Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Николаев Дмитрий Иванович, НПМмд-02-24

Содержание

# 1 Цель работы

Изучить работу алгоритмов разложения чисел на множители: -Метод Полларда; Метод квадратов (Теорема Ферма о разложении); а также реализовать их программно.

# 2 Теоретическое введение

## 2.1 Разложение чисел на множители

Задача разложения на множители — одна из первых задач, использованных для построения криптосистем с открытым ключом.

Задача разложения составного числа на множители формулируется следующим образом: для данного положительного целого числа найти его каноническое разложение , где — попарно различные числа .

На практике не обязательно находить каноническое разложение числа . Достаточно найти его разложение на два нетривиальных сомножителя: , . Далее будем понимать задачу разложения именно в этом смысле.

## 2.2 -Метод Полларда

Пусть — нечетное составное число, и — случайное отображение, обладающее сжимающими свойствами, например . Основная идея метода состоит в следующем. Выбираем случайный элемент и строим последовательность , определяемую рекуррентным соотношением:

где , до тех пор, пока не найдем такие числа , что и . Поскольку множество конечно, такие индексы существуют (последовательность “зацикливается”). Последовательность будет состоять из “хвоста” длины и цикла той же длины.

### 2.2.1 Алгоритм, реализующий -Метод Полларда

**Вход:** Число , начальное значение , функция , обладающая сжимающими свойствами.

**Выход:** Нетривиальный делитель числа .

1. Положить , .
2. Вычислить , .
3. Найти .
4. Если , то положить и результат: . При — “Делитель не найден”; при вернуться на шаг 2.

### 2.2.2 Пример

Найти -методом Полларда нетривиальный делитель . Положим и . Работа иллюстрируется следующей последовательностью:

1. Рассмотрим первый цикл алгоритма
   1. , ;
   2. , ;
   3. ;
   4. , значит возвращаемся на второй шаг.
2. Рассмотрим второй цикл алгоритма
   1. , ;
   2. ;
3. Рассмотрим третий цикл алгоритма
   1. , ;
   2. ;
4. Рассмотрим четвёртый цикл алгоритма
   1. , ;
   2. ;
5. Рассмотрим пятый цикл алгоритма
   1. , ;
   2. ;
6. Рассмотрим шестой цикл алгоритма
   1. , ;
   2. ;
7. Рассмотрим седьмой цикл алгоритма
   1. , ;

Таким образом, является нетривиальным делителем числа .

## 2.3 Метод квадратов (Теорема Ферма о разложении)

Для любого положительного нечетного числа существует взаимно однозначное соответствие между множеством делителей числа , не меньших, чем , и множеством пар таких неотрицательных целых чисел, что .

### 2.3.1 Пример

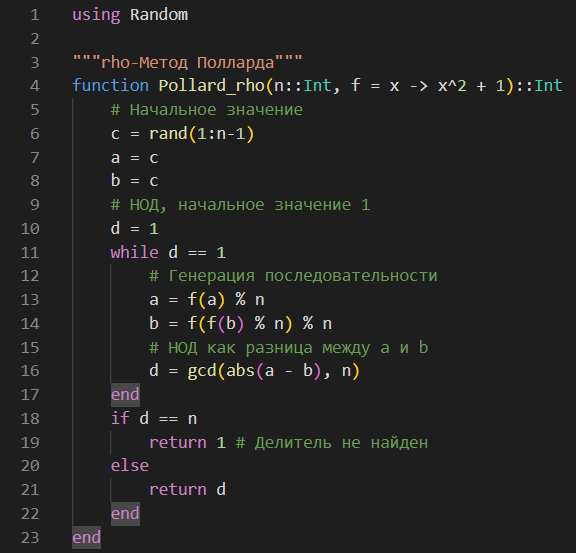
У числа два делителя, не меньших, чем — это числа и . Тогда получаем два представления:

1. , откуда , и ;
2. , откуда , и .

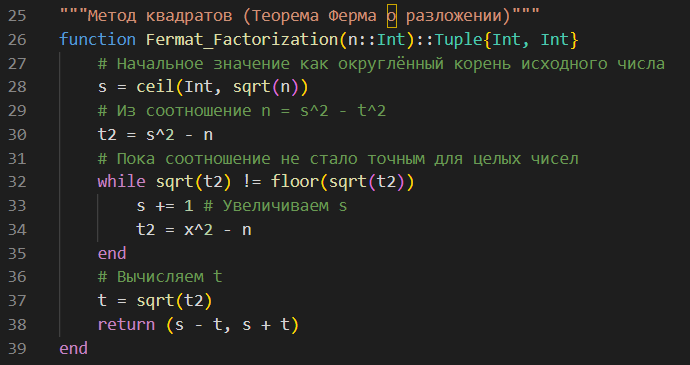
# 3 Выполнение лабораторной работы

Действуя согласно [1], реализуем все описанные алгоритмы на языке Julia.

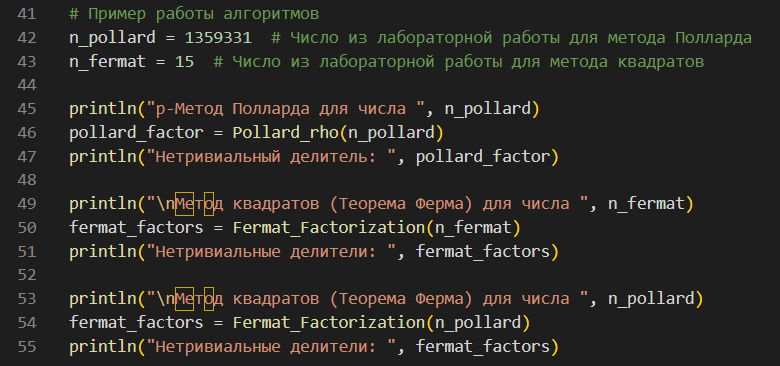
Реализуем функцию -метода Полларда для нахождения нетривиального делителя составного числа (Рис.[??]) и метод квадратов (теорема Ферма о разложении) для разложения составного числа на 2 нетривиальных множителя (Рис.[??]). Найдём делители и разложим на множители числа 15 и 1359331 (Рис.[??]), в результате чего получим следующий вывод, представленный на Рис.[??].



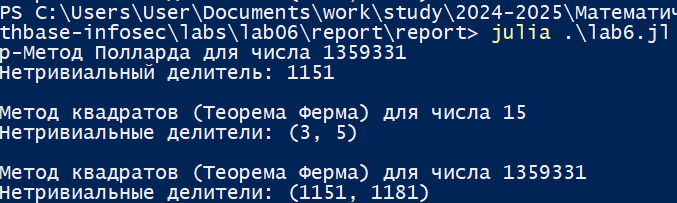
Код алгоритма -метода Полларда на Julia



Код алгоритма метода квадратов (теорема Ферма о разложении) на Julia



Начальные данные для сравнения алгоритмов разложения чисел на множители на Julia



Результат выполнения кода и сравнения алгоритмов разложения чисел на множители на Julia

# 4 Выводы

В ходе выполнения лабораторной работы я изучил работу алгоритмов разложения чисел на множители: -Метод Полларда; Метод квадратов (Теорема Ферма о разложении); а также реализовал их программно.

# Список литературы

1. Лабораторная работа № 6. Разложение чисел на множители [Электронный ресурс]. Саратовский государственный университет имени Н.Г. Чернышевского, 2024.