Математические основы защиты информации и информационной безопасности. Отчет по лабораторной работе № 7

Дискретное логарифмирование в конечном поле

Лубышева Ярослава Михайловна

Содержание

# 1 Цель работы

Выполнить задание к лабораторной работе № 7 [1].

# 2 Задание

1. Ознакомиться с алгоритмом, реализующим p-метод Полларда для задач дискретного логарифмирования.
2. Реализовать алгоритм программно.
3. Проверить правильность работы алгоритма путем вычисления логарифма для заданных значений.

# 3 Выполнение лабораторной работы

Для реализации алгоритмов вычисления наибольшего общего делителя была написана программа на языке программирования Python (fig. 1 - fig. 2).

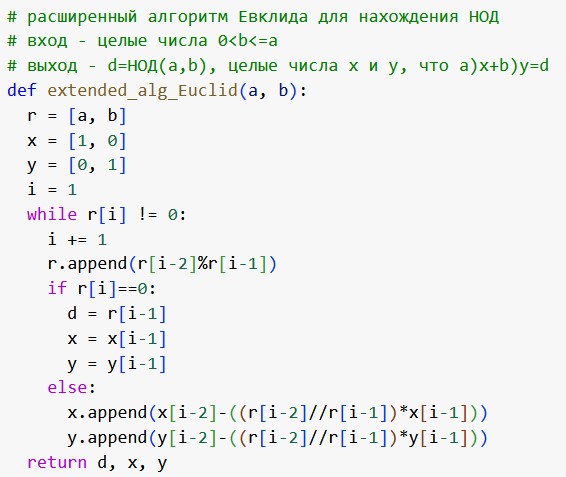


Figure 1: Программная реализация расширенного алгоритма Евклида для нахождения НОД

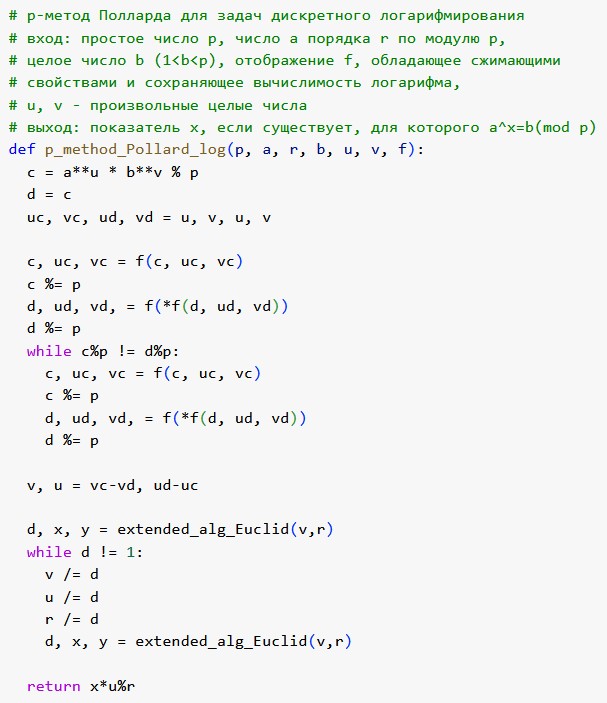


Figure 2: Программная реализация р-метода Полларда для задач дискретного логарифмирования

Результаты работы алгоритмов представлены на рисунке ниже (fig. 3).

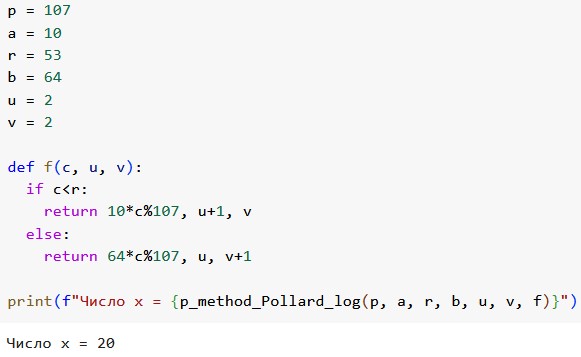


Figure 3: Результаты работы р-метода Полларда для задач дискретного логарифмирования

# 4 Выводы

Выполнено задание к лабораторной работе № 7.

# 5 Список литературы

1. Методические материалы курса