Математические основы защиты информации и информационной безопасности

Отчет по лабораторной работе № 6 : Paложение чисел на множители.

Кейела Патачона, группа НПМмд-02-21

Содержание

[Цель работы 1](#_Toc90600407)

[Выполнение работы 1](#_Toc90600408)

[Метод Полларда 1](#_Toc90600409)

[Алгоритм, реализующий метод Полларда. 2](#_Toc90600410)

[Метод квадратов. (Теорема Ферма о разложении) 3](#_Toc90600411)

[Результаты работы 4](#_Toc90600412)

[Выводы 4](#_Toc90600413)

[Список литературы 4](#_Toc90600414)

# Цель работы

Построить алгоритм, реализующий разложение чисел на множетели.

# Выполнение работы

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

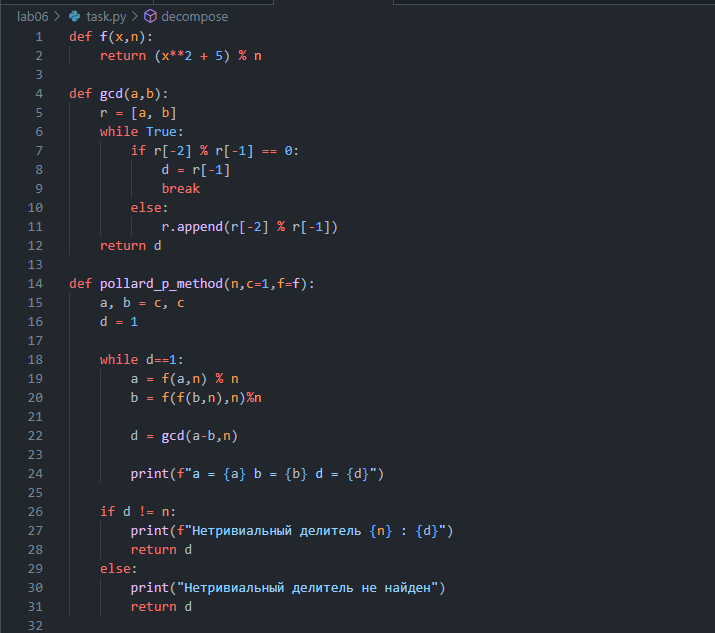
## Метод Полларда

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.

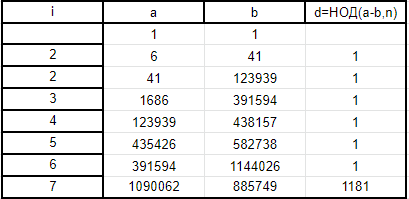
## Алгоритм, реализующий метод Полларда.

***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 результат: “Делитель не найден”; при ввернуться на шаг 2.



метод Полларда

***Пример*** Найти метод Полларда нетривиальный делитель числа . Положим и . Работа алгоритма иллюстрируется следующей таблицей:



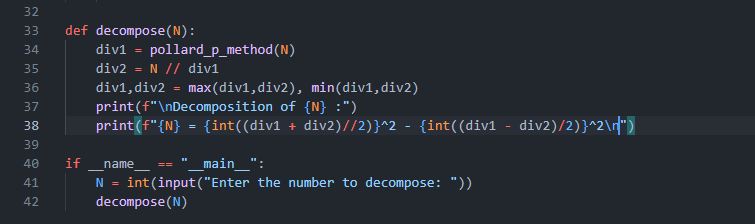
Пример работы алгоритма метода Полларда

Таким образом, 1181 является нетривиальным делителем числа 1359331.

## Метод квадратов. (Теорема Ферма о разложении)

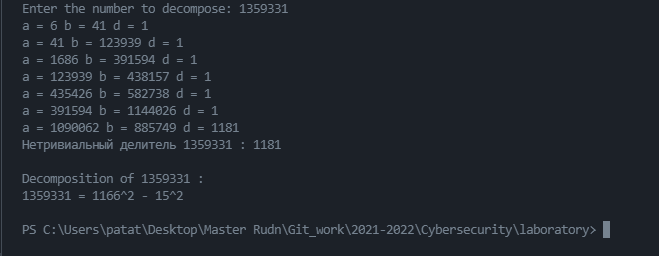
Для любого положительного нечетного числа , существует взаимно однозначное соответствие между множеством делителей числа , не меньших, чем , и множеством пар таких неотрицательных целых чисел, что .

***Пример.*** У числа 15 два делителя, не меньших, чем , - это числа 5 и 15. Тогда получаем два представления: 1. , откуда ; 2. , откуда .

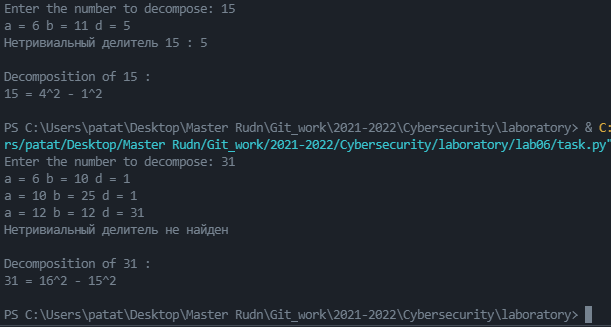


Код программа 1

## Результаты работы



Разложение чисел 1



Разложение чисел 2

# Выводы

В ходе этой лабораторной работы, я изучил и построил алгоритм метода Полларда и научился разложение чисел на множетели и в виде разности квадратов.

# Список литературы

1. [Инструкция к лабораторной работе №6](https://esystem.rudn.ru/pluginfile.php/1283452/mod_folder/content/0/lab06.pdf?forcedownload=1)