Отчёт по лабораторной работе №5

Вероятностные алгоритмы проверки чисел на простоту

Студент: Гонсалес Ананина Луис Антонио, 1032175329

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

# 1 Цель работы

Цель данной лабораторной работы- изучить теорию и реализовать все рассмотренные алгоритмы программно.

# 2 Теоретические сведения

Вопрос определения того, является ли натуральное число *N* простым, известен как проблема простоты.

Тестом простоты (или проверкой простоты) называется алгоритм, который, приняв на входе число *N*, позволяет либо не подтвердить предположение о составности числа, либо точно утверждать его простоту. Во втором случае он называется истинным тестом простоты. Таким образом, тест простоты представляет собой только гипотезу о том, что если алгоритм не подтвердил предположение о составности числа *N*, то это число может являться простым с определённой вероятностью. Это определение подразумевает меньшую уверенность в соответствии результата проверки истинному положению вещей, нежели истинное испытание на простоту, которое даёт математически подтверждённый результат[1].

**Тест простоты Ферма в теории чисел** — это тест простоты натурального числа n, основанный на малой теореме Ферма.

Если n — простое число, то оно удовлетворяет сравнению a^n-1 =1 (mod n) для любого a, которое не делится на n.

Выполнение сравнения a^n-1 =1 (mod n) является необходимым, но не достаточным признаком простоты числа. То есть, если найдётся хотя бы одно a, для которого a^n-1 !=1 (mod n), то число n — составное; в противном случае ничего сказать нельзя, хотя шансы на то, что число является простым, увеличиваются. Если для составного числа n выполняется сравнение a^n-1 =1 (mod n), то число n называют псевдопростым по основанию a . При проверке числа на простоту тестом Ферма выбирают несколько чисел a. Чем больше количество a, для которых a^n-1 =1 (mod n), тем больше шансы, что число n простое[2].

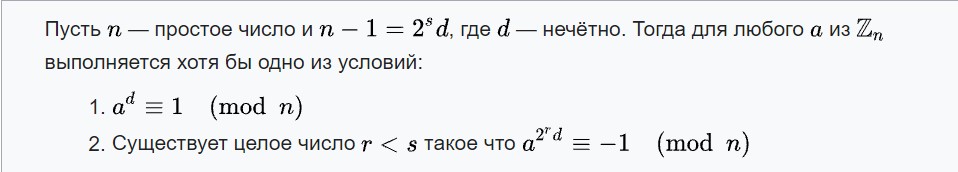
**Тест Соловея — Штрассена** — тест всегда корректно определяет, что простое число является простым, но для составных чисел с некоторой вероятностью он может дать неверный ответ.

Алгоритм Соловея — Штрассена параметризуется количеством раундов k. В каждом раунде случайным образом выбирается число a < n. Если НОД(a,n) > 1, то выносится решение, что n составное. Иначе проверяется справедливость сравнения a^(n-1)/2=(a/n)(mod n). Если оно не выполняется, то выносится решение, что n — составное. Если это сравнение выполняется, то a является свидетелем простоты числа n. Далее выбирается другое случайное a и процедура повторяется. После нахождения k свидетелей простоты в k раундах выносится заключение, что n является простым числом с вероятностью 1-2^-k[3].

**Тест Миллера — Рабина** — вероятностный полиномиальный тест простоты. Тест Миллера — Рабина, наряду с тестом Ферма и тестом Соловея — Штрассена, позволяет эффективно определить, является ли данное число составным. Однако, с его помощью нельзя строго доказать простоту числа. Тем не менее тест Миллера — Рабина часто используется в криптографии для получения больших случайных простых чисел.

Как и тесты Ферма и Соловея — Штрассена, тест Миллера — Рабина опирается на проверку ряда равенств, которые выполняются для простых чисел. Если хотя бы одно такое равенство не выполняется, это доказывает что число составное[4].

Для теста Миллера — Рабина используется следующее утверждение:



Тест Миллера

# 3 Выполнение работы



Тест Ферма



Тест Соловэя



Тест Миллера

# 4 Выводы

В итоге в данной лабораторной работы я изучил теорию и реализовал все рассмотренные алгоритмы программно.

# Список литературы

1. Тест Простоты [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Тест_простоты>.

2. Тест Ферма [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Тест_Ферма>.

3. Тест Соловея [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Тест_Соловея_—_Штрассена>.

4. Тест Миллера [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/Тест_Миллера_—_Рабина>.