Отчёт по лабораторной работе 6

Разложение чисел на множители

Каримов Зуфар Исматович НФИ-01-22

Содержание

# Цель работы

Реализация алгоритма, реализующий p-метод Полларда.

# Теоретические сведения

Один из простейших способов разложить число на простые множители − это проверить, делится ли данное число на 2, 3, 5 ,… и т.д., т.е. проверить, делится ли число на ряд простых чисел. Если число n не делится ни на какое простое число до , то даннаое число является простым, т.к. если число составное, то имеет по крайней мере два множителя и оба они не могут быть больше .

Представим алгоритм разложения числа n на простые множители. Подготовим заранее таблицу простых чисел до s=. Обозначим ряд простых чисел через [1].

**p-алгоритм Поллрада**

* 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 вернуться на шаг 2.

# Выполнение лабораторной работы

1. Написал функцию pollarda для алгоритма полларда. (рис. 1)



Figure 1: Функция для алгоритма полларда

1. Получил результат (рис. 2)

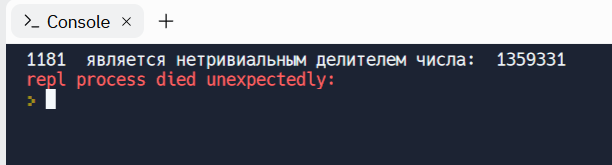


Figure 2: Результат алгоритма

# Выводы

Реализовал алгоритм, реализующий p-метод Полларда.

# Список литературы

1. Разложение числа на простые множители онлайн [Электронный ресурс] - Режим доступа: https://matworld.ru/teorija-chisel/razlozhenie-chisel.php