UNIVERZITET U NIŠU

ELEKTRONSKI FAKULTET

**ZAVRŠNI RAD**

**Implementacija i evaluacija algoritama za testiranje prostih brojeva**

**Nikola Stevanović**

Niš, februar 2018. god.

UNIVERZITET U NIŠU

ELEKTRONSKI FAKULTET

**ZAVRŠNI RAD**

**Implementacija i evaluacija algoritama za testiranje prostih brojeva**

**Zadatak:** Proučiti algoritme za testiranje prostih brojeva. Uočiti razliku izmedju determinističkih i nedeterminističkih algoritama. Implementirati sledeće algoritme za testiranje prostih brojeva:

* Deterministički
  + Naive approach
  + Elliptic curve primality proving – Atkin’s ECPP
* Nedeterministički
  + Miller-Rabin
  + Solovay-Strassen

Izvršiti evaluaciju rada algoritama na 32-bitnim i 64-bitnim brojevima.

#### Mentor: Kandidat:

Prof. dr Vladimir Ćirić Nikola Stevanović

broj indeksa: 14525

Komisija za ocenu i odbranu završnog rada:

1. Datum prijave završnog rada:
2. Datum predaje završnog rada:
3. Datum odbrane završnog rada:

**Sadržaj**

[1. Uvod 4](#_Toc505812594)

[2. Prosti brojevi 6](#_Toc505812595)

[**2.1.** Prosti brojevi i osnovni stav aritmetike 6](#_Toc505812596)

[**2.2.** Značaj prostih brojeva za asimetričnu kriptografiju 7](#_Toc505812597)

# **Uvod**

“Matematičari su do današnjih dana uzaludno pokušavali da otkriju neki red u nizu prostih brojeva i imamo razloga da verujemo da je to tajna u koju um nikada neće prodreti” – Ojler, (Havil 2003, str. 163).

Prosti brojevi su fascinirali ljude veoma dugo. Iako se čini da je pojam prostog broja prilično jednostavan i lako razumljiv, prosti brojevi su zadavali mnogo muke matematičarima u prošlosti.

Prost broj je pozitivan ceo broj p > 1 koji nema pozitivne cele delitelje osim 1 i samog broja p. Pozitivni celi brojevi, osim broja 1[[1]](#footnote-1), koji nisu prosti se zovu složenim brojevima. Možemo da uocimo da je 2 jedini paran prost broj.

Drevni Egipćani su počeli da se pitaju kako da pronađu proste brojeve. Jedan od najintuitivnijih načina za pronalaženje prostih brojeva je isključivanje svih brojeva koji ne mogu biti prosti. Ovaj metod je poznat kao Eratostenovo sito, koji je dobio ime po starogrčkom matematičaru Eratostenu. On jednostavno isključuje sve brojeve koji su deljivi sa unapred poznatim prostim brojevima ( 2,3,5,7... √p), gde je p granica do koje želimo testiramo brojeve. Ovaj metod sa sigurnošću daje rezultat da li je broj prost ili ne, ali je takođe potrebno puno vremena za izračunavanje kada je p veliki broj.

Mnogo godina kasnije, napravljena su važna otkrića o identitetima prostih brojeva. Jedno od otkrića poznato je i kao mala Fermaova teorema: , gde je a pozitivan ceo broj i p prost broj. Ovaj test ne može sa sigurnošću reći da li je broj prost ili ne. Pored ovog testa postoje još nekoliko testova koji se oslanjaju na ovaj identitet.

U 20-om veku su se pojavilo nekoliko atraktivnih rešenja. 30-ih godina prošlog veka D.H.Lehmer je poboljšao test koji je E.Lucas osmislio 1878. Tako je nastao Lucas-Lehmer test. Iako je ovaj test deterministički, on funkcioniše za malu grupu brojeva tzv. Mersenovi brojevi Mp = , gde je p poznat prost broj.

50-ak godina kasnije pojavio se algoritam zasnovan na eliptičnim krivama. Iako u početku test nije bio deterministički, bio je veoma često korišćen za potvrdu da li je broj prost ili ne. Kasnije je poboljšan, tako da može da potvrdi da li je broj prost. Međutim to je znatno usporilo algoritam i zbog toga je postao manje atraktivan za praktičnu primenu.

Međutim u 21. veku došlo je do velikog pomaka. 2002 je objavljen document “Primes is in P” u kojem je predstavljen novi algoritam za testiranje prostih brojeva. Algoritam je nazvan po njegovim stvaraocima: Agrawal, Kayal and Saxena. Za razliku od testova pomenutih ranije u tekstu, ovaj algoritam nam sa sigurnošću moze reći da li je broj p prost.

Danas algoritmi za testiranje prostih brojeva imaju široku primenu u računarstvu, tačnije u kriptografiji. RSA sistem je jedan od podsticaja zbog čega je brzo i efikasno pronalaženje prostih brojeva bitno u kriptografiji. RSA bira dva različita velika prosta broja (preko 100 decimalnih cifara) p i q i izračunava njihov prizvod n = pq. Brojevi p i q se čuvaju u tajnosti, dok je n deo javnog ključa.

Cilj ovog rada je proučavanje algoritama za testiranje prostih brojeva i njihova implementacija. U radu će najpre biti opisani prosti brojevi, nakon toga ce biti reči o podeli algoritama za testiranje prostih brojeva na dve grupe:

* Nedeterminističke
* Determinističke

Zatim će biti opisana po dva predstavnika obe grupe algoritama i biće data njihova implementacija. Na kraju ćemo izvršiti evaluaciju i poređenje algoritama što je značajno za odabir algoritma koji će kasnije biti integrisan sa kriptografskim sistemima.

Nakon uvoda, u drugom poglavlju, biće objašnjen pojam prostog broja i biće date njihove karakteristike, kao i njihov značaj u kriptografiji.

U trećem poglavlju biće reči o algoritmima za testiranje prostih brojeva i biće data njihova podela u dve grupe kao i opis sveke od grupa.

U sledećem poglavlju, četvrtom, biće detaljno opisana po dva algoritma iz obe grupe. Za nedeterminističke to će biti Miller-Rabin i Solovay-Strassen, a za determinističke Naivni algoritam tj. algoritam koji prati definiciju prostih brojeva i Atkinov algoritam zasnovan na eliptičnim krivama. U ovom poglavlju prikazaćemo i implementaciju svakog algoritma u jeziku C#.

U petom, pretposlednjem poglavlju, biće data evaluacija svakog algoritama i njihovo poređenje.

Zaključak će biti dat u poslednjem, šestom poglavlju.

# Prosti brojevi

## Prosti brojevi i osnovni stav aritmetike

Definiciju prostog broja uveo je grčki matematičar Euklid, koji je živeo na prelazu iz 4. u 3. vek pre nove ere. Posmatrajmo broj a ∈ N, a > 1. Svaki prirodni broj a uvek ima dva delitelja: 1 i samog sebe. Te delioce zovemo trivijalnim deljiteljima.

DEFINICIJA: Za svaki prirodni broj p > 1 kažemo da je prost broj ukoliko ima samo trivijalne delitelje.

Delitelje broja a ∈ N zovemo još I faktorima broja a. Faktorizaciju prirodnog broja a prikazujemo u obliku a = bc, gde su b,c ∈ N. Ako je delitelj b prost broj, zovemo ga jos i prostim faktorom broja a. U svrhu dokazivanja osnovne teoreme aritmetike razmotrićemo nekoliko teorema koje ćemo iskoristiti kasnije.

Teorema 1. Neka je a prirodan broj, a > 1 ili je prost ili je proizvod prostih brojeva.

Teorema 2. Ako prost broj p nije deljiv sa a onda je (a,p) = 1.

Teorema 3. Ako p deli ab, onda p deli a ili p deli b. Opštije ako p deli a1a2a3...aN, tada p deli barem jedan od brojeva a1,a2,a3,...,aN.

DEFINICIJA: (Osnovni stav aritmetike) Svaki prirodan broj a > 1 može se predstaviti kao proizvod prostih brojeva na jedinstven način.

Ova teorema je ključni stav u tzv. Multiplikativne teorije brojeva. U faktorizaciji broja a neki prost broj se može pojaviti kao faktor više puta, recimo 24 = 2 x 2 x 2 x 3. Ako su p1,...,pK svi različiti prosti faktori broja a, onda se a može predstaviti kao

a =

gde su α1, α2,..., αk jednoznačno određeni prirodni brojevi. Ovo se naziva kanonska reprezentacija prirodnog broja a, i veoma se često koristi u teoriji brojeva.

Odgovor na pitanje koliko ima prostih brojeva znali su još starogrčki matematičari. Euklid u IX knjizi svojih „Elemenata“ daje sledeći dokaz činjenice da je skup prostih brojeva beskonačan.

Euklidova teorema: Ne postoji naveći prost broj.

## Značaj prostih brojeva za asimetričnu kriptografiju

RSA algoritam je jedan od najpoznatijih I najkorišćenijih asimetričnih šifraskih sistema. Sistem je dobio ime po trojici svojih pronalazača Rivest-Shamir-Adleman.

U literaturi koja se odnosi na RSA algoritme, često se predlaže da se u izboru para ključeva koriste jaki prosti brojevi p I q za generisanje n. Jaki prosti brojevi imaju određene osobine koje čine proizvod n teško faktorizovanim. Razlog za ovakav izbor je to što sun eke od metoda faktorizacije, kao što su Polardove P - 1 i P + 1 metode, naročito pogodne za proste brojeve p za koje je P – 1 ili P + 1 imaju samo male proste faktore. Jaki prosti brojevi su otporni na ovakve napade. Napredak u faktorizaciji tokom poslednjih deset godina pokazuje opravdanost upotrebe jakih prostih brojeva. Za generisanje ključeva u RSA algoritmu preporučuje se upotreba velikih prostih brojeva veličine 100 decimalnih cifara I više.

Generisanje ključa za RSA se odvija na način što se odaberu dva velika broja p i q, a zatim računamo n = p\*q. Nakon toga odaberemo e i d uz poštovanje nekih uslova. Postoji dobar razlog zašto n ima tačno dva prosta faktora. Prvi razlog je jednostavnost formule za izračunavanje ϕ(n) = (p-1)(q-1), a drugi je teža faktorizacija n, jer je poznato da je faktorizaciju teže izvršiti ukoliko broj ima manje prostih faktora. Da bi smo stekli jasniju sliku o trenutno najvećim prostim brojevima u Tabeli 1. prikazaćemo podatke sa Web stranice [\*].

|  |  |  |  |
| --- | --- | --- | --- |
|  | Prost broj | Broj cifara | Godina pronalaska |
| Najveći prost broj | 277232917-1 | 23249425 | 2018 |
| Najveći prost broj “blizanac” | 2996863034895·21290000+1 | 388342 | 2016 |
| Najveći Marsenov prost broj | 277232917-1 | 23249425 | 2018 |
| Najveći Sophie Germain prost broj | 2618163402417·21290000+1 | 388342 | 2016 |

Tabela 1. Najveći poznati prosti brojevi

Kod RSA algoritma za komercijalnu upotrebu se obično koriste brojevi n od 1024 bita, odnosno n ≈ 10308. Za važne potrebe obično se koristi 2048-bitno n, odnosno n ≈ 10617.

1. Broj 1 je poseban slučaj za koji se uzima da nije ni prost, ni složen. Razlog zbog koga se 1 ne uzima kao prost broj je zati što onda ne bi važila jedinstvena faktorizacija broja u *Osnovnoj teoremi aritmetike.* [↑](#footnote-ref-1)