Pseudoprosti brojevi

Prgić, Magdalena

Undergraduate thesis / Završni rad

2019

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:126:017068

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

Magdalena Prgić

Pseudoprosti brojevi

Završni rad

Mentor: izv.prof.dr.sc. Ivan Matić

Osijek, 2019.

Sadržaj

Sažetak

U ovom završnom radu objasnit ćemo što su to pseudoprosti brojevi te navesti neka njihova svojstva. Spomenut ćemo i neke osnovne karakteristike Carmichaelovih brojeva, Eulerovih pseudoprostih brojeva i jakih pseudoprostih brojeva, te objasniti njihov međusobni odnos.

Ključne riječi: prosti brojevi, pseudoprosti brojevi, pseudoprosti brojevi u bazi b, Carmichaelovi brojevi, Eulerovi pseudoprosti brojevi, jaki pseudoprosti brojevi

Abstract

In this final paper we are going to explain what pseudoprime numbers are and bring up some of their characteristics. We will also explain what Carmichael numbers, Euler pseudoprimes and strong pseudoprimes are and how they are related.

Keywords: prime numbers, pseudoprimes, pseudoprimes in base b, Carmichael numbers, Euler pseudoprimes, strongpseudoprimes

1 Uvod

Cilj ovog završnog rada je proučiti značenje i osnovne karakteristike pseudoprostih brojeva kao i njihovu zastupljenost u teoriji brojeva te navesti neke načine kako doći do prostih i pseudoprostih brojeva. Kako bi za početak uopće mogli definirati pseudoproste brojeve, prvo ćemo morati definirati nekoliko fundamentalnih pojmova iz teorije brojeva. Nakon definiranja pseudoprostih brojeva, upoznat ćemo se sa nekim vrstama istih. Objasnit ćemo zašto su Carmichaelovi brojevi bitni i zanimljivi, te što su i kako su povezani Eulerovi i jaki pseudoprosti brojevi. Kako bi sadržaj ovog rada bio što bolje razumljiv, uz sve definicije bit će ilustrirani i lako shvatljivi primjeri.

2 Prosti brojevi

Pitanje je li određeni veliki prirodan broj n prost ili složen jedno je od najvažnijih u teoriji brojeva. Jedan od načina određivanja je li broj prost su testovi prostosti. To su kriteriji za koje vrijedi da ako ih n ne zadovolji, onda je n sigurno složen broj, a ako ih zadovolji, onda je velika vjerojatnost da će n biti prost. Što više testova n „prođe“, veća je vjerojatnost da je prost. No, ako govorimo o primjenama, najčešće ćemo se zadovoljiti brojevima za koja je velika vjerojatnost da su prosti. Pored testova prostosti postoje i brojni algoritmi za traženje prostih brojeva. Tzv. Eratostenovo sito* je jedan od najpoznatijih algoritama takvog tipa.

Definicija 2.1. *Neka su a i b cijeli brojevi te neka je $a \neq 0$. Kažemo da a dijeli b ako postoji cijeli broj d takav da vrijedi $b = a \cdot d$. Tada broj a nazivamo djeliteljem broja b.*

Definicija 2.2. *Prirodan broj p nazivamo prostim brojem ako je $p \geq 2$ i ako su 1 i p jedini pozitivni djelitelji od p. Prirodan broj n nazivamo složenim brojem ako je $n \geq 2$ i n nije prost.*

Definicija 2.3. *Za dva prirodna broja a i b kažemo da su relativno prosti ukoliko je njihov najveći zajednički djelitelj jednak 1. Pišemo $(a, b) = 1$.*

Definicija 2.4. *Neka je n prirodan broj te a i b cijeli brojevi. Ako n dijeli razliku $a - b$, tada kažemo da je a kongruentno b modulo n i pišemo $a \equiv b \pmod{n}$. U suprotnom kažemo da a nije kongruentno b modulo n.*

Propozicija 2.1. *Neka su a, b, c i d cijeli brojevi te n prirodan broj. Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, tada vrijedi: $a \pm c \equiv b \pm d \pmod{n}$ i $a \cdot c \equiv b \cdot d \pmod{n}$.*

Postoje važna svojstva prostih brojeva koja se lako mogu provjeriti, ali ih posjeduju i neki složeni brojevi. Mali Fermatov teorem nam daje tipičan primjer jednog takvog svojstva.

Teorem 2.1 (Mali Fermatov teorem). *Neka je p prost broj. Tada za svaki cijeli broj a, takav da su a i p relativno prosti, vrijedi $a^{p-1} \equiv 1 \pmod{p}$. Općenito, za svaki cijeli broj a vrijedi: $a^p \equiv a \pmod{p}$.*

Prema obratu gornjeg teorema možemo odrediti je li broj složen. Naime, ako postoji prirodan broj $a < n - 1$ takav da a^{n-1} nije kongruentan 1 modulo n, tada je n složen.

Primjer 2.1. $3^{340} \not\equiv 1 \pmod{341}$ *, iz čega slijedi da je* 341 *složen.*

Napomenimo još jednom kako vrijedi samo obrat teorema za dokazivanje složenosti broja, dok iz $a^{p-1} \equiv 1 \pmod{p}$ ne možemo sa sigurnošću zaključiti da je p prost, što možemo vidjeti i u sljedećem primjeru.

Primjer 2.2. $2^{560} \equiv 1 \pmod{561}$*, ali* $561 = 3 \cdot 11 \cdot 17$.

*vidjeti [1], str.157

3 Pseudoprosti brojevi

Ovo poglavlje započet ćemo takozvanom Kineskom slutnjom: „Prirodan broj p je prost ako i samo ako $2^p \equiv 2 \pmod{p}$." Navedena tvrdnja točna je samo u jednom smjeru. Naime, ako je p prost broj, kongruencija vrijedi. No, obrnuto ne možemo tvrditi sa sigurnošću, što je Sarrus[†] 1819. godine i dokazao pronašavši kontraprimjer: $2^{341} \equiv 2 \pmod{341}$, ali je $341 = 11 \cdot 31$.
Svojstvo kongruencija koje glasi: "Ako je $ax \equiv ay \pmod{n}$, tada vrijedi $x \equiv y \pmod{\frac{n}{(a,n)}}$.", omogućuje nam da kongruenciju iz Kineske slutnje, ukoliko je p neparan broj, napišemo u obliku $2^{p-1} \equiv 1 \pmod{p}$. Sada možemo prijeći na definiciju pseudoprostih brojeva.

Definicija 3.1. *Neparne složene brojeve n za koje je $2^{n-1} \equiv 1 \pmod{n}$ nazivamo pseudoprosti brojevi.*

Primjer 3.1. *Lako se pokaže da brojevi $561, 645, 1729, 1905, \ldots$ zadovoljavaju kongruenciju iz prethodne definicije.*

Propozicija 3.1. *Ako je n pseudoprost broj, tada je $n' = 2^n - 1$ također pseudoprost.*

Dokaz. Kako je n pseudoprost, $n \mid 2^{n-1} - 1$ pa $n \mid 2^n - 2 = n' - 1$. Dakle, $n' - 1 = k \cdot n$, gdje je $k \in \mathbb{N}$. Sada imamo:

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

Dakle, $n' = 2^n - 1$ dijeli $2^{n'-1} - 1$ pa je i n' pseudoprost broj. □

Definicija 3.2. *Neparan složen broj n koji zadovoljava kongruenciju $a^{n-1} \equiv 1 \pmod{n}$, gdje je $a \neq 1$ cijeli broj i $(a, n) = 1$, nazivamo pseudoprostim brojem u bazi a.*

Pseudoprosti brojevi u bazi a ponašaju se kao prosti, tj. prolaze test prostosti. Ovakve brojeve često nazivamo i Fermatovim pseudoprostim brojevima. Postojanje pseudoprostih brojeva u bazi a pokazuje da nije dovoljno testirati neki broj n u samo jednoj bazi kako bi mogli zaključiti je li on prost.

Primjer 3.2. *Vrijedi $3^{90} \equiv 1 \pmod{91}$, ali ako pogledamo $2^{90} \not\equiv 1 \pmod{91}$. Iz ovoga možemo zaključiti da 91 nije prost broj. Zaista, $91 = 7 \cdot 13$.*

Teorem 3.1. *Za svaki prirodan broj $a \geq 2$ postoji beskonačno mnogo pseudoprostih brojeva u bazi a.*

Dokaz. Neka je p proizvoljan neparan prost broj koji ne dijeli $a^2 - 1$. Promotrimo prirodan broj $n = \frac{a^{2p}-1}{a^2-1}$. Kako vrijedi

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

slijedi da je n složen broj. Iz Malog Fermatovog teorema i Propozicije 1.1. slijedi da je $a^{2p} \equiv a^2 \pmod{p}$. Dakle, p dijeli $a^{2p} - a^2 = (n-1)(a^2-1)$. Kako p ne dijeli $a^2 - 1$, zaključujemo da p dijeli $n - 1$. 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 $a^{n-1} \equiv 1 \pmod{n}$. To znači da je n pseudoprost u bazi a. Kako ima beskonačno mnogo prostih brojeva, ima i beskonačno mnogo pseudoprostih brojeva u bazi a. □

[†]Pierre Frederic Sarrus - francuski matematičar

3.1 Carmichaelovi brojevi

Definicija 3.3. *Složen broj n nazivamo Carmichaelovim[‡] brojem ako za svaki cijeli broj a, takav da je $1 < a < n$ i $(a, n) = 1$, vrijedi $a^{n-1} \equiv 1 \pmod{n}$.*

Dakle, postoje brojevi koji su pseudoprosti u svakoj bazi. Carmichael pronašao je prvih 15 takvih brojeva: $561, 1105, 1729, 2465, 2821, 6601, \ldots$ i pretpostavio kako ih ima beskonačno mnogo.

Definicija 3.4. *Kažemo da je neki broj n kvadratno slobodan ako je 1 najveći kvadrat koji dijeli n.*

Teorem 3.2 (Korseltov[§] kriterij). *Ako je n kvadratno slobodan, tada je n Carmichaelov broj ako i samo ako za svaki prost faktor p od n vrijedi $p - 1 \mid n - 1$.*

Primjer 3.3.

$$\begin{aligned}
561 &= 3 \cdot 11 \cdot 17 \quad (2 \mid 560; 10 \mid 560; 16 \mid 560)\\
1105 &= 5 \cdot 13 \cdot 17 \quad (4 \mid 1104; 12 \mid 1104; 16 \mid 1104)\\
1729 &= 7 \cdot 13 \cdot 19 \quad (6 \mid 1728; 12 \mid 1728; 18 \mid 1728)\\
2465 &= 5 \cdot 17 \cdot 29 \quad (4 \mid 2464; 16 \mid 2464; 28 \mid 2464)\\
2821 &= 7 \cdot 13 \cdot 31 \quad (6 \mid 2820; 12 \mid 2820; 30 \mid 2820)\\
6601 &= 7 \cdot 23 \cdot 41 \quad (6 \mid 6600; 22 \mid 6600; 40 \mid 6600)\\
8911 &= 7 \cdot 19 \cdot 67 \quad (6 \mid 8910; 18 \mid 8910; 66 \mid 8910)
\end{aligned}$$

Propozicija 3.2. *Svaki Carmichaelov broj je produkt najmanje tri međusobno različita prosta broja.*

Dokaz. Pretpostavimo da je Carmichaelov broj n produkt točno dva prosta broja, tj. neka je $n = p \cdot q$, gdje su p i q dva različita prosta broja t.d. je $p < q$. Slijedi da $q - 1 \mid n - 1$, tj. da je $n - 1 \equiv 0 \pmod{q - 1}$. Ali

$$n - 1 = p(q - 1 + 1) - 1 = p(q - 1) + p - 1 \equiv p - 1 \pmod{q - 1}$$

pa kako je $p - 1 < q - 1$, slijedi $p - 1 \not\equiv 0 \pmod{q - 1}$, što nas dovodi do kontradikcije. □

Primjer 3.4. *Prvi Carmichaelovi brojevi sa $k = 3, 4, 5, 6, 7, 8, 9$ prostih faktora*

$$\begin{aligned}
561 &= 3 \cdot 11 \cdot 17\\
41041 &= 7 \cdot 11 \cdot 13 \cdot 41\\
825265 &= 5 \cdot 7 \cdot 17 \cdot 19 \cdot 73\\
321197185 &= 5 \cdot 19 \cdot 23 \cdot 29 \cdot 37 \cdot 137\\
5394826801 &= 7 \cdot 13 \cdot 17 \cdot 23 \cdot 31 \cdot 67 \cdot 73\\
232250619601 &= 7 \cdot 11 \cdot 13 \cdot 17 \cdot 31 \cdot 37 \cdot 73 \cdot 163\\
9746347772161 &= 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 641
\end{aligned}$$

[‡]Robert Daniel Carmichael, američki matematičar, 1879-1967
[§]Alwin Reinhold Korselt, njemački matematičar, 1864-1947

3.2 Eulerovi pseudoprosti brojevi

Eulerov kriterij, kojeg ćemo u ovom poglavlju iskazati, također se koristi kao test prostosti, kako bi se pokazalo da neki neparan prirodan broj nije prost. No, najprije moramo definirati neke nove pojmove koji će nam trebati u ovom poglavlju.

Definicija 3.5. *Neka su a i n relativno prosti prirodni brojevi. Ako kongruencija*

$$x^2 \equiv a \pmod{n}$$

ima rješenja, tada kažemo da je a kvadratni ostatak modulo n. U suprotnom kažemo da je a kvadratni neostatak modulo n.

Definicija 3.6. *Neka je p neparan prost broj i a cijeli broj. Legendreov simbol $\left(\frac{a}{p}\right)$ definiran je na sljedeći način:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ kvadratni ostatak modulo } p \\ 0, & p \mid a \\ -1, & a \text{ kvadratni neostatak modulo } p \end{cases}$$

Primjer 3.5. $\left(\frac{2}{11}\right) = -1$ *jer je 2 kvadratni neostatak modulo 11. S druge strane,* $\left(\frac{3}{11}\right) = 1$ *jer je* $5^2 \equiv 3 \pmod{11}$.

Propozicija 3.3. *Neka je p neparan prost broj i a cijeli broj koji je relativno prost sa p. Tada vrijedi:* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Generalizacija Legendreovog simbola je Jacobijev simbol $\left(\frac{a}{n}\right)$, gdje je a proizvoljan cijeli broj i n neparan prirodan broj. Ukoliko je $n = p_1 p_2 \cdots p_k$ faktorizacija od n na međusobno različite neparne proste brojeve, onda definiramo Jacobijev simbol kao $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$, gdje su $\left(\frac{a}{p_i}\right)$ pripadni Legendreovi simboli za $i = 1, 2, \ldots, k$.

Primjer 3.6. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$. *Vidimo da, za složene brojeve kao što je 15,* $\left(\frac{2}{15}\right) = 1$ *ne znači da je 2 kvadratni ostatak modulo 15, jer* $x^2 \equiv 2 \pmod{15}$ *nema rješenje.*

Teorem 3.3 (Eulerov kriterij). *Neka je p neparan prost broj koji ne dijeli a. Ako je a kvadratni ostatak modulo p, onda* $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. *U suprotnom, ako je a kvadratni neostatak modulo p onda* $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Definicija 3.7. *Neka je b proizvoljan cijeli broj. Neparan pozitivan složen broj n koji je relativno prost sa b nazivamo Eulerov pseudoprost broj u bazi b ako* $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$.

Primjer 3.7.

n	*Eulerovi pseudoprosti brojevi u bazi n*
1	9, 15, 21, 25, 27, 33, 35, 39, 45, 51, ...
2	561, 1105, 1729, 1905, 2047, 2465, 3277, 4033, 4681, 5461, ...
3	121, 703, 1541, 1729, 1891, 2465, 2821, 3281, 4961, 7381, ...
4	341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, ...
5	217, 781, 1541, 1729, 5461, 5611, 6601, 7449, 7813, ...
6	185, 217, 301, 481, 1111, 1261, 1333, 1729, 2465, 2701, ...
7	25, 325, 703, 817, 1825, 2101, 2353, 2465, 3277, 4525, ...
8	9, 21, 65, 105, 133, 273, 341, 481, 511, 561, ...
9	91, 121, 671, 703, 949, 1105, 1541, 1729, 1891, 2465, ...
10	9, 33, 91, 481, 657, 1233, 1729, 2821, 2981, 4187, ...
11	133, 305, 481, 645, 793, 1729, 2047, 2257, 2465, 4577, ...
12	65, 91, 133, 145, 247, 377, 385, 1649, 1729, 2041, ...

3.3 Jaki pseudoprosti brojevi

Neka je n neparan prirodan broj i $b < n$ prirodan broj koji je relativno prost sa n. Neka je n pseudoprost u bazi b, tj. neka vrijedi $b^{n-1} \equiv 1 \pmod{n}$. Ako je n prost broj, slijedi da je $b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$ jer jedini korijeni od 1 u $\mathbb{Z}$ su ± 1. Nadalje, ako je $b^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ i ako je $\frac{n-1}{2}$ parno, slijedi $b^{\frac{n-1}{4}} \equiv \pm 1 \pmod{n}$, itd. To nas motivira za sljedećom definicijom.

Definicija 3.8. *Neka je n neparan prirodan broj koji nije prost i $b < n$ prirodan broj koji je relativno prost sa n. Definiramo n kao $n = 2^s t + 1$, gdje je t neparan. Tada kažemo da je takav n jaki pseudoprost broj u bazi b ukoliko vrijedi jedna od sljedećih tvrdnji: ili*

$$b^t \equiv 1 \pmod{n},$$

ili postoji nenegativan $r < s$ takav da

$$b^{2^r t} \equiv -1 \pmod{n}.$$

Primjer 3.8. *Broj 25 je jaki pseudoprost broj u bazi 7. Doista, $7^2 = 49 \equiv -1 \pmod{25}$ pa je i $7^{12} = 7^{\frac{25-1}{2}} \equiv 1 \pmod{25}$.*

Primjer 3.9. *2047 je najmanji jaki pseudoprost broj u bazi 2.*
Primjetimo, $\frac{2047-1}{2} = \frac{2046}{2} = 1023 = 11 \cdot 93$. Sada je $2^{11} = 2048 \equiv 1 \pmod{2047}$, pa tada i $2^{2046} \equiv 1 \pmod{2047}$.

Sljedeće dvije propozicije govore o odnosu jakih i Eulerovih pseudoprostih brojeva.

Propozicija 3.4. *Neka je n neparan prirodan broj i $b < n$ pozitivan 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. $\boxed{\Rightarrow}$ Zadržavajući oznake iz Definicije 3.7., ako je $n \equiv 3 \pmod{4}$, s mora biti jednak 1. Tada je n jaki pseudoprost broj u bazi b ako i samo ako vrijedi

$$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}. \tag{3.1}$$

Sada, 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 (3.1) i n je jaki pseudoprost broj.
$\boxed{\Leftarrow}$ Neka je n jaki pseudoprost broj u bazi b. Iz $n \equiv 3 \pmod{4}$ slijedi

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

pa je

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

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

Propozicija 3.5. *Neka je n neparan pozitivan broj i $b < n$ pozitivan broj koji je relativno prost sa n. Ako je n jaki pseudoprost broj u bazi b, tada je n i Eulerov pseudoprost broj u bazi b.*

Literatura

[1] M. W. Baldoni, C. Ciliberto, G.M. Piacentini Cattaneo, *Elementary number theory, cryptography and codes*, Springer Verlag, 2009

[2] L. N. Childs, *A Concrete Introduction to Higher Algebra*, Springer, 2009

[3] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, 1994

[4] I. Matić, *Uvod u teroju brojeva*, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, 2013