prema Lemi 2.2, ova kongruencija ima rješenja ako i samo ako je $r < u$, a broj rješenja je $2^r(t, v) \cdot 2^r(t, z) \leq 2^{2r} vz$. Budući da je $n - 1 > \varphi(n) = \varphi(pq) = (p-1)(q-1) = 2^u v \cdot 2^w z = 2^{u+w} vz$, slijedi da prirodnih brojeva $b, 0 < b < n$, za koje je n jaki pseudoprosti broj u bazi b ima najviše

$$vz + \sum_{r=0}^{u-1} 2^{2r} vz = vz \left(1 + \frac{2^{2u} - 1}{3}\right) < (n-1) \cdot 2^{-u-w} \cdot \frac{2^{2u} + 2}{3}.$$

Ako je $u < w$, onda je desna strana ove nejednakosti

$$\leq (n-1) \cdot 2^{-2u-1} \left(\frac{2}{3} + \frac{2^{2u}}{3}\right) \leq (n-1) \cdot \left(\frac{1}{8} \cdot \frac{2}{3} + \frac{1}{6}\right) = \frac{n-1}{4}.$$

Ako je $u = w$, onda barem jedna od nejednakosti $(t, v) \leq v, (t, z) \leq z$ mora biti stroga jer bismo inače imali $0 = 2^s t \equiv pq - 1 \equiv q - 1 \pmod{v}$, pa bi iz $v \mid q - 1 = 2^w z$ slijedilo da $v \mid z$. Analogno bismo dobili da $z \mid v$, što bi značilo da je $v = z$ i $p = q$, a to je kontradikcija. Stoga, u gornjim ocjenama možemo zamijeniti vz s $\frac{vz}{3}$, jer je t neparan, a v ili $z > 1$, pa je njihov najveći zajednički djelitelj $< v/3$. To dovodi do sljedeće gornje ograde za broj baza b za koje je n jaki pseudoprosti broj u bazi b

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

3. slučaj: $n = p_1 p_2 \cdot \dots \cdot p_k$, gdje je $k \geq 3$, a p_i-ovi su različiti prosti brojevi.

Neka je $p_j - 1 = 2^{s_j} t_j, t_j$ neparan. Postavimo kao u 2. slučaju. Možemo pretpostaviti da je $s_1 \geq s_j$, za svaki j. Dobivamo sljedeću gornju ogradu za broj baza b takvih da je n jaki pseudoprosti broj u bazi b

$$\begin{aligned}
&(n-1)2^{-s_1-s_2-\dots-s_k} \left(1 + \frac{2^{ks_1} - 1}{2^k - 1} \right) \leq (n-1)2^{-ks_1} \left(\frac{2^k - 2}{2^k - 1} + \frac{2^{ks_1}}{2^k - 1} \right) \\
&= (n-1) \left(2^{-ks_1} \frac{2^k - 2}{2^k - 1} + \frac{1}{2^k - 1} \right) \leq (n-1) \left(2^{-k} \frac{2^k - 2}{2^k - 1} + \frac{1}{2^k - 1} \right) \\
&= (n-1) \cdot \frac{1}{2^{k-1}} \leq \frac{n-1}{4}.
\end{aligned}$$

□

2.5. Lucasovi pseudoprosti brojevi

Nova vrsta pseudoprostih brojeva je dobila ime po Francois Edouard Lucasu koji se rodio u Francuskoj. Otkrio je 12-ti Mersenneov prosti broj. Poglavlje je bazirano na [6] i [14].

Neka su α i β korijeni polinoma $x^2 - ax + b = 0, a, b \in \mathbb{Z} \setminus \{0\}$. Definirajmo *Lucasove nizove* $\mathrm{U}_k(a, b) = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \mathrm{V}_k(a, b) = \alpha^k + \beta^k$. Ako u nizove uvrstimo $a = 1, b = -1$, U_k su Fibonaccijevi brojevi, a V_k su (obični) Lucasovi brojevi. Ako su p prosti brojevi, takve da $p \nmid 2bD$, gdje je $D = a^2 - 4b$, onda vrijedi:

$$\mathrm{U}_{\delta(p)} \equiv 0 \pmod{p},$$

gdje je $\delta(p) = p - \left(\frac{D}{p}\right)$.

Pomoću ovog svojstva možemo definirati novu vrstu pseudoprostih brojeva.

Definicija 2.5. *Ako za neparan složen broj n vrijedi $\mathrm{U}_{\delta(n)} \equiv 0 \pmod{n}$, onda kažemo da je n* ***Lucasov pseudoprost broj s parametrima*** *a, b (označavamo ga s $\mathrm{lpsp}(a, b)$).*

Teorem 2.8 (vidi [14]). *Neka je $n \in \mathbb{N}$ i neka je n neparan, $\left(\frac{D}{n}\right)$ Jacobijev simbol i $\delta(n) = n - \left(\frac{D}{n}\right)$. Ako je n prosti broj i vrijedi $(n, b) = 1$ onda je*

$$U_{\delta(n)} \equiv 0 \pmod{n}. \tag{6}$$

Iako Teorem 2.8 vrijedi ako je $\left(\frac{D}{n}\right) = 1$, bilo bi najbolje to izbjegavati. Najbolji način za to je odabrati prikladan D tako da vrijedi $\left(\frac{D}{n}\right) = -1$. Navedimo dvije metode kako to postići:

(1) Neka je D prvi element niza $5, -7, 9, -11, \ldots$ za koji je $\left(\frac{D}{n}\right) = -1$. Neka su $a = 1, b = (1 - D)/4$.
(2) Neka je D prvi element niza $5, 9, 13, 17, 21, \ldots$ za koji je $\left(\frac{D}{n}\right) = -1$. Neka je a zadnji neparan broj koji premašuje $\sqrt{D}$ i $b = (a^2 - D)/4$.

Primjer 2.9. *Prvih 5 Lucasovih pseudoprostih brojeva koji su pronađeni prvom metodom su:*

$$323, 377, 1159, 1829, 3827,$$

a prvih 5 pronađenih drugom metodom su:

$$323, 377, 1349, 2033, 2651.$$

Teorem 2.9 (Lucasov test, vidi [14])**.** *Neka je n neparan pozitivan cijeli broj. Ako $p \nmid U_{n+1}$, onda je n složen broj.*

Ako izaberemo parametre D, a, b kako je opisano u drugoj metodi, tada prvih 50 Carmichaelovih brojeva i još par drugih Fermatovih pseuprostih brojeva u bazi 2 nikada neće biti Lucasovi pseudoprosti brojevi ([14]).

Kombinacija testova s jakim pseudoprostim brojevima i Lucasovim pseudoprostim brojevima je jako dobra i vjeruje se da broj koji prođe po jedan njihov test, mora biti prost. Njihovi testovi su neovisni jedan o drugome. Ako je n vjerojatno prost u prvoj vrsti testa, to ne utječe na vjerojatnost da n bude vjerojatnosno prost po drugoj vrsti.

2.6. Superpseudoprosti brojevi

Posljednja vrsta pseudoprostih brojeva s kojim ćemo se upoznati su superpseudoprosti brojevi te je ovaj dio rada baziran na [12]. Preko Fermatovih brojeva ćemo pokazati kako možemo stvoriti beskonačno mnogo superpseudoprostih brojeva kao i pseudoprostih brojeva.

Definirat ćemo prvo primitivnog prostog djelitelja kako bi lakše razumjeli ostatak izlaganja.

Definicija 2.6. *Neka su a, b prosti cijeli brojevi i vrijedi $|a| > |b| \geq 1$ i neka je $n \geq 1$ pozitivni cijeli broj. Kažemo da je p* ***primitivni prosti djelitelj od*** *$a^n - b^n$ ako $p \mid a^n - b^n$, ali $p \nmid a^m - b^m$ za $1 \leq m < n$.*
Ako $p^m \mid a^n - b^n$, ali $p^m \nmid a^k - b^k$, $1 \leq k < n$ kažemo da je ***p m-struki primitivni prosti djelitelj od*** *$a^n - b^n$.*

Napomena 2.1 (vidi [12])**.** *Ako je p m-struki primitivni prosti djelitelj od $a^n - 1$, tada za $1 \leq i \leq m$ vrijedi*

$$\mathrm{ord}_{p^i} a = n. \tag{7}$$

Prije same definicije superpseudoprostih brojeva iskažimo lemu koju će kasnije primijeniti.

Lema 2.3 (vidi [12])**.** *Ako je neparan prosti broj p primitivni prosti djelitelj od $a^n - 1$, tada je:*

$$\begin{aligned} &(1) \quad p \equiv 1 \pmod{n}, \\ &(2) \quad p \equiv 1 \pmod{2n} \text{ ako je } n \text{ neparan ili je } \left(\frac{a}{p}\right) = 1. \end{aligned}$$

Dokaz: (1) Po Malom Fermatovom teoremi i (7), $n \mid p-1$ pa imamo

$$p \equiv 1 \pmod{n}.$$

(2) Iz (1) slijedi da je $p \equiv 1 \pmod{2n}$ ako je n neparan broj. Sada pretpostavimo da je $\left(\frac{a}{p}\right) = 1$. Eulerov kriterij (Teorem 1.7) povlači da vrijedi

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

iz čega slijedi da $n \mid (p-1)/2$. Tada slijedi da je $p \equiv 1 \pmod{2n}$. □

Definicija 2.7. ***Superpseudoprost broj n u bazi a*** *je pseudoprost broj u bazi a čiji su djelitelji veći od 1 ili prosti ili pseudoprosti brojevi u bazi a; tj. ako $d \mid n$, tada vrijedi*

$$a^{d-1} \equiv 1 \pmod{n}. \tag{8}$$

Sada prvo iskažimo i dokažimo teorem koji nam daje nužan i dovoljan uvjet da neparni složeni cijeli broj n bude superpseudoprost u bazi a. Prisjetimo se da najmanji zajednički višekratnik brojeva $a, b \in \mathbb{Z} \setminus \{0\}$ označavamo s $[a, b]$.

Teorem 2.10 (vidi [12]). *Neka su $p_1, p_2, \ldots, p_r$ različiti neparni prosti brojevi i neka je $a \geq 2$ takav da vrijedi $(a, p_i) = 1$ za svaki $i = 1, 2, \ldots, r$. Pretpostavimo da je p_i m_i-terostruki primitivni prosti djelitelj od $a^{t_i} - 1$ za $1 \leq i \leq r$. Dozvoljen je i slučaj $t_i = t_j$ za $1 \leq i < j \leq r$. Označimo $[t_1, t_2, \ldots, t_r] = h$. Neka je n složeni cijeli broj za koji vrijedi*

$$n = \prod_{i=1}^{r} p_i^{l_i},$$

gdje je $1 \leq l_i \leq m_i$. Tada je n superpseudoprost broj u bazi a ako i samo ako za svaki $i = 1, 2, \ldots, r$ postoji cijeli broj k_i tako da vrijedi

$$p_i = k_i h + 1. \tag{9}$$

Dokaz: Pretpostavimo da vrijedi (9) za $1 \leq i \leq r$. Neka je $d = p_1^{g_1} p_2^{g_2} \cdots p_r^{g_r}$ složeni djelitelj od n, gdje je $0 \leq g_i \leq l_i, i = 1, 2, \ldots, r$. Kako bi pokazali da je d superpseudoprost broj u bazi a, dovoljno je pokazati da vrijedi

$$\mathrm{ord}_d a \mid d - 1. \tag{10}$$

Kako vrijedi $p_i \equiv 1 \pmod{h}, i = 1, 2, \ldots, r$ po (9), imamo $d \equiv 1 \pmod{h}$, ili ekvivalentnu kongruenciju

$$d - 1 \equiv 0 \pmod{h}. \tag{11}$$

Označimo sa e_i red od a modulo $p_i^{g_i}, i = 1, \ldots, r$. Prema Napomeni 2.1, ako je $g_i \geq 1$, onda za e_i vrijedi $e_i = t_i$ u suprotnom je $e_i = 1$. Kako je $(p_i^{g_i}, p_j^{g_j}) = 1, 1 \leq i < j \leq r$, slijedi da

$$\mathrm{ord}_d a = [e_1, e_2, \ldots, e_r] \mid [t_1, t_2, \ldots, t_r] = h. \tag{12}$$

Sada iz (11) i (12) dobivamo (10).
Sa druge strane, pretpostavimo da je n supepseudoprost broj u bazi a i neka postoji prosti djelitelj p_i od n tako da vrijedi $p_i \not\equiv 1 \pmod{h}$ za neki i, $1 \leq i \leq r$. Tada postoji prosti broj

q za koji vrijedi $q^m \parallel h$ (znači da je q^m najveća potencija od q koja dijeli h), ali $q^m \nmid p_i - 1$ za neki pozitivni cijeli broj m. Po definiciji od h, $q^m \parallel t_j$ za neki j za koji vrijedi $1 \leq j \leq r$. Kako je p_j primitivni prosti djelitelj od $a^{t_j} - 1$, po Lemi 2.6. vrijedi da je $p_j \equiv 1 \pmod{t_j}$. što nam daje kongruenciju

$$p_j \equiv 1 \pmod{q^m}.$$

Tvrdimo da $p_i p_j$ nije psp(a) što je kontradikcija sa pretpostavkom da je n superpseudoprost broj u bazi a. Kako vrijedi $p_i \not\equiv 1 \pmod{q^m}$ i $p_j \equiv 1 \pmod{q^m}$, dobivamo $p_i p_j \not\equiv 1 \pmod{q^m}$, tj.

$$p_i p_j - 1 \not\equiv 0 \pmod{q^m}.$$

Dakle,

$$\mathrm{ord}_{p_j} a = t_j \nmid p_i p_j - 1,$$

što nam daje

$$\mathrm{ord}_{p_i p_j} a \nmid p_i p_j - 1.$$

Što nas dovodi do toga da $p_i p_j$ nije psp(a). □

Koristeći Teorem 8, lako možemo konstruirati superpseudoprost broj iz tablice primitivnih prostih djelitelja od broja $2^n - 1$. Pokažimo to sljedećim primjerom.

Primjer 2.10. *Pokažimo da je* $n = 89 \cdot 2113 \cdot 353 \cdot 2931542417$ *superpseudoprosti broj. Svaki od njegovih 4 prostih faktora je kogruentan* 1 *modulo* 88.

Broj 89 *je primitivni prosti djelitelj broja* $2^{11} - 1$,
broj 2113 *je primitivni prosti djelitelj broja* $2^{44} - 1$,
brojevi 353 *i* 2931542417 *su primitivni prosti djelitelji broja* $2^{88} - 1$,

i $[11, 44, 88] = 88$.

Slijedeći teorem nam pokazuje kako Fermatove brojeve možemo iskoristiti za kreiranje beskonačno mnogo superpseudoprostih brojeva.

Teorem 2.11 (vidi [12]). *(1) Ako je F_m složen, onda je F_m superpseudoprost.*
(2) $F_m F_{m+1}$ je superpseudoprost za svaki $m \geq 2$. Konkretno, postoji beskonačno mnogo superpseudoprostih brojeva.
(3) Pretpostavimo da je $m \geq 3$ i da je svaki prosti djelitelj od F_m oblika $k2^{m+3}+1$, gdje je $k \in \mathbb{N}$. Tada je $F_m F_{m+1} F_{m+2}$ superpseudoprost broj sa barem tri različita prosta djelitelja.
(4) Pretpostavimo da su $p_1, p_2, \ldots, p_s$ prosti djelitelji od F_m takvi da je $p_i \equiv 1 \pmod{2^{m+3}}$ za $1 \leq i \leq s$. Tada je $p_1 p_2 \cdots p_s F_{m+1} F_{m+2}$ superpseudoprost sa barem tri različita prosta djelitelja.
(5) Ako je n pseudoprost s točno dva prosta djelitelja, onda je n superpseudoprost.
(6) Ako je Mersenneov broj M_p složen, onda je M_p superpseudoprost.
(7) Neka je $n = 2^t - 1$ složen cijeli broj s barem dva primitivno prosta djelitelja. Ako su $p_1, p_2, \ldots, p_s$ bilo koji primitivni prosti djelitelji od n, gdje je $s \geq 2$ i ponavaljanja su dopuštena do višestrukosti od primitivnog prostog djelitelja, tada je $p_1 p_2 \cdots p_s$ superpseudoprost.
(8) Neka je $t \geq 5$ neparan cijeli broj i neka su $p_1, p_2, \ldots, p_s$ bilo koji primitivni prosti djelitelji od $2^t - 1$, gdje je $s \geq 1$ i neka su $q_1, q_2, \ldots, q_j$ bilo koji primitivni prosti djelitelji od $2^{2t} - 1$, gdje je $j \geq 1$. Ponavljanja su dopuštena za sve p-ove i

q-ove do višestrukosti primitivnih prostih djelitelja. Tada je $p_1p_2\cdots p_sq_1q_2\cdots q_j$ *superpseudoprost broj.*
(9) Pretpostavimo da $8 \mid t$. *Neka su* $p_1, p_2, \ldots, p_s$ *bilo koji primitivni prosti djelitelji od* $2^t - 1$, *gdje je* $s \geq 1$ *i neka su* $q_1, q_2, \ldots, q_j$ *bilo koji primitivni prosti djelitelji od* $2^{2t} - 1$, *gdje je* $j \geq 1$. *Tada je* $p_1p_2\cdots p_sq_1q_2\cdots q_j$ *superpseudoprost broj.*
(10) Bilo koji složeni djelitelj d superpseudoprostog broja je također superpseudoprost.

Napomena 2.2 (vidi [12]). *Jedini indeksi za koje je broj* $F_mF_{m+1}F_{m+2}$ *superpseudoprost su* $m = 3, 4, 8$. *Kako bi utvrdili je li* $M_{2,m}$ *superpseudoprost broj trebamo ispitati sve proste faktore od* $F_m, m \geq 3$ *i provjeriti jesu li oni svi oblika* $k2^{m+3} + 1$. *Jedini Fermatovi brojevi koji su faktorizirani do kraja, su oni brojevi gdje je* $0 \leq m \leq 11$.

Sljedeći teorem koristi Fermatove brojeve kako bi se izgeneriralo beskonačno mnogo superpseuroprostih brojeva sa barem tri različita prosta djelitelja.

Teorem 2.12 (vidi [12]). *Neka je p prosti djelitelj od* F_m, *gdje je* $m \geq 3$. *Tada je* $(p - 1)/2 > 2^{m+1}$. *Neka su* $p_1, p_2, \ldots, p_s$ *različiti primitivni prosti djelitelji od* $2^{(p-1)/2} - 1$ *i neka su* $q_1, q_2, \ldots, q_j$ *različiti primitivni prosti djelitelji od* $2^{p-1} - 1$, *gdje je* $j, s \geq 1$. *Tada je* $n = pp_1p_2\cdots p_sq_1q_2\cdots q_j$ *superpseudoprost broj sa barem tri različita prosta djelitelja. Posebno, postoji beskonačno mnogo superpseudoprostih brojeva koji imaju barem tri različita primitivna prosta korijena.*

Napomena 2.3 (vidi [12]). *Pošto je bilo koji složeni djelitelj superpseudoprostog broja također superpseudoprost broj po Teoremu 2.11 (10), Teorem 2.12 implicira da postoji beskonačno mnogo superpseudoprostih brojeva koji imaju točno tri različita prosta djelitelja.*

3. Testiranje prostosti

Postoje dvije vrste testova prostosti deterministički i probabilistički. U ovom radu ćemo pobliže objasniti probabilističke testove prostosti. Dok deterministički testovi sa sigurnošću daju odgovor je li neki broj prosti ili ne, probabilistički testovi prostosti će nam dati odgovor je li neki broj vjerojatno prost ili ne. Pored testiranog broja n, koriste i slučajno odabrane brojeve a. Ovakvim testovima se za prost broj nikada ne može dobiti rezultat da je složen, ali je moguće da složen broj testom bude prepoznat kao prost. Broj koji prođe probabilistički test, ali je zapravo složen, naziva se *pseudoprost broj*. Fermatov i Miller-Rabinov test su dva najčešće korištena testa, gdje za bilo koji složeni broj n najmanje polovina brojeva koje je moguće birati za a detektiraju da je n složen. Ovo znači da k ponavljanja smanjuje grešku vjerojatnosti za najviše 2^{-k} i može se učiniti proizvoljno malom povećavanjem broja pokušaja k.

3.1. Fermatov test prostosti

Ako je n neparan složen broj, vrijedi Mali Fermatov teorem i $(b, n) = 1$, onda je taj broj pseudoprost broj u bazi b.
Ispitivanje se provodi slučajnim odabirom baze $0 < b < n, d = (n, b)$. Pojavljuju se dvije mogućnosti. Prva je da je $d > 1$ što znači da je ispitivani broj sigurno složen i tu ispitivanje staje. Druga je da je $d = 1$, i tada se b potencira na $(n - 1)$. Ukoliko test nije zadovoljan, broj koji smo ispitivali je sigurno složen, a ukoliko je zadovoljen, slučajno odabiremo novu bazu po spomenutom ograničenju. Kako se postupak više puta ponavlja, vjerojatnost da je broj složen se smanjuje, odnosno povećava se vjerojatnost da je broj prost (vidi [4]).

Teorem 3.1 (Jaki Fermatov test, vidi [11]). *Neka je $n > 1$ neparan cijeli broj. Označimo $n - 1 = 2^k s$, gdje je s neparan i $k \geq 1$. Izaberimo $b \in \mathbb{Z}$ tako da vrijedi $1 < b < n$. Definiramo,*

$$\begin{aligned} b_0 &\equiv b^2 \pmod{n}, \\ b_1 &\equiv b_0^2 \pmod{n}, \\ b_2 &\equiv b_1^2 \pmod{n}, \\ &\vdots \\ b_k &\equiv b_{k-1}^2 \pmod{n}. \end{aligned}$$

Pretpostavimo da je n prost broj. Tada vrijedi $b_k \equiv 1 \pmod{n}$, i ako je j najmanji indeks za koji vrijedi $b_j \equiv 1 \pmod{n}$, onda je $j = 0$ ili $b_{j-1} \equiv -1 \pmod{n}$. Dakle, ako $b_k \not\equiv 1 \pmod{n}$ ili $b_{j-1} \not\equiv -1 \pmod{n}$, onda n nije prost broj.

Dokaz: Neka je $n \in \mathbb{N}$ i neka je n neparan broj, $(b, n) = 1$ te $b^{n-1} \equiv 1 \pmod{n}$. Budući da je $n - 1$ paran, možemo pokušati izvaditi drugi korijen iz ove kongruencije, tj. računati $b^{(n-1)/2} \pmod{n}, b^{(n-1)/4} \pmod{n}, \ldots$ Pretpostavimo da u i-tom koraku prvi puta dobijemo na desnoj strani kongruencije nešto različito od 1, recimo $b^{(n-1)/2^i} \equiv a \pmod{n}$. Ako je n prost, onda mora biti $a \equiv -1$ jer je $b^{(n-1)/2^{i-1}} \equiv 1 \pmod{n}$, a jedina rješenja kongruencije $x^2 \equiv 1 \pmod{n}$, ako je n prost, su $x \equiv \pm 1 \pmod{n}$. $\square$

Dakle, kombinirajući Mali Fermatov teorem sa svojstvom kongruencije $x^2 \equiv 1 \pmod{p}$ dobivamo jači zahtjev od onog iz definicije pseudoprostih brojeva (vidi [5]).

Primjer 3.1. *Neka su $n = 41$ i $b = 2$. Tada $n - 1 = 2^3 \cdot 5$, pa je $s = 5$ i $k = 3$. Računamo.*

$$\begin{aligned} b_0 &= 32, \\ b_1 &\equiv 32^2 \equiv 40 \pmod{41}, \\ b_2 &\equiv 40^2 \equiv 1 \pmod{41}, \\ b_3 &\equiv 1^2 \equiv 1 \pmod{41}. \end{aligned}$$

Primjetimo da je $b_k = b_3 = 1$. Najmanji indeks za kojeg je $b_{j-1} = 1$ je $j = 2$. Tada vrijedi $b_{j-1} = b_1 = 40 \equiv 1 \pmod{41}$. Zaključujemo da je 41 vjerojatno prosti broj.

Što prije pronađemo neki $b_i = 1$, možemo prestati tražiti i pogledamo prethodni korak je li $b_{j-1} \equiv -1$, da vidimo ako možda nećemo morati koristiti nekoliko zadnjih kvadriranja. U praksi, kada je n složen, pokažemo da je $b_k \neq 1$, pa je Fermatov test zadovoljen.

Sljedećim primjerom ćemo pokazati kako pomoću Jakog Fermatovog testa možemo pokazati je li neki broj jaki pseudoprosti broj.

Primjer 3.2. *Pokažimo da je $4033 = 37 \cdot 109$ spsp(2). Faktorizirajmo $4032 = 2^6 \cdot 63$, pa je $k = 6$ i $s = 63$. Tada računamo:*

$$\begin{aligned} b_0 &\equiv 2^{63} \equiv 3521 \pmod{4033} \\ b_1 &\equiv 3521^2 \equiv -1 \pmod{4033} \\ b_2 &\equiv (-1)^2 \equiv 1 \pmod{4033}. \end{aligned}$$

Očito svaki slijedeći b je također kongruentan 1 (mod 4033). Pošto je $b_2 \equiv 1$ i prethodni njemu $b_1 \equiv -1$, vidimo da je 4033 spsp(2).

3.2. Miller - Rabinov test prostosti

Miller-Rabinov test prostosti temelji se na jakim pseudoprostim brojevima i on je najrasprostranjeniji test prostosti. Miller-Rabinov test je poboljšani oblik Fermatovog testa prostosti. Dok većina testova otkriva je li neki broj prosti ili ne, Miller-Rabinov test dokazuje je li broj složen. Stoga bi se ovaj test trebao zvati test složenosti.

Formiranje testa se temelji na sljedećoj propoziciji, koja ima svojstvo da svaki složeni broj ima veliki broj svjedoka.

Propozicija 3.1 (vidi [8]). *Neka je p neparan prosti broj i pišemo*

$$p - 1 = 2^k q$$

gdje je q neparan. Neka je a bilo koji broj koji je djeljiv sa p. Onda je jedan od sljedećih uvjeta istinit:

(1) $a^q \equiv 1 \pmod{p}$,

(2) jedan od $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ *kongruentan je* $s \; -1 \pmod{p}$.

Dokaz: Po Malom Fermatovom teoremu imamo $a^{p-1} \equiv 1 \pmod{p}$. Iskaz nam govori da zadnji broj u nizu

$$a^q, a^{2q}, a^{4q}, \ldots a^{2^{k-1}}, a^{2^k q}$$

(koji je jednak a^{p-1}) je kongruentan 1 modulo p. Pošto je svaki sljedeći broj kvadrat prethodnom, jedan uvjet od sljedećih mora biti zadovoljen:

(1) prvi broj iz niza je kongruentan 1 modulo p,
(2) neki broj iz niza nije kongruentan 1 modulo p, ali postaje kongruentan kada se kvadrira. Jedini broj koji zadovoljava oba izraza

$$b \not\equiv 1 \pmod{p} \text{ i } b^2 \equiv 1 \pmod{p}$$

je -1, pa je jedan broj iz niza kongruentan -1 modulo p. □

Iskažimo sada *Miller-Rabinov test prostosti* ([6]):

Neka je n neparan broj za koji želimo ustanoviti je li prost ili složen. Prvo postavljamo da n bude sljedećeg oblika $n-1 = 2^s t$, gdje je t neparan. Na slučajan način odaberemo $b, 0 < b < n$ te izračunamo $b^t \mod n$ (najmanji ostatak po apsolutnoj vrijednosti). Ako dobijemo ± 1, zaključujemo da je n prošao test te biramo sljedeći b. U protivnom, uzastopno kvadriramo $b^t \mod n$ sve dok ne dobijemo rezultat -1. Kada dobijemo -1, onda je n prošao test i kažemo da je n prost. Ako nikad ne dobijemo -1, tj. ako dobijemo da je $b^{2^{r+1}t} \equiv 1 \pmod{n}$, ali $b^{2^r t} \equiv -1 \pmod{n}$, onda znamo da je sigurno n složen.

Prilikom testiranja prostosti, u najviše slučajeva biramo upravo ovaj test jer ako n prođe test za k b-ova, onda je vjerojatnost da je n složen izrazito mala, tj. $\leq \frac{1}{4^k}$. Tako npr. za $k = 20$ je vjerojatnost da je n složen manja od 10^{-12}. Tako dobiveni vjerojatno prosti brojevi se nazivaju još i *industrijski prosti brojevi.* Poznato je da ne postoji nijedan broj manji od 10^{12} za $b = 2, 3, 5, 7, 11$ koji je istodobno spsp(b) broj. Ocjena iz Teorema 2.7 može značajno poboljšati za velike brojeve n. Tako je vjerojatnost da je 500-bitni broj koji prođe samo jedan test složen manja od $\frac{1}{4^{28}}$ ([6]).

Primjer 3.3. *Ispitajmo Miller-Rabinovim testom prostosti je li broj* 35 *prost. Tada je* $n-1 = 34 = 2^1 \cdot 17, k = 1, m = 17$. *Stavimo da je* $a = b$. *Računamo koliko je* $6^m \pmod{35}$, $6^{17} = 6^1 \cdot 6^{16}$. *Imamo:*

$$\begin{aligned} 6^2 &\equiv 36 \pmod{35} \equiv 1 \pmod{35} \\ 6^4 &\equiv (6^2)^2 \equiv 36^2 \pmod{35} \equiv 1 \pmod{35} \\ &\vdots \\ 6^{16} &\equiv 1 \pmod{35}. \end{aligned}$$

Dobivamo da je $b_0 = 6^{17} = (6^{16})(6^1) \pmod{35} \equiv 6 \pmod{35} \not\equiv \pm 1 \pmod{35}$, *pa računamo* $b_1 = (b_0)^2 = 6^2 = 36 \pmod{35} \equiv 1 \pmod{35}$. *Sada nam Miller-Rabinov test prostosti vrati da je broj* 35 *složen.*
Fermatov test bi nam za broj 35 *vratio da je "vjerojatnosno" prost jer* $6^{34} \equiv 1 \pmod{35}$.

3.3. Pocklington - Lehmerov test prostosti

Prvo ćemo iskazati Pocklington - Lehmerov test prostosti te kroz primjer pokazati kako test funkcionira.

Propozicija 3.2 (Pocklington-Lehmer, vidi [11]). *Neka je* $n-1 = FN$ *gdje je* $(F, N) = 1$ *(*F *je faktoriziran, a* N *nije nužno faktoriziran). Pretpostavimo da postoji* b *tako da vrijedi*

$$b^{n-1} \equiv 1 \pmod{n} \tag{13}$$

i

$$(b^{(n-1)/q} - 1, n) = 1, \tag{14}$$

za svaki prosti broj q koji dijeli F. Tada svaki prosti faktor p od n zadovoljava kongruenciju $p \equiv 1 \pmod{F}$. Također, ako je $F > N$, onda je n prosti broj.

Dokaz: Neka vrijedi $p \mid n$. Kako je $b^{n-1} \equiv 1 \pmod{p}$, Teorem 1. implicira da tada vrijedi $\mathrm{ord}_p(b) \mid n-1$. Zapišimo

$$n - 1 = k \cdot \mathrm{ord}_p(b).$$

Neka je q jedan od prostih djelitelja od F. Ako $q \mid k$, onda je

$$(n-1)/q = (k/q)\mathrm{ord}_p(b)$$

višekratnik od $\mathrm{ord}_p(b)$. Dakle,

$$b^{(n-1)/q} = \left(b^{\mathrm{ord}_p(b)}\right)^{k/p} \equiv (1)^{k/p} \equiv 1 \pmod{p}.$$

To je u suprotnosti s pretpostavkom (14) pošto p dijeli n. Onda slijedi $p \nmid k$. To dobivamo za svaki djelitelj od F, znači da vrijedi $(F, k) = 1$. Poznato nam je svojstvo da ako su $a, b, c \in \mathbb{Z}$ i $(a, b) = 1$ onda iz $a \mid bc$ slijedi $a \mid c$. Kako je

$$FN = n - 1 = k \cdot \mathrm{ord}_p(b),$$

i $\mathrm{ord}_p(b) \mid p-1$, po svojstvu iznad $F \mid p-1$.
Ako je $F > N$, onda vrijedi $F^2 > FN = n-1$, pa je $F^2 \geq n$. Ako $F \mid p-1$, onda je $p > F \geq \sqrt{n}$. Znamo da ako je n složen broj onda on ima prosti faktor $p \leq \sqrt{n}$. Pošto su svi prosti faktori veći od $\sqrt{n}$, vidimo da n ne može biti složen, pa je n prost. □

Primjer 3.4. *Pokažimo da je $n = 9473$ prost broj. Prvo faktoriziramo $9472 = 2^8 \cdot 37$. Imamo $F = 2^8 = 256, N = 37$. Ubacimo sada to u kongruenciju iz Pocklington-Lehmer testa $2^{(n-1)/2} \equiv 1 \pmod{n}$, pa $b = 2$ ne zadovoljava (14). Ali, $3^{n-1} \equiv 1 \pmod{n}$ i $3^{(n-1)/2} \equiv -1 \pmod{n}$, pa je*

$$(3^{(n-1)/2} - 1, n) = (-2, n) = 1.$$

Stoga $b = 3$ što zadovoljava (13) i (14) za $q = 2$. Kako je 2 jedini prosti djelitelj od F, pretpostavka je zadovoljena. Pošto je $F > N$, n je prosti broj.

Ako većinu faktorizacija od $n-1$ ne znamo (pa ne možemo reći da je $F > N$), test ne može pokazati da je n prost.

3.4. Solovay - Strassenov test prostosti

Za druge vrste pseudoprostih brojeva postoje drugi testovi zasnivani na njima. Tako je sljedeći test, Solovay - Strassenov test zasnovan na Eulerovim pseudoprostim brojevima i manje je efikasan od Miller-Rabinova testa. Solovay - Strassenov test prostosti se u nekim izvorima naziva i Eulerov test pseudoprostosti.

Teorem 3.2 (Solovay - Strassenov test prostosti, vidi [3]). *Neka je n neparan prirodan broj. Tada postoji cijeli broj $a \in \{1, \ldots, n-1\}$ takav da vrijedi*

$$(a, n) = 1 \text{ i } a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Dokaz: Moramo pogledati slučaj kada je n kvadratno slobodan i kada se u faktorizaciji od n nalaze višestruki prosti faktori.
Pretpostavimo prvo da je n složen i kvadratno slobodan, pa n ima oblik $n = p_1 p_2 \dots p_r$ gdje je $r \geq 2$ i p_i su različiti prosti brojevi, $i \geq 2$. Pola faktora koji nisu nula $\bmod p_1$ su kvadratno slobodni, pa postoji $b \in \mathbb{Z}$ takav da je $\left(\frac{b}{p_1}\right) = -1$. Po Kineskom teoremu o ostacima, postoji neki $a \in \{1, \dots, n-1\}$ koji zadovoljava

$$a \equiv b \pmod{p_1}, a \equiv 1 \pmod{p_2 \cdots p_r}.$$

Znamo da je $b \not\equiv 1 \pmod{p}, a \neq 1$. Tada je $(a, p_1) = 1$ i $(a, p_2 \cdots p_r) = 1$, tako da je $(a, n) = 1$. Također, $\left(\frac{a}{p_1}\right) = \left(\frac{b}{p_1}\right) = -1$ i $\left(\frac{a}{p_i}\right) = \left(\frac{1}{p_i}\right) = 1$ za $i > 1$, pa je

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right) = \left(\frac{a}{p_1}\right) = -1.$$

Pretpostavimo da je $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$, pa je $a^{(n-1)/2} \equiv -1 \pmod{n}$. Kako p_2 dijeli n, možemo reducirati kongruenciju $a^{(n-1)/2} \equiv -1 \pmod{n}$ do modula p_2, pošto je $a \equiv 1 \pmod{p_2}$ dobivamo

$$1 \equiv -1 \pmod{p_2}.$$

To je kontradikcija pošto je p_2 veći od 2.
Sada pretpostavimo da n ima višestruki prosti faktor i označimo ga s p. Neka je $n = p^k m$ gdje je $k \geq 2$ i $(p, m) = 1$. Po Kineskom teoremu o ostacima, postoji $a \in \{1, \dots, n-1\}$ koji zadovoljava

$$a \equiv 1 + p \pmod{p^2}, a \equiv 1 \pmod{m}.$$

Kako je $a \neq 1$, a nije djeljiv s p, i $(a, m) = 1$, to je $(a, n) = 1$. Ako je $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ onda nam kvadriranje daje $a^{n-1} \equiv 1 \pmod{n}$, pa ćemo pokazati da to nije moguće. Reducirajmo kongruenciju do modulo p^2 (a je faktor od n) da bi dobili $a^{n-1} \equiv 1 \pmod{p^2}$. Kako je $a \equiv 1 + p \pmod{p^2}$ dobivamo $(1+p)^{n-1} \equiv 1 \pmod{p^2}$. Koristeći Binomni teorem, $(1+p)^{n-1} \equiv 1 + (n-1)p \pmod{p^2}$, pa je $1 + (n-1)p \equiv 1 \pmod{p^2}$. Oduzimanjem 1 s obje strane, $(n-1)p \equiv 0 \pmod{p^2}$, pa dobivamo $(n-1) \equiv 0 \pmod{p}$. Ali je n višekratnik od p, pa imamo kontradikciju. □

Ako je k dovoljno velik, n proglašavamo *"vjerojatno prostim"*.

Iako neki smatraju da je Fermatov test prvi test prostosti, to nije istina. Carmichaelovi brojevi mogu izgledati kao prosti kada prođu kroz Fermatov test, iako oni nisu prosti. Tek Solovay-Strassenovim testom se pokaže koji Carmichaelovi brojevi su zapravo prosti.

Primjer 3.5. *Ispitajmo Solovay-Strassenovim testom prostosti je li broj* 91 *prost. Slučajno izaberemo* $a = 10$*, pa prvo računamo Jacobijev simbol*

$$\left(\frac{10}{91}\right) = \left(\frac{2}{91}\right)\left(\frac{5}{91}\right) = (-1)\left(\frac{91}{5}\right) = -(1)\left(\frac{1}{5}\right) = (-1)(1) = -1.$$

Dalje računamo kongruenciju

$$10^{(91-1)/2} \equiv 10^{45} \equiv 10^{32+8+4+1} \pmod{91}. \tag{15}$$

Računamo redom 10 *na svaku potenciju modulo* 91. *Dobivamo sljedeće:*

$$\begin{aligned}
10^2 &\equiv 9 \pmod{91} \\
10^4 &\equiv (10^2)^2 \equiv 9^2 \equiv 81 \pmod{91} \equiv -10 \pmod{91} \\
10^8 &\equiv (10^4)^2 \equiv (-10)^2 \equiv 100 \pmod{91} \equiv 9 \pmod{91} \\
10^{16} &\equiv (10^8)^2 \equiv 9^2 \equiv 81 \pmod{91} \equiv -10 \pmod{91} \\
10^{32} &\equiv (10^{16})^2 \equiv (-10)^2 \equiv 100 \pmod{91} \equiv 9 \pmod{91}.
\end{aligned}$$

Nadalje uvrstimo sve u početnu kongruenciju (15) *te dobivamo* $\equiv 9 \cdot 9 \cdot (-10) \cdot 10 \equiv 9^2 \cdot (-100) \pmod{91} \equiv (-10) \cdot (-9) \equiv 90 \pmod{91}$. *Provjerimo je li stvarno* $-1 \equiv \frac{10}{91} \equiv 10^{45} \pmod{91}$, *što je točno. Iz ovoga bi nam Solovay-Strassenov test prostosti dao zaključak da je* 91 *vjerojatnosno prost.*
Slučajno ponovno odaberemo $a = 11$, *pa prvo računamo Jacobijev simbol*

$$\left(\frac{11}{91}\right) = (-1)\left(\frac{91}{11}\right) = -(1)\left(\frac{3}{11}\right) = \left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Dalje računamo kongruenciju

$$11^{(91-1)/2} \equiv 11^{45} \equiv 11^{32+8+4+1} \pmod{91}. \tag{16}$$

Računamo redom 11 *na svaku potenciju mogulo* 91. *Dobivamo sljedeće:*

$$\begin{aligned}
11^2 &\equiv 121 \pmod{91} \equiv 30 \pmod{91} \\
11^4 &\equiv (11^2)^2 \equiv 30^2 \equiv 900 \pmod{91} \equiv -10 \pmod{91} \\
11^8 &\equiv (11^4)^2 \equiv (-10)^2 \equiv 100 \pmod{91} \equiv 9 \pmod{91} \\
11^{16} &\equiv (11^8)^2 \equiv 9^2 \equiv 81 \pmod{91} \equiv -10 \pmod{91} \\
11^{32} &\equiv (10^{16})^2 \equiv (-10)^2 \equiv 100 \pmod{91} \equiv 9 \pmod{91}.
\end{aligned}$$

Nadalje uvrstimo sve u početnu kongruenciju (16) *te dobivamo* $\equiv 9 \cdot 9 \cdot (-10) \cdot 11 \equiv 9^2 \cdot (-10) \cdot 11 \pmod{91} \equiv (-10)^2 \cdot 11 \equiv 9 \cdot 11 \pmod{91}$. *Provjerimo je li stvarno* $-1 \equiv \frac{11}{91} \equiv 8 \pmod{91}$, *što je netočno. Iz ovoga nam Solovay-Strassenov test prostosti daje zaključak da je* 91 *složen broj.*

Literatura

[1] K. Conrad, *Carmichael numbers and Korselt's criterion*, `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/carmichaelkorselt.pdf`

[2] K. Conrad, *The Miller - Robin test*, `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf`

[3] K. Conrad, *The Solovay–Strassen test*, `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/solovaystrassen.pdf`

[4] R. Crandall, C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer, New York, 2001.

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

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

[7] B. Fine, B. Rosenberger, *Number Theory*, Birkhäuser, Berlin, 2007.

[8] J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, New York, 2014.

[9] A. Jurasić, M. Rukavina, *Pseudoprosti brojevi*, Matematičko fizički list **62**(2011), 20–25.

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

[11] J. S. Kraft, L. C. Washington, *An Introduction to Number Theory with Cryptography*, CRC Press, New York, 2008.

[12] M. Križek, F. Luca, L. Somer, *17 Lectures on Fermat Numbers*, CMS, Springer-Verlag, New York, 2001.

[13] I. Matić, *Uvod u teoriju brojava*, Sveučilište Josipa Jurja Strossmayera u Osijeku - Odjel za matematiku, Osijek, 2015.

[14] S. Y. Yan, M. E. Hellman, *Number Theory for Computing*, Springer, Berlin, 2002.

Sažetak

U ovom radu upoznajemo se sa pseudoprostim brojevima i njihovim podvrstama. U početku se prisjećamo osnovnih definicija i svojstva. Sličnostima i razlikama samih pseudoprostih brojeva se bavimo u nastavku. Na kraju analiziramo probabilističke testove prostosti da bi utvrdili je li broj prosti ili nije. Sa svakim od njih ćemo povezati jednu vrstu pseudoprostih brojeva te kroz primjere pokazati kako testovi funkcioniraju.

Ključne riječi: Pseudoprosti brojevi, Carmichaelovi brojevi, Eulerovi pseudoprosti brojevi, jaki pseudoprosti brojevi, Lucasovi pseudoprosti brojevi, Superspseudoprosti brojevi, Fermatov test prostosti, Miller - Rabinov test prostosti, Pocklington - Lehmerov test prostosti, Solovay - Strassenov test prostosti

Pseudoprime numbers

Summary

In this work we introduce the pseudoprime numbers and their subtypes. At the beginning, we are reminded of the basic subtypes and properties. Simmilarities and differences between each pseudoprime number variations can be found later in the work. At the very end there are analyses of the probabilistic tests of the numbers' primality. Each of the tests is related to some type of the pseudoprime numbers and their manner of functioning is shown through examples.

Keywords: Pseudoprime numbers, Charmichael numbers, Euler pseudoprimes, strong pseudoprimes, Lucas pseudoprimes, superpseudoprimes, Fermat primality test, Miller Rabin primality test, Pocklington-Lehmer primality test, Solovay Strassen primality test

Životopis

Rođena sam 30. ožujka 1996. godine u Osijeku. U Bizovcu završavam Osnovnu školu Bratoljuba Klaića te 2010. godine upisujem Opću gimnaziju u Valpovu. Nakon mature, 2014. godine upisujem Preddiplomski studij matematike u Osijeku na Odjelu za matematiku. Naziv sveučilišne prvostupnice matematike stječem 2019. godine sa završnim radom Osnovna svojstva unitarnih prostora pod mentorstvom doc. dr. sc. Suzane Miodragović, te nakon toga nastavljam studij na Odjelu za matematiku na smjeru Financijska matematika i statistika. Od prosinca 2021. godine radim na održavanju bolničkog i laboratorijskog informatičkog sustava pri In2 grupi u Osijeku.