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

Magdalena Moguš

Testovi prostosti

Završni rad

Osijek, 2022.

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

Magdalena Moguš

Testovi prostosti

Završni rad

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

Osijek, 2022.

Sažetak: Tema ovog rada bit će testovi prostosti. Testove prostosti dijelimo na determinističke i vjerojatnosne. Sukladno tome, rad je podijeljen na dva dijela. Najprije ćemo obraditi probno dijeljenje, Wilsonov teorem, Lucas-Lehmerov test, Pepinov test, AKS test te GK i ECPP algoritme koji pripadaju determinističkim testovima prostosti. Zatim ćemo obraditi Frematov test prostosti, Jaki Frematov test, Pocklington–Lehmerov test, Miller-Rabinov test i Solovay-Strassenov test prostosti koji pripadaju vjerojatnosnim testovima prostosti. Za svaki test, osim njega samog, navest ćemo i njegovu efikasnost te za većinu testova, primjere njihove upotrebe.

Ključne riječi: prosti brojevi, složeni brojevi, pseudoprosti brojevi, jaki pseudoprosti brojevi

Primality Testing

Abstract: The topic of this paper will be primality testing. There are two types of primality tests: deterministic and probabilistic. Accordingly, the paper is divided into two sections. First section covers deterministic tests. Here we have trial division, Wilson's theorem, Lucas-Lehmer test, Pepin test, AKS test and GK and ECPP algorithms. Second section covers probabilistic tests. Here we have Fermat Primality test, Strong Fermat test, Pocklington–Lehmer test, Miller-Rabin test and Solovay-Strassen test. For each test, except itself, we give its efficiency. For most of the test, we give the examples of their use.

Keywords: prime numbers, composite numbers, pseudoprime numbers, strong pseudoprime numbers

Sadržaj

Uvod

Jedan od središnjih pojmova u teoriji brojeva su prosti brojevi. Prisjetimo se, za prirodan broj n kažemo da je **prost** ako su mu jedini djelitelji broj 1 i on sam. U suprotnom kažemo da je n **složen** broj. Broj 1 nije niti prost niti složen.

Zbog svojih lijepih svojstava, prosti su brojevi oduvijek privlačili pažnju matematičara i time imali vrlo važnu ulogu u razvoju teorije brojeva. Još je oko 300. g. pr. Kr. Euklid pokazao da prostih brojeva ima beskonačno mnogo.[1] Još veći interes za prostim brojevima, točnije za pronalaskom načina kako pokazati da je neki broj prost, došao je razvojem kriptografije[2] i kriptografskih metoda (preciznije, razvojem RSA kriptosustava[3], gdje su potrebni prosti brojevi s više od 150 znamenki). Te brojeve tražimo tako da provjeravamo prostost brojeva od nekog slučajno odabranog broja pa na dalje koristeći jedan od testova prostosti.

Testovi prostosti su teorijski rezultati koji sadrže kriterije prostih brojeva. Razlikujemo **determinističke** i **vjerojatnosne** testove prostosti. Deterministički testovi prostosti su formulirani tako da će broj n proći test ako i samo ako je prost. Vjerojatnosni testovi prostosti su formulirani tako da ako ih neki broj n ne prođe, onda je on sigurno složen, ali ako ga prođe onda je *vjerojatno prost*. Što više vjerojatnosnih testova broj prođe, to je veća vjerojatnost da je prost.

Vjerojatnosni testovi su u praksi puno brži od deterministič kih. Brzina testa, odnosno složenost pripadnog algoritma, mjeri se u graničnom broju operacija koje je potrebno izvršiti. Uvedimo najprije oznaku $\mathcal{O}$ koju koristimo za granični broj operacija, to jest složenost algoritma.

Definicija. *Neka su $f, g : S \to \mathbb{R}$ dane funkcije, pri čemu je S je neki podskup od $\mathbb{R}$ (najčeće je $S = \mathbb{N}$). Tada pišemo $f(n) = \mathcal{O}(g(n))$ ako postoje konstante $B, C > 0$ takve da je $|f(n)| \leq C|g(n)|$, za sve $n \in S$ takve da je $n > B$.*

Za algoritam kažemo da je **polinomijalan** ako mu je, uz činjenicu da mu je ulazni podatak prirodan broj n, broj operacija potrebnih za izvršavanje jednak $\mathcal{O}(n^k)$, gdje je $k > 0$ neka pozitivna konstanta.

Obzirom na to da postoje dvije vrste testova prostosti, rad je podijeljen na dva dijela. U prvom poglavlju rada obradit ćemo neke deterministič ke testove prostosti i to probno dijeljenje (i pojam Eratostenovog sita), test baziran na Wilsonovom teoremu i njegovom obratu, Lucas-Lehmerov test prostosti, Pepinov test prostosti i AKS test prostosti te ćemo spomenuti testove prostosti koji koriste elipič ke krivulje (GK i ECPP algoritme). U drugom poglavlju ćemo obraditi neke vjerojatnosne testove prostosti. To su Fermatov test pseudoprostosti, Jaki Fermatov test, Pocklington-Lehmerov test prostosti, Miler-Rabinov test i Solovay-Strassenov test prostosti. Mada su ovi testovi dizajnirani za velike brojeve, za ilustraciju primjene većine testova u radu korišteni su mali brojevi. Osim primjera korištenja, za većinu testova navedena je i složenost pripadnog algoritma.

[1] Vidi [10], Theorem 1.2.3.

[2] Više o kriptografiji moguće je pronaći u [3], 1. Klasična kriptografija, 1.1. Osnovni pojmovi.

[3] Više o RSA kriptosustavu moguće je pronaći u [3], 3.2. RSA kriptosustav

1. Deterministički testovi prostosti

1.1. Probno dijeljenje i Eratostenovo sito

Najjednostavniji deterministički test prostosti je **probno dijeljenje**. Ovaj se test zasniva na sljedećem teoremu.

Teorem 1.1 (vidi [10], Theorem 2.2.1.)**.** *Neka je n prirodan broj, $n > 1$. Ako n nema niti jedan prost faktor koji je manji ili jednak od $\sqrt{n}$, onda je n prost broj.*

Dokaz. Neka je $n > 1$ prirodan broj koji nema niti jedan prost faktor koji je manji ili jednak od $\sqrt{n}$ i pretpostavimo da je n složen broj. Tada postoje prirodni brojevi k i l, $1 < k, l < n$, takvi da je $n = kl$. Obzirom na to da je $n = \sqrt{n} \cdot \sqrt{n}$, slijedi da je $k \leq \sqrt{n}$ ili $l \leq \sqrt{n}$. Bez smanjenja općenitosti pretpostavimo da je $k \leq \sqrt{n}$. Prema pretpostavci teorema, k ne može biti prost. Dakle, k je složen. Kako je k složen, mora postojati neki njegov prost faktor q takav da je $q < k$. Dakle imamo $q < k \leq \sqrt{n}$ i q je prost broj. To je u kontradikciji s pretpostavkom teorema. Dakle, n je prost. Za slučaj $l \leq \sqrt{n}$, dokaz ide analogno. □

Ovaj teorem nam kaže da je dovoljno podijelti broj n, za kojeg želimo provjeriti je li prost, sa svim prostim brojevima koji su manji ili jednaki od $\sqrt{n}$. Ako broj n nije djeljiv niti s jednim od tih brojeva, onda je on prost.

Primjer 1.1. *Pokažimo da je $n = 223$ prost broj. Kako je $\sqrt{223} \approx 14.93$, sve što trebamo napraviti je podijeliti broj 223 s prostim brojevima od broja 1 do broja 14, tj. sa brojevima $2, 3, 5, 7, 11$ i 13. Kako broj 223 nije djeljiv ni s jednim od tih brojeva, prema Teoremu 1.1, on je prost broj.*

Za male brojeve, taj je test primjenjiv, no za velike brojeve, kakvi se, na primjer, koriste u RSA kriptosustavu, ovaj test nije praktičan jer oduzima previše vremena. Potrebno je $\mathcal{O}(\sqrt{n}\log(n))$ operacija[4] da bi se ovom metodom provjerila prostost danog broja.

Teorem 1.1 se može iskoristiti i u generiranju tablice prostih brojeva metodom **Eratostenovog sita**. Pretpostavimo da želimo napraviti tablicu svih prostih brojeva do nekog prirodnog broja n. Najprije ispišemo sve brojeve od 2 do n. U prvom koraku označimo broj 2 te prolazimo redom tablicom i križamo sve višekratnike broja 2. U svakom novom koraku prvi neprekriženi broj je prost, njega označimo te križamo sve njegove višekratnike. U drugom kroraku je to broj 3. Broj 4 je prekrižen kao višekratnik od 2. Broj 5 je neprekrižen pa je prost. Broj 6 je prekrižen kao višekratnik od 3. Nakon njega slijedi neprekriženi broj 7. Nastavljamo postupak do broja koji je manji ili jednak od $\sqrt{n}$, točnije do broja $\lfloor\sqrt{n}\rfloor$. Kada prekrižimo sve višekratnike broja $\lfloor\sqrt{n}\rfloor$, preostali neprekriženi brojevi u tablici su prosti.

1.2. Wilsonov teorem

Prisjetimo se Wilsonovog teorema.

Teorem 1.2 (Wilsonov teorem; vidi [8], Teorem 2.3.1.)**.** *Ako je p prost broj, onda je*

$$(p-1)! \equiv -1 \pmod{p}.$$

Vrijedi i obrat koji je iskazan u sljedećoj propoziciji.

Propozicija 1.1 (vidi [8], Propozicija 2.3.2.)**.** *Ako za prirodan broj n vrijedi da je*

[4] Vidi [3].

$$(n-1)! \equiv -1 \pmod{n},$$

onda je n prost broj.

Dakle, dobili smo sljedeću karakterizaciju prostog broja: broj n je prost ako i samo ako vrijedi

$$(n-1)! \equiv -1 \pmod{n}.$$

Stoga, da bi odredili je li neki dani broj n prost, treba izačunati $(n-1)! \mod n$. No i ova metoda je vrlo spora i neefikasna za velike brojeve jer zahtjeva velik broj koraka. Pokažimo primjenu ovog testa na primjeru malog broja.

Primjer 1.2. *Koristeći se upravo izrečenom karakterizacijom, pokažimo da je $n = 11$ prost broj.*

Dakle, 11 *je prost broj ako i samo ako je*

$$(11-1)! = 10! \equiv -1 \pmod{11}.$$

Kako je $10! = 10 \cdot 9 \cdots 2 \cdot 1$ *i vrijedi*

$$\begin{aligned} 10 &\equiv -1 \pmod{11}, \\ 9 &\equiv -2 \pmod{11}, \\ 8 &\equiv -3 \pmod{11}, \\ 7 &\equiv -4 \pmod{11}, \\ 6 &\equiv -5 \pmod{11}, \end{aligned}$$

imamo

$$\begin{aligned} 10 \cdot 9 \cdots 2 \cdot 1 &\equiv (-1) \cdot (-2) \cdot (-3) \cdot (-4) \cdot (-5) \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \pmod{11} \\ &\equiv -5^2 \cdot 4^2 \cdot 3^2 \cdot 2^2 \pmod{11} \\ &\equiv (-3) \cdot 5 \cdot (-2) \cdot 4 \pmod{11} \\ &\equiv 10 \pmod{11} \\ &\equiv -1 \pmod{11} \end{aligned}$$

to jest

$$10! \equiv -1 \pmod{11}.$$

Sada ćemo se baviti puno bržim deterministčkim testovima. Najprije pogledajmo testove za posebne brojeve - Fermatove i Mersennove.

1.3. Lucas-Lehmerov test prostosti

Lucas-Lehmerov test prostosti se koristi za provjeravanje prostosti Mersennovih brojeva. **Mersennovi brojevi**[5] su brojevi oblika

$$M_p = 2^p - 1,$$

[5]Brojevi nazvani prema francuskom redovniku Marinu Mersennu. Za više informacija o Mersennovim brojevima vidi [8], str. 17 i 18 ili [7], poglavlje 2.9.

gdje je p prost broj. Među tim brojevima ima i prostih i složenih. Ako je broj M_p prost, on se naziva **Mersennov prost broj**. Može se pokazati da, ako je M_n Mersennov prost broj, onda je n prost.[6]

Test je nazvan po francuskom matematičaru Édouardu Lucasu i američkom matematičaru Derricku H. Lehmeru. Lucas je otkrio temeljnu ideju 1876. godine, a Lehmer je 1930. godine nadogradio metodu.

Sljedeći nam teorem daje karakterizaciju Mersennovih prostih brojeva.

Teorem 1.3 (Lucas-Lehmerov test; vidi [7], Proposition 14.8.)**.** *Neka je p prost broj. Definiramo niz induktivno*

$$s_0 = 4, \tag{1}$$
$$s_{i+1} = s_i^2 - 2, \tag{2}$$

pri čemu je $i = 0, 1, 2, 3, \ldots$ Tada vrijedi: broj M_p je prost ako i samo je

$$s_{p-2} \equiv 0 \pmod{M_p}. \tag{3}$$

Napomena 1.1. *Niz $(s_i)_{i\geq 0}$ definiran u Teoremu 1.3 naziva se Lucas-Lehmerov niz.*[7]

Ilustrirajmo primjenu ovog testa sljedećim primjerom.

Primjer 1.3. *Provjerimo prostost Mersennovih brojeva za $p = 3$ i $p = 5$. Nađimo najprije Lucas-Lehmerov niz do s_3. Imamo*

$$\begin{aligned} s_0 &= 4, \\ s_1 &= 4^2 - 2 = 14, \\ s_2 &= 14^2 - 2 = 194, \\ s_3 &= 194^2 - 2 = 37634. \end{aligned}$$

Za $p = 3$ i $M_3 = 2^3 - 1 = 7$ treba provjeriti vrijedi li

$$s_1 \equiv 0 \pmod{M_3},$$

to jest je li

$$14 \equiv 0 \pmod{7}.$$

Kako $7 \mid 14$, prethodna kongruencija je zadovoljena, pa je $M_3 = 7$ Mersennov prost broj prema Teoremu 1.3.

Za $p = 5$ i $M_5 = 2^5 - 1 = 31$ treba provjeriti je li

$$s_3 \equiv 0 \pmod{M_5},$$

to jest vrijedi li

$$37634 \equiv 0 \pmod{31}.$$

Zaista, $31 \mid 37634$ pa je prethodna kongruencija zadovoljena. Odnosno $M_5 = 31$ je Mersennov prost broj prema Teoremu 1.3.

[6] Vidi [8], Propozicija 1.4.11.

[7] Vidi [10], str 251. U ovom je izvoru niz označen s L_i.

Ovaj test je vrlo efikasan jer je brz. Za testiranje jednog Mersennovog broja M_n, pripadnom algoritmu potrebno je $\mathcal{O}(n^3)$ koraka da bi odredio je li uneseni broj prost ili nije.[8] Primjetimo da broj koraka ne ovisi o samom broju M_n kojeg testiramo, kao kod ostalih testova, već o broju n.

Lucas-Lehmerov test prostosti koristi se kao alat u otkrivanju Mersennovih prostih brojeva u GIMPS projektu ("The Great Internet Mersenne Prime Search").[9] U sklopu tog projekta, 7. prosinca 2018. godine otkriven je do sada najveći poznati prost broj, ali i najveći Mersennov prost broj, i to je broj

$$M_{82589933} = 2^{82589933} - 1$$

koji ima čak 24862048 znamenki. To je tek 51. poznati Mersennov prost broj.[10]

Mada se čini da je brojka 51 mala, poznatih Mersennovih prostih brojeva je daleko više od poznatih prostih Fermatovih brojeva, koji su tema sljedećeg potpoglavalja.

1.4. Pépinov test

Fermatovi brojevi[11] su brojevi oblika

$$F_n = 2^{2^n} + 1,$$

gdje je n prirodan broj.

Zanimljiva činjenica je da su jedini dosada dokazani prosti Fermatovi brojevi F_0, F_1, F_2, F_3 i F_4. Dakle, najveći poznati Fermatov prost broj je $F_4 = 65537$. Za $n = 5, \ldots, 11$ dokazano je da je F_n složen i pronađena je njihova faktorizacija. Osim toga, pokazano je za još neke Fermatove brojeve da su prosti, ali im još nije pronađena faktorizacija. Upravo zato, vjeruje se da niti jedan broj F_n, za $n \geq 5$, nije prost.[12] Međutim, ta tvrdnja još nije pokazana.

Alat kojim možemo provjeriti je li neki Fermatov broj prost ili ne naziva se Pépinov test[13] i iskazan je u sljedećoj propoziciji.

Propozicija 1.2 (Pépinov test; vidi [7], Proposition 14.7.)**.** *Neka je n prirodan broj. Fermatov broj F_n je prost ako i samo ako vrijedi*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}. \tag{4}$$

Ilustrirajmo primjenu ovoga testa sljedećim primjerom.

Primjer 1.4. *Neka je $n = 2$. Koristeći Pépinov test, pokažimo da je broj $F_2 = 2^{2^2} + 1 = 17$ prost broj.*

Prema prethodnoj propoziciji, treba pokazati da je

$$3^{\frac{17-1}{2}} \equiv -1 \pmod{17},$$

[8] Vidi [10], Algoritam 2.2.3.

[9] Vidi [7], str. 346.

[10] Vidi [5]. Tu je moguće pronaći i više informacija o samom projektu.

[11] Brojevi nazvani po francuskom pravniku i matematičaru iz hobija, Pierre de Fermatu. Za više informacija o Fermatovim brojevima vidi npr. [8], str. 15 i 16 ili [7], poglavlje 2.9.

[12] Vidi [7].

[13] Nazvan po francuskom matematičaru J. F. T. Pépinu.

odnosno da je

$$3^8 \equiv -1 \pmod{17}.$$

Kako je $3^3 = 27 \equiv 10 \pmod{17}$*, imamo*

$$3^8 = 3^3 \cdot 3^3 \cdot 3^2 \equiv 10 \cdot 10 \cdot 9 = 900 \equiv 16 \equiv -1 \pmod{17}$$

što je i trebalo pokazati.

Broj operacija potrebnih za provođenjeg ovog testa, odnosno za računanje izraza (4) je $\mathcal{O}(F_n)$.[14]

1.5. AKS test prostosti

Agrawal - Kayal - Saxena test prostosti, ili kraće AKS test, je deterministički test prostosti objavljen 6. kolovoza 2002. godine u članku *"Primes is in P"* (vidi [1]), a njegovi autori su matematičari i računalni znanstvenici Manindra Agrawal, Neeraj Kayal i Nitin Saxena sa Indijskog instituta za tehnologiju Kanpur.[15] Ovaj test, odnosno njemu pripadni algoritam, koji će biti naveden u nastavku, ubraja se u polinomijalne algoritme.[16] Kod originalnog AKS testa, broj koraka ograničen je s $\mathcal{O}(\log_2^{\frac{21}{2}+\epsilon}(n))$, za neki $\epsilon > 0$.[17]

Bazu AKS testa čini sljedeći teorem.

Teorem 1.4 (vidi [9], Lemma 2.10)**.** *Neka je* $n > 1$ *neparan prirodan broj i neka je* a *cijeli broj takav da je* $(a, n) = 1$*. Tada je* n *prost broj ako i samo ako vrijedi*

$$(x + a)^n \equiv x^n + a \pmod{n}.$$

Primijetimo da je kongruencija iz Teorema 1.4 zapravo jednakost u prstenu polinoma $\mathbb{Z}_n[x]$, pri čemu je $\mathbb{Z}_n = \{0, \ldots, n-1\}$. Ako bismo kongruenciju rješavali u kvocijentnom prstenu $\mathbb{Z}_n[x]/(x^r - 1)$, ona bi bila oblika

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}.^{18} \tag{5}$$

Dakle, njezino rješavanje bi ovisilo o stupnju r, a time bi i vrijeme potrebno za izvršavanje algoritma, koji se temelji na ovom teoremu, ovisilo o stupnju r. Navedimo sada spomenuti algoritam.[19]

AKS algoritam: Neka je $n > 1$ cijeli broj.

1. Ako je n potpun kvadrat, vrati SLOŽEN.
2. Pronaći najmanji r takav da je $\text{ord}_r(n) > \log_2^2(n)$.[20]
3. Ako je $1 < (a, n) < n$, za neki $a < r$, vrati SLOŽEN.

[14] Vidi [10], str. 205.
[15] Vidi [9], 2.6. AKS primality test.
[16] Vidi [7], str. 327.
[17] Vidi [1], Theorem 5.1.
[18] Kongruencija (5) je kongruencija u polinomima. Ostatak pri dijeljenju polinoma $(x + a)^n - (x^n + a)$ s polinomom $x^r - 1$ je polinom s koeficijentima koji su svi djeljivi s n.
[19] Algoritam je preuzet iz [1].
[20] Za prirodan broj r i cijeli broj a, **red od** a **modulo** r je najmanji prirodan broj k takav da je $a^k \equiv 1 \pmod{r}$ i označava se s $\text{ord}_r(a)$.

4. Ako je $n \leq r$, vrati PROST.

5. Za brojeve $a = 1, \ldots, \lfloor \sqrt{\phi(n)} \log_2(n) \rfloor$, ako je $(x+a)^n \not\equiv x^n + a \pmod{x^r - 1, n}$, vrati SLOŽEN.

6. Vrati PROST.

Mada je ovaj algoritam temeljen na Teoremu 1.4, koji u sebi sadrži i nužan i dovoljan uvjet prostosti, potrebno je dodatno pokazati da će navedeni algoritam vratiti PROST ako i samo ako je broj koji testiramo uistinu prost. Taj je dokaz složen i nećemo ga navoditi u ovom radu. U originalnom članku, *"Primes is in P"*, ta je tvrdnja iskazana u Teoremu 4.1., a dokaz je naveden kroz dokaze Lema 4.2. i 4.3. te Lema 4.5. do 4.9.

Kao što je već navedeno, vrijeme potrebno za izvršavanje algoritma određeno je stupnjem r polinoma $x^r - 1$ u kongruenciji (5). Agrawal, Kayal i Saxena su pokazali da za r vrijedi sljedeća ocjena:

$$r \leq \max(3, \lceil \log_2^5(n) \rceil).^{21}$$

Idealan slučaj bi bio kada bi vrijedilo da je $r = \mathcal{O}(\log_2^2(n))$ jer bi u tom slučaju vrijeme potrebno za izvršenje algoritma bilo $\mathcal{O}(\log_2^{6+\epsilon}(n))$ koraka, za neki $\epsilon > 0$. Ta vrijednost broja r može biti ostvarena uz uvjet da vrijedi jedna od sljedeće dvije pretpostavke:[22]

1. (**Artinova pretpostavka**) Za prirodan broj n s m znamenki koji nije potpun kvadrat, broj prostih brojeva q takvih da je $q \leq m$, za koje vrijedi $\mathrm{ord}_q(n) = q-1$, je asimptotski jednak $A(n) \cdot \frac{m}{\ln m}$, gdje je $A(n)$ Artinova konstanta za koju vrijedi $A(n) > 0.35$.

2. (**Sophie-Germain pretpostavka o gustoći prostih brojeva**) Broj prostih brojeva $q \leq m$, takvih da je i $2q + 1$ također prost broj, je asimptotski jednak $\frac{2mC_2}{\ln^2(m)}$, gdje je C_2 konstanta koja približno iznosi 0.66.

Artinova pretpostavka vrijedi ako je zadovoljena Generalizirana Riemmanova hipoteza (GRH).[23]

1.6. Testiranje prostosti pomoću eliptičkih krivulja

Jedan od najpraktičnijih načina testiranja prostosti je ECPP ("Elliptic Curve Primality Proving") algoritam koji koristi eliptičke krivulje, točnije njihova svojstva nad konačnim poljima vezanim uz kompleksno množenje. Ovaj test su osmisli britanski matematičar Arthur O. L. Atkin i francuski matematičar François Morain 1991. godine. On zapravo pripada vjerojatnosnim testovima prostosti, ali možemo ga uvrstiti u deterministične jer je odgovor koji da uvijek točan.

Sam test i teorija na kojoj se temelji su vrlo složeni pa ćemo u ovom radu navesti i definirati osnovne pojmove kao što su eliptičke krivulje te navesti neke općenite informacije o algoritmu, a za više informacija moguće je pogledati sam članak (vidi [2]) u kojem je objavljen algoritam i [10], stranice 222. do 225., na kojima se i temelji ovo potpoglavlje.

Da bismo definirali pojam eliptičke krivulje, najprije se prisjetimo pojma polja i definirajmo karakteristiku polja.

Definicija 1.1. *Neka je $\mathbb{F}$ neprazan skup na kojemu su definirane binarne operacije zbrajanja $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ i množenja $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$. Uređenu trojku $(\mathbb{F}, +, \cdot)$ nazivamo **polje** ako vrijedi*

[21] Vidi [1], Lemma 4.3.
[22] Vidi [1].
[23] Za GRH, vidi [10], str. 163, Conjecture 1.5.2.

(1) $(\mathbb{F}, +)$ *je komutativana Abelova grupa s neutralnim elementom* e*,*

(2) $(\mathbb{F}/\{e\}, \cdot)$ *je komutativna Abelova grupa i*

(3) množenje je distributivno obzirom na zbrajanje.

Za polje kažemo da je ***konačno*** *ako je skup* $\mathbb{F}$ *konačan skup.*

Definicija 1.2. *Neka je* $\mathbb{F}$ *polje s neutralnim elementima* 0 *za zbrajanje i* 1 *za množenje. Za najmanji prirodan broj* n *takav da je* $1+1+\cdots+1 = 1 \cdot n = 0$ *kažemo da je* ***karakteristika polja*** $\mathbb{F}$*. Ako ne postoji takav* n*, onda kažemo da je* $\mathbb{F}$ *polje* ***karakteristike nula****.*

Sada definirajmo eliptičke krivulje.

Definicija 1.3. *Neka je* K *polje karakteristike različite od 2 i 3 i neka je* $f(x) = x^3 + ax + b$ *polinom s koeficijentima iz polja* K *koji nema višestruke nultočke.* ***Eliptička krivulja*** E *nad poljem* K *je skup svih točaka* $(x, y) \in K \times K$ *koje zadovoljavaju jednadžbu*

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

zajedno s još jednim elementom, kojeg označavamo s O *i zovemo točka u beskonačnosti.*

Prvi pokušaj korištenja svojstava eliptičkih krivulja za testiranje prostosti vidljiv je u Goldwasser-Kilian (GK) algoritmu.[24] Kako je taj algoritam više teorijski i nepraktičan za korištenje, Atkin i Morain su osmislili ECPP algoritam.[25]

Oba ova algoritma uzimaju *vjerojatno prost* broj n i pokazuju da je on uistinu prost. Za dani vjerojatno prost broj n, očekivano vrijeme za provedbu ECPP algoritma je proporcionalno s $\mathcal{O}(\log^{6+\epsilon}(n))$, gdje je $\epsilon > 0$.[26]

[24] Vidi [10], Algorithm 2.2.4.
[25] Vidi [2], str. 38 ili [10], Algorithm 2.2.5.
[26] Vidi [10], Theorem 2.2.24.

2. Vjerojatnosni testovi prostosti

2.1. Fermatovi testovi pseudoprostosti

Prisjetimo se Malog Fermatovog teorema.

Teorem 2.1 (Mali Fermatov teorem; vidi [3], 4.1. Pseudoprosti brojevi)**.** *Ako je n prost broj, onda za svaki cijeli broj b sa svojstvom $(b, n) = 1$ vrijedi*

$$b^{n-1} \equiv 1 \pmod{n}. \tag{6}$$

U sljedećem primjeru ćemo pokazati da obrat Malog Fermatovog teorema općenito ne vrijedi.

Primjer 2.1. *Neka je $n = 341$ i neka je $b = 2$. Vrijedi $(2, 341) = 1$. Broj n je očito složen jer je $341 = 11 \cdot 31$. Pokažimo da n zadovoljava kongruenciju (6). Vrijedi*

$$2^{341-1} = 2^{340} = (2^{10})^{34}$$

i kako je

$$2^{10} = 1024 \equiv 1 \pmod{341},$$

imamo

$$2^{340} = (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{341}.$$

Dakle, $2^{341-1} \equiv 1 \pmod{341}$, ali 341 nije prost broj.

Iz ovoga je primjera vidljivo da postoje složeni brojevi koji zadovoljavaju kongruenciju (6). Takvi su brojevi opisani u sljedećoj definiciji.

Definicija 2.1. *Ako je n neparan složen broj, te b cijeli broj takav da je $(b, n) = 1$ i*

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

onda kažemo da je n ***pseudoprost broj u bazi*** *b.*

Primjer 2.2. *Broj 341 iz Primjera 2.1 je pseudoprost u bazi 2.*

Kao što smo mogli vidjeti kroz prethodnu definiciju i primjer, postoje složeni brojevi za koje možemo, koristeći neke alate, zaključiti da su prosti. U tu su nam svrhu potrebni testovi koji će testirati, ne prostost, nego složenost nekog broja. Jedna od takvih tvrdnji naziva se Fermatov test prostosti, a iskazan je u sljedećoj propoziciji.

Propozicija 2.1 (Fermatov test prostosti; vidi [7], Proposition 14.1.)**.** *Neka je $n > 1$ neparan cijeli broj i neka je b proizvoljan cijeli broj takav da je $1 < b < n$. Ako vrijedi*

$$b^{n-1} \not\equiv 1 \pmod{n},$$

onda je n složen broj.

Dokaz. Pretpostavimo da je dani n prost broj. Prema Malom Fermatovom teoremu za sve b sa svojstvom $1 < b < n$ mora vrijediti kongruencija (6). Pretpostavka ovog teorema je da kongruencija nije zadovoljena niti za jedan takav b. Dakle n nije prost broj, pa mora biti složen. □

Napomena 2.1. *Za b iz prethodne propozicije se obično uzima broj* 2.

Fermatov test prostosti koristi se kao baza algoritma koji će za dani broj n i m različitih baza $b_1, \ldots, b_m$ imati dva moguća izlaza: *složen* ili *vjerojatno prost*. Postupak algoritma je sljedeći. Iz skupa brojeva $\{2, \ldots, n-2\}$ m puta slučajno biramo bazu b. Za svaku slučajno odabranu bazu b, provedemo Fermatov test prostosti. Ako n prođe Fermatov test za neku bazu b, onda je on SLOŽEN. Ako broj n ne prođe Fermatov test niti za jednu od tih slučajno odabranih m baza b, onda za n možemo reći samo da je VJEROJATNO PROST broj. Ne možemo reći da je n zasigurno prost broj jer postoje složeni brojevi koji zadovoljavaju kongruenciju (6) za svaku bazu b. Takvi su brojevi opisani u sljedećoj definiciji.

Definicija 2.2. *Složen broj n za kojeg kongruencija*

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

vrijedi za svaki cijeli broj b takav da je $(b, n) = 1$ nazivamo ***Carmichaelov broj****.*

Sljedeći nam teorem daje karakterizaciju Carmichaleovih brojeva.

Teorem 2.2 (Korseltov kriterij; vidi [8], Teorem 2.4.8.)**.** *Prirodan broj n je Carmichaelov broj ako i samo ako je kvadratno slobodan te za svaki prost broj p, koji dijeli n, vrijedi da i $p-1$ dijeli $n-1$.*

Primjer 2.3. *Brojevi* 561 *i* 1729 *su Carmichaelovi brojevi. To se lako može provjeriti koristeći Korseltov kriterij.*

Za ispitivanje složenosti Carmichaelovih brojeva, potrebna nam je mala dorada na Fermatovom testu prostosti. Taj se novi, dorađeni test naziva Jaki Fermatov test i iskazan je u sljedećoj propoziciji.

Propozicija 2.2 (Jaki Fermatov test; vidi [7], Proposition 14.4.)**.** *Neka je $n > 1$ neparan cijeli broj i neka je b proizvoljan cijeli broj takav da je $1 < b < n$. Neka je $n - 1 = 2^k s$, gdje je s neparan cijeli broj, a k prirodan broj. Induktivno definiramo sljedeći niz*

$$\begin{aligned} b_0 &\equiv b^s \pmod{n}, \\ b_1 &\equiv b_0^2 \pmod{n}, \\ b_2 &\equiv b_1^2 \pmod{n}, \\ b_3 &\equiv b_2^2 \pmod{n}, \\ &\vdots \\ b_{k+1} &\equiv b_k^2 \pmod{n}. \end{aligned}$$

Ako je n prost broj, onda je $b_k \equiv 1 \pmod{n}$ i ako je j najmanji indeks za koji je $b_j \equiv 1 \pmod{n}$, onda je $j = 0$ ili $b_{j-1} \equiv -1 \pmod{n}$.

Ako je $b_k \not\equiv 1 \pmod{n}$ ili $b_{j-1} \not\equiv -1 \pmod{n}$, onda je n složen broj.

Dokaz. Neka je n prost broj. Tada, prema Malom Fermatovom teoremu vrijedi

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

Opći član definiranog niza možemo zapisati na sljedeći način:

$$b_k \equiv (b^s)^{2^k} \pmod{n}.$$

Kako je $2^k s = n - 1$ slijedi $b_k \equiv b^{n-1} \pmod{n}$ pa je zato

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

Neka je sada $j > 0$ najmanji indeks za koji je $b_j \equiv 1 \pmod{n}$. Tada je, prema definiciji niza, $b_{j-1}^2 \equiv 1 \pmod{n}$. Obzirom na to da je n prost broj, jedina rješenja jednadžbe

$$x^2 \equiv 1 \pmod{n}$$

su 1 i -1.[27] Dakle $b_{j-1} \equiv 1 \pmod{n}$ ili $b_{j-1} \equiv -1 \pmod{n}$. Kako je j najmanji indeks takav da je $b_j \equiv 1 \pmod{n}$, slijedi da je $b_{j-1} \equiv -1 \pmod{n}$. □

Napomena 2.2. *Navedimo nekoliko napomena vezanih uz Jaki Fermatov test.*

(1) Isto kao i u Feramatovom testu, za broj b se obično uzima broj 2.

(2) Ako n zadovoljava kongruencije $b_k \equiv 1 \pmod{n}$ i $b_{j-1} \equiv -1 \pmod{n}$, onda kažemo da je n prošao Jaki Fermatov test i u tom slučaju kažemo da je n vjerojatno prost broj.

(3) Ovaj test se može iskoristiti i za provjeru prostosti i za provjeru složenosti nekoga broja.

Korištenje ovoga testa ilustrirat ćemo sljedećim primjerima i to u oba slučaja, to jest kada ga koristimo da pokažemo da je neki broj vjerojatno prost (Primjer 2.4) i kada ga koristimo da pokažemo složenost broja (Primjer 2.5).

Primjer 2.4. *Neka je $n = 31$ i neka je $b = 2$. Tada je $n - 1 = 30 = 2^1 \cdot 15$. Dakle $k = 1$, a $s = 15$. Sada imamo sljedeći niz:*

$$b_0 \equiv 2^{15} \pmod{31},$$
$$b_1 \equiv b_0^2 \pmod{31}.$$

Vrijedi $2^5 \equiv 1 \pmod{31}$. Odatle slijedi $b_0 \equiv 1 \pmod{31}$ pa je i $b_1 \equiv 1 \pmod{31}$. Kako je $b_0 \equiv 1 \pmod{31}$, slijedi da je $j = 0$. Dakle, broj n je prošao Jaki Fermatov test pa možemo zaključiti da je on vjerojatno prost.

Primjer 2.5. *Neka je $n = 33$ i neka je $b = 2$. Tada je $n - 1 = 32 = 2^5 \cdot 1$ iz čega je $k = 5$, a $s = 1$. Sada je $b_0 \equiv 2^1 \pmod{33}$, to jest $b_0 = 2$. Nadalje je*

$$b_1 \equiv 4 \pmod{33},$$
$$b_2 \equiv 8 \pmod{33},$$
$$b_3 \equiv 64 \pmod{33} \equiv 21 \pmod{33},$$
$$b_4 \equiv 441 \pmod{33} \equiv 12 \pmod{33},$$
$$b_5 \equiv 144 \pmod{33} \equiv 12 \pmod{33}.$$

Dakle imamo slučaj kada je $b_k \not\equiv 1 \pmod{n}$ pa zaključujemo da je n složen, što i jest jer je $33 = 3 \cdot 11$.

Jaki Fermatov test je vrlo efikasan jer je vjerojatnost da neki složen broj prođe taj test vrlo mala, a za provedbu algoritma potrebno je $\mathcal{O}(\log^3(n))$ operacija.[28] Jedini nedostatak je što postoje složeni brojevi koji ga prolaze.

[27] vidi [7], Corollary 6.11.
[28] Vidi [10], str. 214, Remark 2.2.4.

Definicija 2.3. *Složen broj $n > 1$ nazivamo* ***jaki pseudoprost broj u bazi*** *b ako prođe Jaki Fermatov test za neku bazu b.*

Primjer 2.6. *Navedimo primjere jakih pseudoprostih brojeva.*

(1) Broj 4033 je jaki pseudoprost broj u bazi 2.

(2) Broj 121 je jaki pseudoprost broj u bazi 3.

Jakim pseudoprostim brojevima bavit ćemo se u sljedeća 2 potpoglavlja, a u posljednjem poptpoglavlju, bavit ćemo se pseudoprostim brojevima.

2.2. Pocklington–Lehmerov test prostosti

U prethodnom potpoglavlju, vidjeli smo da, ako neki broj n prođe Jaki Fermatov test, on je vjerojatno prost, ali postoji mogućnost i da je složen. Slično kao ECPP algoritam, Pocklington-Lehmerov test, kojeg su osmisli Henry C. Pocklington i Derrick H. Lehmer 1914. godine, nam služi da bi pokazali da je neki vjerojatno prost broj, točnije broj koji je prošao Jaki Fermatov test, uistinu prost.[29] On je iskazan u sljedećoj propoziciji.

Propozicija 2.3 (Pocklington–Lehmerov test; vidi [7], Proposition 14.6.)**.** *Neka je $n > 1$ neparan prirodan broj i neka je $n - 1 = FN$, gdje je F "faktorizran", a N "nije nužno faktoriziran". Pretpostavimo da postoji baza b takva da je*

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

i da je

$$(b^{\frac{n-1}{q}} - 1, n) = 1,$$

za sve proste brojeve q koji dijele F. Onda svaki prost faktor p od n zadovoljava

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

Štoviše, ako je $F > N$, onda je n prost.

Dakle, ako želimo iskoristiti ovaj test kako bismo pokazali da je neki dani vjerojatno prost broj n uistinu prost, najprije trebamo provjeriti vrijede li pretpostavke prethodne propozicije, a zatim samo provjeriti vrijedi li $F > N$. Ilustritat ćemo primjenu ovoga testa sljedećim primjerom.

Primjer 2.7. *Koristeći se Pocklington-Lehmerovim testom, pokažimo da je $n = 13$ prost broj.*

Najprije zapišimo $n - 1 = 12 = 4 \cdot 3$. Tada je $F = 4 = 2 \cdot 2$ i $N = 3$. Sada pronađimo bazu b za koju vrijedi da je $b^{n-1} \equiv 1 \pmod{n}$. Krenimo redom.
Za $b = 2$ imamo

$$2^{12} = (2^4)^3 \equiv 3^3 \equiv 1 \pmod{13}.$$

Dakle, $b = 2$. Kako je $F = 4$, jedini prosti broj koji ga dijeli je $q = 2$. Odredimo sada $(b^{\frac{n-1}{q}} - 1, n)$, za $b = 2$ i $q = 2$. Imamo

$$(2^{\frac{12}{2}} - 1, 13) = (2^6 - 1, 13) = (64, 13) = 1.$$

Dakle, uvjeti Propozicije 2.3 su ispunjeni i $4 = F > N = 3$. Zaključujemo da je 13 prost broj.

[29] Cijelo potpoglavlje je bazirano na [7].

2.3. Miller-Rabinov test prostosti

Kao što je najavljeno, nastavljamo se baviti jakim pseudoprostim brojevima.

Najprije pogledajmo kolika je vjerojatnost da je složen broj n za neku slučajno odabranu bazu b jaki pseudoprost broj u toj bazi. Odgovor nam daje sljedeća propozicija, koja će nam poslužiti kasnije u analizi efikasnosti Miler-Rabinovog testa.

Propozicija 2.4 (vidi [10], Corollary 2.2.2.)**.** *Neka je $n > 1$ neparan složen broj i neka je $1 < b < n$ proizvoljan cijeli broj. Vjerojatnost da n prođe Jaki Fermatov test za bazu b je manja od $\frac{1}{4}$.*

Miller-Rabinov test je, u deterističkoj verziji, koja se naziva Millerov test, osmislio Gary L. Miller 1976. godine i dokazao ga pretpostavljajući da je Generilizirana Riemannova Hipoteza točna. Ta deterministička verzija testa kaže sljedeće: ako je n složen broj, onda postoji baza b, $b < 2\ln^2(n)$ u kojoj n nije jaki pseudoprost broj u bazi b. Michael O. Rabin je 1980. godine doradio Millerovu deterističku tvrdnju i dobio vjerojatnosti test prostosti koji u dokazu ne koristi GRH. On je izrečen u sljedećem teoremu.

Teorem 2.3 (Miller-Rabinov test; vidi [9], Theorem 2.9.)**.** *Neka je dan neparan broj n za kojeg vrijedi $n = 2^k s + 1$, gdje je s također neparan, a k prirodan broj. Ako postoji b takav da je*

$$b^s \not\equiv 1 \pmod{n}$$

i

$$b^{2^r s} \not\equiv -1 \pmod{n},$$

za sve $0 < r < k - 1$, onda je n nije prost.

Dokaz. Dokaz provodimo po kontrapoziciji. Točnije, pretpostavimo da je n prost broj takav da je $n > 2$. Tada je n neparan pa je $n - 1$ paran. U tom slučaju postoje pozitivni cijeli brojevi s i k takvi da je je $n-1 = 2^k s$, pri čemu je s neparan broj. Neka je $b \in \mathbb{Z}_n$ proizvoljan. Pokažimo da je zadovoljena jedna od sljedeće dvije kongruencije:

1. $b^s \equiv 1 \pmod{n}$ ili
2. $b^{2^r s} \equiv -1 \pmod{n}$, za neki r, takav da je $0 < r < k - 1$.

Kako je n prost broj, prema Malom Fermatovom teoremu vrijedi $b^{n-1} \equiv 1 \pmod{n}$. Osim toga, opet jer je n prost, jednadžba $x^2 \equiv 1 \pmod{n}$ može imati samo dva rješenja, a to su 1 i -1. Prema tome slijedi $b^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ ili $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. Ako dobijemo -1, onda je zadovoljena 2. kongruencija. Ako dobijemo 1, pošto je n prost broj, opet slijedi da je $b^{\frac{n-1}{4}} \equiv 1 \pmod{n}$ ili $b^{\frac{n-1}{4}} \equiv -1 \pmod{n}$. Ponovno, ako dobijemo -1, zadovoljena je 2. kongruencija. U suprotnom nastavljamo dalje. Ako niti u jednom budućem koraku ne dobijemo -1, onda nam preostaje 1. mogućnost. Time je teorem dokazan. □

Koristeći ovaj teorem, prostost broja testiramo na sljedeći način.

Miller-Rabinov test: Neka je n neparan broj takav da je $n = 2^k s+1$, gdje je s neparan. Na slučajan način izaberemo b takav da je $0 < b < n$. Izračunamo $b^s \mod n$. Ako dobijemo 1 ili -1, zaključujemo da je n prost jer je zadovoljena kontrapozicija Teorema 2.3 te biramo sljedeći b. U protivnom, uzastopno kvadriramo $b^s \mod n$ sve dok ne dobijemo rezultat -1. Ako dobijemo -1, onda je n prost jer je opet zadovoljena kontrapozicija Teorema 2.3. Ako

nikad ne dobijemo -1, to jest ako dobijemo da je $b^{2^{r+1}s} \equiv 1 \pmod{n}$, ali $b^{2^r s} \not\equiv -1 \pmod{n}$, onda znamo da je n sigurno složen.[30]

Pogledajmo kolika je efikasnost ovoga testa, odnosno kolika je vjerojatnost da složen broj proglasi prostim. Pretpostavimo da smo neki broj n testirali Miller-Rabinovim testom m puta, to jest da smo ga testirali na m baza $b_1, \ldots, b_m$. Vjerojatnost da je n složen, a prođe Miller-Rabinov test, odnosno da je n jaki pseudoprost broj, je, prema Propoziciji 2.4, manja od $\frac{1}{4}$. Prema tome, vjerojatnost da složen broj prođe kao prost, odnosno da ga proglasimo vjerojatno prostim u svih m iteracija je manja od $\frac{1}{4^m}$. Odnosno, vjerojatnost da je testirani broj n uistinu prost je najmanje $1 - \frac{1}{4^m}$.[31]

Osim toga, ovaj algoritam je i vrlo brz jer je za provedbu ovog algoritma potrebno $\mathcal{O}(m \log^3(n))$ operacija.[32] Kao takav, efikasan i brz, često se koristi u kriptografiji pri izboru prostih brojeva.

Završimo ovo potpoglavlje s primjerima korištenja Miller-Rabinovog testa.

Primjer 2.8. *Neka je* $n = 2047$*. Tada je* $n - 1 = 2046$*, tj.* $n = 2^1 \cdot 1023 + 1$*. Slijedi* $k = 1$ *i* $s = 1023$*. Za* $b = 2$ *računamo* $2^{1023} \mod 2047$*. Kako je* $2^{11} \equiv 1 \pmod{2047}$*, imamo*

$$2^{1023} = 2^{11 \cdot 93} = (2^{11})^{93} \equiv 1^{93} \equiv 1 \pmod{2047}.$$

Kako je $2047 = 23 \cdot 89$*, očito je da je* 2047 *složen broj. No kako je*

$$2^{1023} \equiv 1 \pmod{2047},$$

to jest pošto broj 2047 *prolazi Miller-Rabinov test za* $b = 2$*, slijedi da je* 2047 *jaki pseudoprost broj u bazi* 2*.*

Primjer 2.9. *Neka je* $n = 11$*. Tada možemo pisati* $n = 2^1 \cdot 5 + 1$*. Dakle,* $k = 1$*, a* $s = 5$*. Za bazu* b *odaberimo broj* $b = 2$*. Računamo* $b^s \mod n$ *točnije, u ovom slučaju* $2^5 \mod 11$*. Kako je*

$$2^5 \equiv -1 \pmod{11},$$

zaključujemo da je n *prošao Miller-Rabinov test i proglašavamo ga vjerojatno prostim. Obzirom da smo koristili test na samo jednoj bazi* $b = 2$*, tj.* $m = 1$*, možemo reći da je* $n = 11$ *vjerojatno prost broj s vjerojatnošću većom od* $1 - \frac{1}{4}$*, to jest* 75%*.*

Primjetimo da n *prolazi Miller-Rabinov test i za* $b = 3$ *jer je*

$$3^5 \equiv 1 \pmod{11}.$$

Sada je n *vjerojatno prost s vjerojatnošću većom od* $1 - \frac{1}{4^2}$*, to jest* 93.75%*, jer je prošao Miller-Rabinov test za dvije baze.*

Nadalje, kako je i

$$4^5 \equiv 1 \pmod{11},$$

n *je prošao Miller-Rabinov test za* $m = 3$ *različitih baza pa je on vjerojatno prost s vjerojatnošću većom od* $1 - \frac{1}{4^3}$*, to jest* 98.44%*.*

Analogno se pokaže da n *prolazi Miller-Rabinov test za sve ostale moguće baze tj.* $5, 6, 7, 8, 9$ *i* 10*. Dakle, prolazi ga za ukupno* $m = 9$ *baza. Zaključujemo da je* n *vjerojatno prost s vjerojatnošću većom od* $1 - \frac{1}{4^9}$*, tj.* 99.9996%*.*

Prisjetimo se da smo koristeći deterministički test baziran na Wilsonovom teoremu i njegovom obratu, u Primjeru 1.2 pokazali da je $n = 11$ *prost broj.*

[30] Vidi [3], 4.3.Miller-Rabinov test.
[31] Vidi [7], str. 324.
[32] Vidi [9], str. 5.

2.4. Solovay-Strassenov test prostosti

I u ovom poglavlju nastavljamo se baviti pseudoprostim brojevima.

Američki matematičar Robert M. Solovay i njemački matematičar Volker Strassen izumili su, 1977. godine, test pseudoprostosti koji se bazira na Eulerovom kriteriju za Legendrov simbol. Zato se test ponekad u literaturi naziva i Eulerov test pseudoprostosti.[33] U čast izumiteljima, test se može i naći pod imenom Solovay-Strassenov test prostosti.

Najprije definirajmo potrebne pojmove i izrecimo potrebne tvrdnje.

Definicija 2.4. *Neka je a cijeli broj i neka je n prirodan broj. Neka je $(a,n)=1$. Ako kongruencija $x^2 \equiv a \pmod{n}$ ima rješenja, onda kažemo da je a **kvadratni ostatak modulo** n. U protivnom kažemo da je a **kvadratni neostatak modulo** n.*

Definicija 2.5. *Neka je a cijeli broj i neka je p neparan prost broj. Po definiciji, **Legendreov simbol**, u oznaci $\left(\frac{a}{p}\right)$, jednak je 1 ako je a kvadratni ostatak modulo a, -1 ako je a kvadratni neostatak modulo p, a 0 ako $p \mid a$.*

Definicija 2.6. *Neka je a cijeli broj i neka je P neparan prirodan broj takav da je $P = p_1 \cdot p_2 \cdots p_s$, gdje su p_i, $i = 1, \ldots, s$, ne nužno različiti neparni prosti brojevi. Tada se **Jacobijev simbol**, u oznaci $\left(\frac{a}{P}\right)$, definira kao*

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

gdje je $\left(\frac{a}{p_j}\right)$ Legendreov simbol.

Iskažimo sada Eulerov kriterij za Legendrov simbol.

Teorem 2.4 (Eulerov kriterij; vidi [8], Teorem 4.1.2.)**.** *Ako je a cijeli broj i p neparan prost broj, tada vrijedi*

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

Sljedeće nam dvije propozicije daju svojstva za računanje Legendrovog simbola koja su korisna za provedbu Solovay-Strassenovog testa.

Propozicija 2.5 (vidi [3], Propozicija 3.3)**.** *Neka je p neparan prost broj te neka su a i b cijeli brojevi. Tada vrijedi:*

(1) ako je $a \equiv b \pmod{n}$, onda je $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

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

(3) ako je $(a,p)=1$, onda je $\left(\frac{a^2}{p}\right) = 1$,

(4) $\left(\frac{1}{p}\right) = 1$ i

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

[33] Pod tim imenom je zabilježen u [10].

Propozicija 2.6 (vidi [7], Theorem 13.4.(c))**.** *Neka je p neparan prost broj. Tada vrijedi*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Slično Fermatovom pseudoprostom broju, imamo i Eulerov pseudoprost broj.

Definicija 2.7. *Ako je n neparan složen broj i b cijeli broj takav da je $(b, n) = 1$ te vrijedi*

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

gdje je $\left(\frac{b}{n}\right)$ Jacobijev simbol, onda kažemo da je n ***Eulerov pseudoprost broj u bazi*** *b.*

Primjer 2.10. *Pokažimo da je broj $n = 133$ Eulerov pseudoprost broj u bazi $b = 11$.*

Vrijedi $11 \equiv 1 \pmod{133}$.
Računamo

$$\left(\frac{11}{133}\right) = \left(\frac{11}{19}\right) \cdot \left(\frac{11}{7}\right) = 11^{\frac{19-1}{2}} \cdot 11^{\frac{7-1}{2}} = 11^9 \cdot 11^3 = 11^{12} \equiv 1 \pmod{133}.$$

S druge strane je

$$11^{\frac{133-1}{2}} = 11^{66} \equiv 1 \pmod{133}.$$

Dakle, dobili smo da vrijedi

$$\left(\frac{11}{133}\right) \equiv 11^{\frac{133-1}{2}} \pmod{133},$$

što znači da je 133 *Eulerov pseudoprost broj u bazi* 11*.*

Solovay-Stressenov test izrečen je u obliku sljedećeg teorema.

Teorem 2.5 (Solovay-Stressenov test; vidi [10], Theorem 2.2.14.)**.** *Neka je $n > 1$ cijeli broj. Slučajno izaberimo k cijelih brojeva $b_1, b_2, \ldots, b_k$ takvih da je $1 < b_i < n$ i takvih da je $(b_i, n) = 1$, $\forall i \in \{1, 2, \ldots, k\}$. Izračunajmo*

$$\left(\frac{b_i}{n}\right) \equiv b_i^{\frac{n-1}{2}} \pmod{n}, \tag{7}$$

za sve $i = 1, 2, \ldots, k$. Ako jedna od tih konguencija ne vrijedi, onda je n složen broj.

Primjedba 2.1. *Primjetimo da ako neki složen broj $n > 1$ prođe Solovay-Strassenov test za neku bazu b, onda je on Eulerov pseudoprost broj u bazi b.*

Napomena 2.3. *Broj $n > 1$ koji prođe Solovay-Strassenov test za neku bazu b zovemo* ***vjerojatni Eulerov prost broj u bazi*** *b. Što više baza uzmemo, vjerojatnost da je n uistinu prost je veća. Najčešće se uzima $k = 50$ ili $k = 100$.*[34]

[34]Vidi [3], 4.2.Solovay-Strassenov test.

Vjerojatnost da neki složen broj prođe Solovay-Strassenov test za svih k baza je najviše $\frac{1}{2^k}$. Vidimo da je ta vjerojatnost veća od vjerojatnosti u Miller-Rabinovom testu. Dakle, on je manje efikasan od Miller-Rabinovog testa. Isto tako, više složenih brojeva će proći Solovay-Strassenov test nego Jaki Fermatov test. Ova činjenica proizlazi iz činjenice da je svaki jaki pseudoprost broj u bazi b ujedno i Eulerov pseudoprost broj u bazi b. Obrat općenito ne vrijedi. Ova dva pojma su ekvivalentna uz uvjet da je $n \equiv 3 \pmod 4$.[35] S druge strane, brzina Solovay-Strassenovog testa jednaka je brzini Jakog Fermatovog testa i iznosi, podsjetimo se, $\mathcal{O}(\log^3(n))$ operacija.[36]

Za kraj, pogledajmo jedan primjer korištenja ovog testa.

Primjer 2.11. *Neka je* $n = 23$ *i neka su* $b_1 = 2$, $b_2 = 3$, $b_3 = 5$, $b_4 = 7$ *i* $b_5 = 11$ *dane baze. Dakle* $k = 5$. *Vrijedi* $(b_i, 23) = 1$, $\forall i \in \{1, \ldots, 5\}$, *jer su svi brojevi* b_i, $i = 1, \ldots, 5$, *prosti.*

Za baze $b_2, \ldots, b_5$ *vrijedi (7) prema Eulerovom kriteriju.*

Za bazu $b_1 = 2$, *prema Propoziciji 2.6, imamo*

$$\left(\frac{2}{23}\right) = (-1)^{\frac{23^2-1}{8}} = (-1)^{\frac{528}{8}} = (-1)^{\frac{528}{8}} = (-1)^{66} \equiv 1 \pmod{23}.$$

Vrijedi $2^4 \equiv 7 \pmod{23}$ *i* $2^3 \equiv 9 \pmod{23}$. *Sada imamo*

$$\begin{aligned} 2^{\frac{23-1}{2}} = 2^{11} = (2^4)^2 \cdot 2^3 \equiv 7^2 \cdot 8 \pmod{23} &\equiv 3 \cdot 8 \pmod{23} \\ &\equiv 24 \pmod{23} \equiv 1 \pmod{23}. \end{aligned}$$

Dakle, i za $b_1 = 2$ *vrijedi (7).*

Zaključujemo da je $n = 23$ *vjerojatno prost broj s vjerojatnošću većom od* $1 - \frac{1}{2^5} = 1 - \frac{1}{32} = \frac{31}{32} = 0.96875$ *tj.* 96.88%.

[35] Vidi [3], Teorem 4.3.

[36] Vidi [10], str. 214, Remark 2.2.4.

Literatura

[1] M. Agrawal, N. Kayal, N. Saxena, *Primes is in P*, Annals of Mathematics **160**(2004), 781–793

[2] A. O. L. Atkin, F. Morain, *Elliptic Curves and Primality Proving*, Mathematics of Computation **61**(1993), 29–68

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

[4] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilite u Zagrebu (skripta).

[5] Great Internet Mersenne Prime Search, *51st Known Mersenne Prime Found! (2018-Dec-21)*, `https://www.mersenne.org/` [pristupljeno 10.5.2022.]

[6] S. Kopparty, *Primality Testing*, Rutgers University, Lecture notes, 2014.

[7] J. Kraft, L. Washington, *An Introduction to Number Theory with Cryptography*, CRC Press, Boca Raton, 2018.

[8] I. Matić, *Uvod u teoriju brojeva*, Sveučilšte Josipa Jurja Strossmayera - Odjel za matematiku, Osijek, 2015.

[9] Z. Wang, *Methods of Primality Testing* (2021), preuzeto s `https://www.researchgate.net/publication/348899360_Methods_of_Primality_Testing` [pristupljeno 25.6.2022.]

[10] S. Y. Yan, *Number Theory for Computing*, Springer-Verlag, Berlin, 2002.