

Вероятностные алгоритмы проверки чисел на простоту

Фань Яньцзе

30 октября, 2025, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритов Ферма, Соловэя-Штассена,
Миллера-Рабина.

Выполнение лабораторной работы

Наибольший общий делитель

Для построения многих систем защиты информации требуются простые числа большой разрядности. В связи с этим актуальной является задача тестирования на простоту натуральных чисел.

Тест Ферма

- Вход. Нечетное целое число $n \geq 5$.
 - Выход. «Число n , вероятно, простое» или «Число n составное».
1. Выбрать случайное целое число a , $2 \leq a \leq n - 2$.
 2. Вычислить $r = a^{n-1} \pmod{n}$
 3. При $r = 1$ результат: «Число n , вероятно, простое». В противном случае результат: «Число n составное»..

Тест Соловэя-Штрассена

- Вход. Нечетное целое число $n \geq 5$.
 - Выход. «Число n , вероятно, простое» или «Число n составное».
1. Выбрать случайное целое число a , $2 \leq a \leq n - 2$.
 2. Вычислить $r = a^{(\frac{n-1}{2})} (mod n)$
 3. При $r \neq 1$ и $r \neq n - 1$ результат: «Число n составное».
 4. Вычислить символ Якоби $s = (\frac{a}{n})$
 5. При $r = s (mod n)$ результат: «Число n , вероятно, простое». В противном случае результат: «Число n составное».

Тест Миллера-Рабина.

1. Представить $n - 1$ в виде $n - 1 = 2^s r$, где r - нечетное число
2. Выбрать случайное целое число a , $2 \leq a \leq n - 2$.
3. Вычислить $y = a^r \pmod{n}$
4. При $y \neq 1$ и $y \neq n - 1$ выполнить действия
 - Положить $j = 1$
 - Если $j \leq s - 1$ и $y \neq n - 1$ то
 - Положить $y = y^2 \pmod{n}$
 - При $y = 1$ результат: «Число n составное».
 - Положить $j = j + 1$
 - При $y \neq n - 1$ результат: «Число n составное».
5. Результат: «Число n , вероятно, простое».

Пример работы алгоритма

```
In [8]: 1 n = 35023
In [9]: 1 Fermat(n, 500)
Simple
Out[9]: True
In [10]: 1 SoloveiStrassen(n, 500)
Out[10]: True
In [11]: 1 MillerRabin(n)
Complex
Complex
Complex
Complex
Complex
Complex
Complex
Complex
Complex
Simple
Out[11]: True
In [12]: 1 n = 35024
In [13]: 1 Fermat(n, 500)
Complex
Out[13]: False
In [14]: 1 SoloveiStrassen(n, 500)
Complex
Out[14]: False
In [15]: 1 MillerRabin(n)
Simple
Complex
Out[15]: False
```

Выводы

Результаты выполнения лабораторной работы

Изучили алгоритмы Ферма, Соловэя-Штассена,
Миллера-Рабина.