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](#_Toc505708976)

# **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.

Cilj ovog rada je proučavanje algoritama za testiranje prostih brojeva i

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)