A09 - CAL

Vinicius Gasparini e Lucas Meneghelli

14 de outubro de 2019

1 Miller-Rabin

Segue execução do algoritmo

```
Primos identificados corretamente 20
Nao-primos identificados corretamente 20
Erros 0
Base usada: 37

Primos identificados corretamente 20
Nao-primos identificados corretamente 20
Erros 0
Base usada: 71

Primos identificados corretamente 20
Nao-primos identificados corretamente 20
Erros 0
Base usada: 94
```

Foi utilizado o seguintes primos como controle

10 151 10 091 10 007 10 061 10 093 10 103 10 141 10 159 10 169 10 067
10 099 10 037 10 069 10 039 10 133 10 009 10 163 10 139 10 111 10 079

A vantagem deste método frente ao Crivo de Eratóstenes está na sua complexidade $O(k \log^3 n)$, sendo k a quantidade de bases usadas.

Sua desvantagem esta no fato de ser um algoritmo não determinístico, então pseudo-primos podem acusar falso verdadeiro. Quando maior a certeza demandada, maior a quantidade de bases utilizadas e portanto maior a complexidade final.