Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Данилова Анастасия Сергеевна

Содержание

[Цель работы 1](#_Toc183010777)

[Задание 1](#_Toc183010778)

[Теоретическое введение 1](#_Toc183010779)

[Выполнение лабораторной работы 2](#_Toc183010780)

[Выводы 3](#_Toc183010781)

[Список литературы 4](#_Toc183010782)

# Цель работы

Изучить методы разложения чисел на множители и реализовать их программно на языке программмирования Julia.

# Задание

* Изучить теоретическую часть об алгоритме, который реализует метод Полларда;
* Изучить метод разложения квадратов на множители(теорема Ферма о разложении);
* Реализовать оба метода программно.

# Теоретическое введение

**P-метод Полларда**

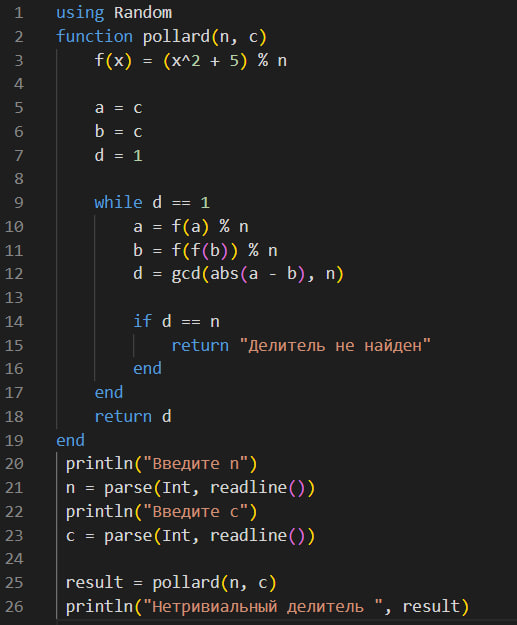
Ро-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Данный алгоритм основывается на алгоритме Флойда поиска длины цикла в последовательности и некоторых следствиях из парадокса дней рождения. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении.

**Метод Квадратов(теорема Ферма о разложении)**

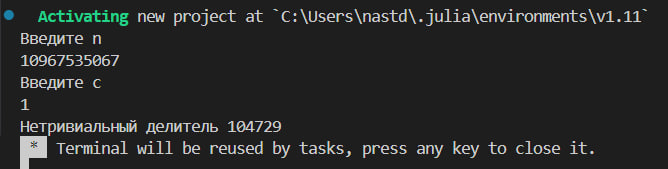
Метод квадратов, связанный с теоремой Ферма о разложении, представляет собой эффективный способ работы с целыми числами и обнаружения свойств связи между делителями и квадратами чисел. Это понимание имеет широкие применения в различных теоретических и практических аспектах математического анализа.

Для каждого нечетного числа мы можем найти пары (s, t), которые позволяют записать число как разность квадратов двух других целых чисел. Метод квадратов показывают, что существуют различные способы представления каждого положительного нечетного числа в виде разности квадратов, что делает этот метод полезным в различных задачах теории чисел.

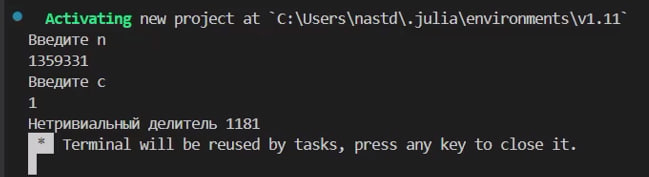
# Выполнение лабораторной работы



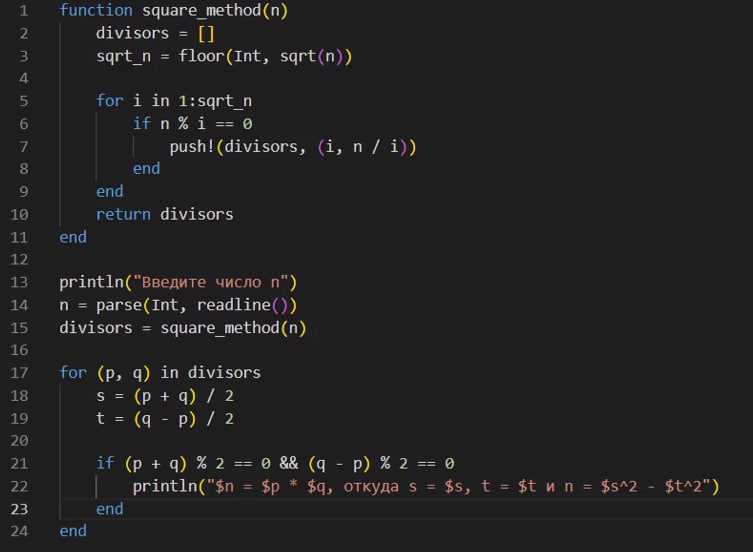
P-Метод Полларда



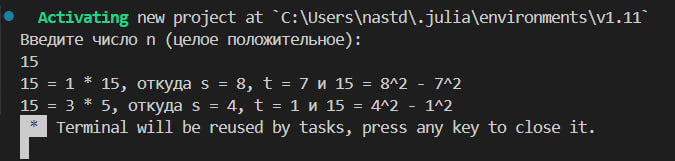
Результат 1



Результат 2



Метод квадратов



Результат

# Выводы

Мы изучили методы разложения чисел на множители и реализовали их программно на языке программмирования Julia.

# Список литературы

1. Mathematics // Julia URL: https://docs.julialang.org/en/v1/base/math/