

# Лабораторная работа №5

Вероятностные алгоритмы проверки чисел на простоту

---

Баулин Егор Александрович, НФИМд-02-22

12 ноября 2022

Российский университет дружбы народов, Москва, Россия

# Цели и задачи

---

# Цель лабораторной работы

Изучение алгоритмов Ферма, Соловья-Штрассена, Миллера-Рабина.

# **Выполнение лабораторной работы**

---

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

- 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 Соловья-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  $r = a^{(\frac{n-1}{2})} \pmod n$
  3. При  $r \neq 1$  и  $r \neq n - 1$  результат: «Число  $n$  составное».
  4. Вычислить символ Якоби  $s = \left(\frac{a}{n}\right)$
  5. При  $r = s \pmod n$  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

Тест Ферма

Введите число для теста Ферма: 5

Число  $n$ , вероятно, простое

Тест Миллера-Рабина

Введите число для теста Миллера-Рабина: 5

Число  $n$ , вероятно, простое

Тест Соловья-Штрассена

Введите число для теста Соловья-Штрассена: 5

Число  $n$ , вероятно, простое

**Figure 1:** Пример работы алгоритмов для  $n$  - простого

## Пример работы алгоритма

Тест Ферма

Введите число для теста Ферма: 8

Число  $n$  составное

Тест Миллера-Рабина

Введите число для теста Миллера-Рабина: 8

Число  $n$  составное

Тест Соловья-Штрассена

Введите число для теста Соловья-Штрассена: 8

Число  $n$  составное

**Figure 2:** Пример работы алгоритмов для  $n$  - составного

## **Выводы**

---

## Результаты выполнения лабораторной работы

В ходе выполнения работы мне удалось изучить алгоритмы Ферма, Соловья-Штрассена, Миллера-Рабина, а также реализовать данные алгоритмы программно на языке Python.