Лабораторна работа № 6

Разложение чисел на множители

Покрас Илья Михайлович

Содержание

# 1 Цель работы

Реализовать алгоритм разложения чисел на множители.

# 2 Задание

Реализовать алгоритм, реализующий -метод Полларда.

# 3 Теоретическое введение

-алгоритм Полларда — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. -алгоритм строит числовую последовательность, элементы которой образуют цикл, начиная с некоторого номера n, что может быть проиллюстрировано, расположением чисел в виде греческой буквы ρ, что послужило названием семейству алгоритмов

# 4 Выполнение лабораторной работы

Я создал функцию алгоритма, реализующего -метод Полларда, принимающий число для разложения n и начальное значение c. Далее я задал число для разложения множителей, вызвал функцию и вывел полученные данные (рис. 1).

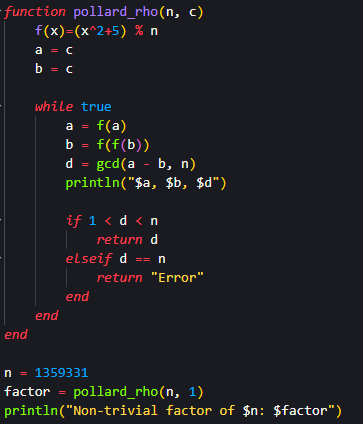


Рис. 1: Функция -метода Полларда

И получил следующий результат (рис. 2).

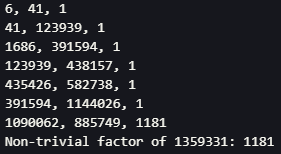


Рис. 2: Результат выполнения кода

Здесь выведены значения a, b и n на каждой итерации и финальный резльутат.

# 5 Выводы

Я реализовал алгоритм реализующий -метод Полларда.

# Список Литературы

1. [Julia - Control Flow](https://docs.julialang.org/en/v1/manual/control-flow/)
2. [Julia - Mathematical Operations](https://docs.julialang.org/en/v1/manual/mathematical-operations/)
3. [Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone - Handbook of Applied Cryptography](https://cacr.uwaterloo.ca/hac/)