Лабораторная работа №7

Математические основы защиты информации и информационной безопасности

Дарижапов Тимур Андреевич

Содержание

# Цель работы

Познакомиться с дискретным логарифмированием в конечном поле.

# Задание

Реализовать алгоритм, реализующий р-метод Полларда.

# Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

Для реализации р-метода Полларда была написана следующая программа (рис. 1 ) (рис. 2 ):

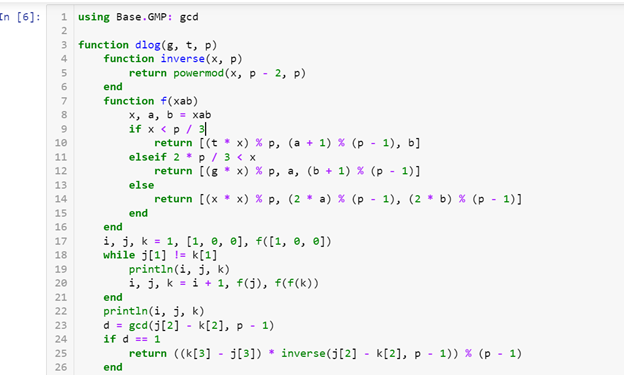


Figure 1: Программа реализации р-метода Полларда

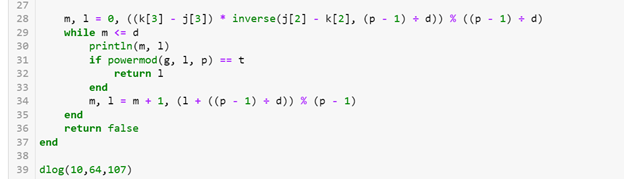


Figure 2: Программа реализации р-метода Полларда

В данной программе:

1 строка: подключение библиотеки для нахождения НОД

3: задание функции

4-16: задание внутренней функции для вывода результатов

17: Задаём начальные значения

18: Начинаем вычисление, пока не получим равенство

18-36: запускаем основной алгоритм, который с помощью вычисления остатков от деления и формул, представленных в лабораторной работе, формирует таблицу ответов.

39: запускаем функцию.

Мы можем видеть результат на (рис. 3 ) . Программа работает верно.

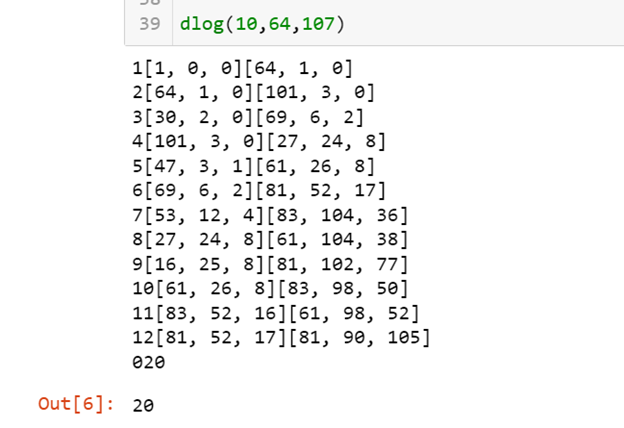


Figure 3: Выводы

# Выводы

Я познакомился с алгоритмом разбора числа на множители и реализовал алгоритм р-метод Полларда.

# Список литературы

Лабораторная работа №7

Разложение чисел на множители [Электронный ресурс]. URL: https://esystem.rudn.ru/mod/folder/view.php?id=1150980