Отчёт по лабораторной работе №5. Вероятностные алгоритмы проверки чисел на простоту

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Майорова О.А., 1032212322
Группа: НФИмд-02-21
Преподаватель: д.ф.-м.н., Кулябов Д. С.

Москва, 2021

Цель и задачи

Цель: Ознакомиться с некоторыми вероятностными алгоритмами проверки чисел на простоту.

Задача: Программно реализовать следующие вероятностные алгоритмы проверки чисел на простоту: тест Ферма, тест Соловэя-Штрассена, тест Миллера-Рабина. А также алгоритм вычисления символа Якоби.

Теоретическое введение

Тесты на простоту: детерминированные и вероятностные.

- *Детерминированные тесты* - однозначно определяют простое число, или нет; требуют больших вычислительных мощностей.
- *Вероятностные тесты* - делают более слабое утверждение; определяют, число вероятно простое, или составное.

тест Ферма

Для простого числа n и $a : 1 \leq a \leq n-1$ выполняется равенство:

$a^{n-1} \equiv 1(\mod n)$.

Проверка функции теста Ферма:

```
1 Fermat(47)
```

```
'Число n, вероятно, простое'
```

```
1 Fermat(69)
```

```
'Число n составное'
```

алгоритм вычисления символа Якоби

Символ Якоби $\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right) \dots \left(\frac{m}{p_r}\right)$, где $m, n \in Z, n = p_1 \dots p_r, p_i \neq 2$ - простые (не обязательно различные)

Проверка функции вычисления символа Якоби:

```
1 Jacobi(1, 3)
```

```
1
```

```
1 Jacobi(2, 3)
```

```
-1
```

```
1 Jacobi(3, 3)
```

```
0
```

тест Соловэя-Штрассена

Для простого числа n и $a : 1 \leq a \leq n-1$ выполняется равенство:

$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \left(\mod n\right).$

Проверка функции теста Соловэя-Штрассена:

```
1 SolStr(47)
```

```
'Число n, вероятно, простое'
```

```
1 SolStr(69)
```

```
'Число n составное'
```

тест Миллера-Рабина

Для простого числа n, причём $n-1=2^s t$, где s – целое, t – нечётное, и $a: 1 \leq a \leq n-1$ выполняется хотя бы одно из условий:

- $a^t \equiv 1(\mod n)$
- $a^{2^k t} \equiv n-1(\mod n), k: 0 \leq k < s$

Проверка функции теста Миллера-Рабина:

```
1 MillRab(47)
```

```
'Число n, вероятно, простое'
```

```
1 MillRab(69)
```

```
'Число n составное'
```

Заключение

Таким образом, была достигнута цель, поставленная в начале лабораторной работы.

- Было осуществлено знакомство с некоторыми вероятностными алгоритмами проверки чисел на простоту: тест Ферма, тест Соловэя-Штрассена и тест Миллера-Рабина.
- Также была получена реализация на языке Python рассмотренных алгоритмов, а также алгоритма вычисления символа Якоби.

Спасибо за внимание