Vaja 1

Praštevila

V tej nalogi sem implementiral aplikacijo za generiranje praštevil z uporabo dveh metod: naivne metode in Miller-Rabinovega testa. Aplikacija omogoča uporabniku, da vnese število bitov (n) za generiranje n-bitnega praštevila (do 32 bitov). Uporabnik lahko tudi določi parameter S za Miller-Rabinov test, ki vpliva na število krogov preverjanja.

Poleg tega lahko aplikacija preveri, ali je dano število praštevilo, in sicer z obema metodama – naivno in Miller-Rabinovo. Glavni cilj je primerjati časovno zahtevnost obeh metod, zato sem izmeril čas trajanja generiranja n-bitnih praštevil z obema metodama v območju od 4 do 32 bitov. Prav tako sem izmeril čas generiranja 32-bitnih praštevil z Miller-Rabinovim testom glede na parameter S (v območju od 1 do 20).

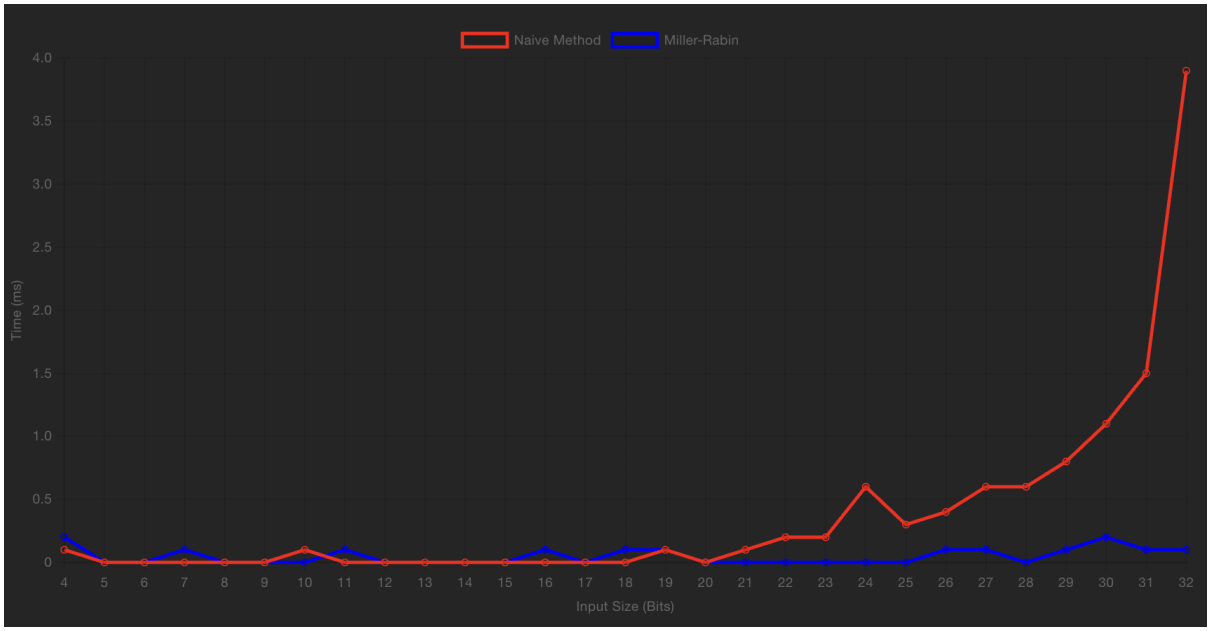
V naslednjih grafih so prikazane meritve časovne zahtevnosti za obe metodi ter vpliv parametra S na Miller-Rabinov test.

(Naivna metoda in Miller-Rabinov test)

Ta graf prikazuje primerjavo časovne zahtevnosti dveh metod generiranja praštevil: naivne metode in Miller-Rabinovega testa. Na **x-osi** je število bitov vhodnih podatkov (od 4 do 32), medtem ko **y-os** prikazuje čas v milisekundah (ms), potreben za generiranje praštevil.

- **Rdeča črta** predstavlja časovno zahtevnost naivne metode, kjer se za vsako število preverja deljivost do kvadratnega korena. Vidimo, da časovna zahtevnost eksponentno narašča z večanjem števila bitov.
- **Modra črta** predstavlja časovno zahtevnost Miller-Rabinovega testa. Pri tej metodi je časovna zahtevnost veliko nižja, saj gre za verjetnosten algoritem, ki ne preverja vsake delitve posebej, temveč na podlagi večkratnih krogov preverja, ali je število verjetno praštevilo.

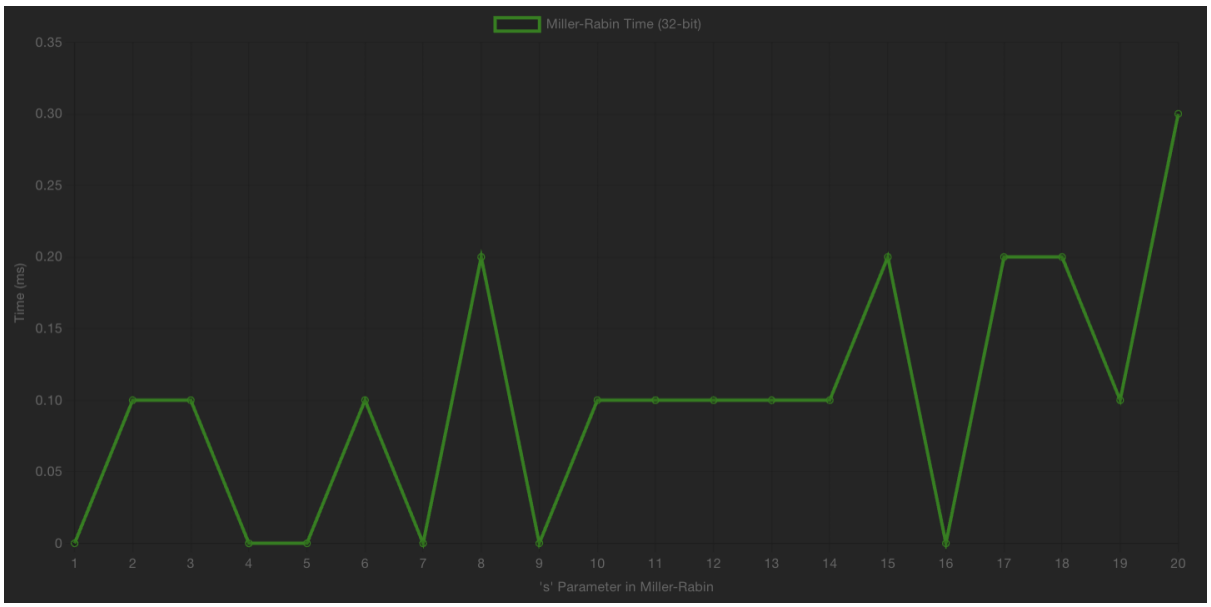
Graf jasno prikazuje, da je Miller-Rabinov test bistveno hitrejši pri večjih bitnih vrednostih, kar kaže na njegovo prednost pred naivno metodo.



Graf 2: Časovna zahtevnost generiranja 32-bitnega praštevila z Miller-Rabinovim testom glede na parameter S

Ta graf prikazuje časovno zahtevnost Miller-Rabinovega testa za generiranje 32-bitnega praštevila glede na parameter S, ki določa število krogov preverjanja. **X-os** predstavlja vrednost parametra S od 1 do 20, medtem ko y**-os** prikazuje čas v milisekundah (ms), potreben za izvedbo testa.

Z večanjem vrednosti S opazimo postopno naraščanje časovne zahtevnosti. To je pričakovano, saj večje število krogov preverjanja povečuje natančnost testa, vendar zahteva več časa za izvedbo. Kljub temu je Miller-Rabinov test tudi pri višjih vrednostih S še vedno relativno učinkovit v primerjavi z naivno metodo.



Graf 3: Časovna zahtevnost generiranja 32-bitnega praštevila z Miller-Rabinovim testom glede na parameter S (od 1 do 200)

V tem grafu sem razširil vrednosti parametra S od 1 do 300, da bi jasneje prikazal časovno zahtevnost Miller-Rabinovega testa pri večjem številu krogov preverjanja. **X-os** prikazuje vrednost S (število krogov), medtem ko **y-os** prikazuje čas v milisekundah (ms).

Pri tej razširjeni lestvici opazimo bolj enakomerno in linearen trend naraščanja časovne zahtevnosti, kar potrjuje, da se časovno breme testa povečuje pretežno linearno s povečevanjem števila krogov S. Ta test je bil izveden, da bi izločili morebitna odstopanja iz prejšnjega grafa, kjer so bili prisotni nenadni skoki v časovnih meritvah.