Отчет по лабораторной работе №7

Дисциплина: Математические основы защиты информации и информационной безопасности

Выполнила Дяченко Злата Константиновна, НПМмд-02-22

Содержание

# 1 Цель работы

Ознакомится и реализовать алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования.

# 2 Задание

Реализовать программно алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования.

# 3 Теоретическое введение

Алгоритм, реализующий p-метод Полларда. *Вход*. Простое число ,число порядка по модулю , целое число , 1<b<p; отображение обладающее сжимающими свойствами и сохраняющее вычислимость логарифма. *Выход*. Показатель x для которого если такой показатель существует. 1. Выбрать произвольные целые числа и положить . 2. Выполнять , вычисляя при этом логарифмы для и как линейные функции от x по модулю , до получения . 3. Приравняв логарифмы для и , вычислить логарифм x решением сравнения по модулю . Результат: x или “Решений нет”

# 4 Выполнение лабораторной работы

## 4.1 Шаг 1

Ознакомилась с предоставленными теоретическими данными. Для выполнения задания решила использовать язык Python. Написала функцию, реализующую 1-2 шаг алгоритма p-метода Полларда для задач дискретного логарифмирования. Код функции и результат ее использования представлен на Рисунке 1 (рис. - fig. 1) и Рисунке 2 (рис. - fig. 2). Функция принимает на вход число и число . Пример работы алгоритма для числа из представленых для лабораторной работы материалов также представлен на рисунке.

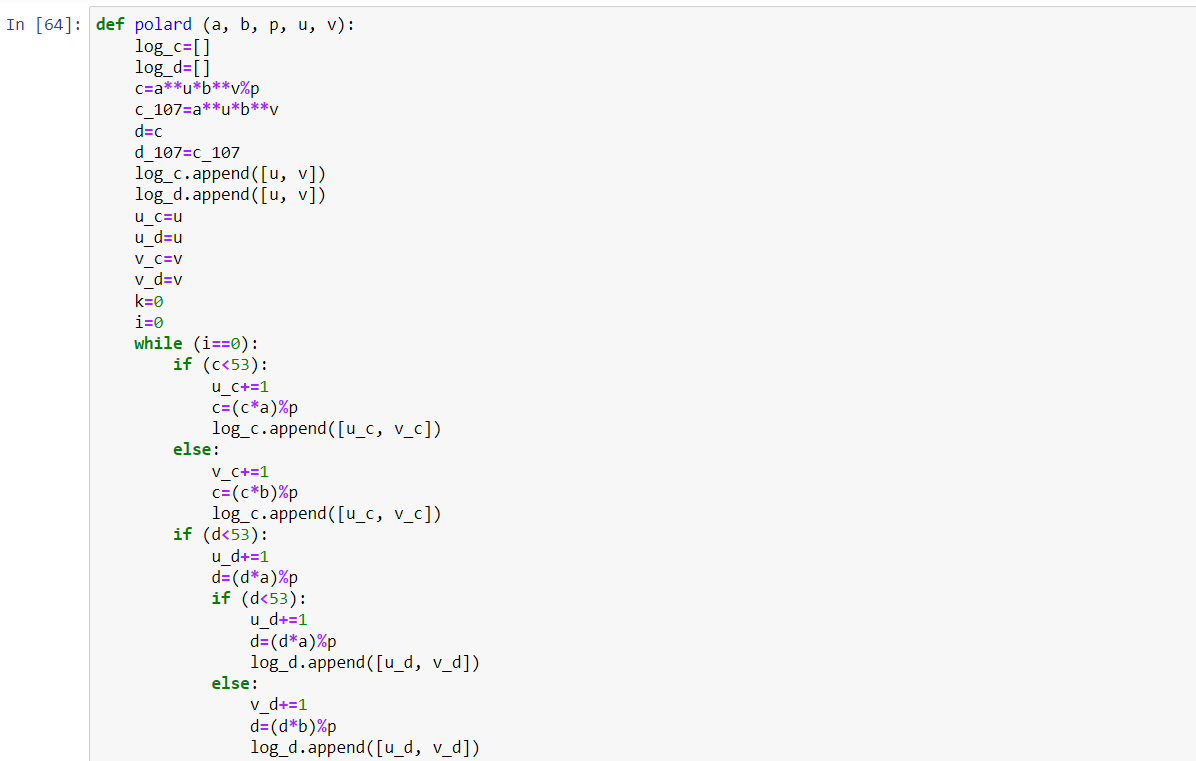


Figure 1: Реализация шагов 1 и 2 алгоритма, реализующего p-метод Полларда для задач дискретного логарифмирования

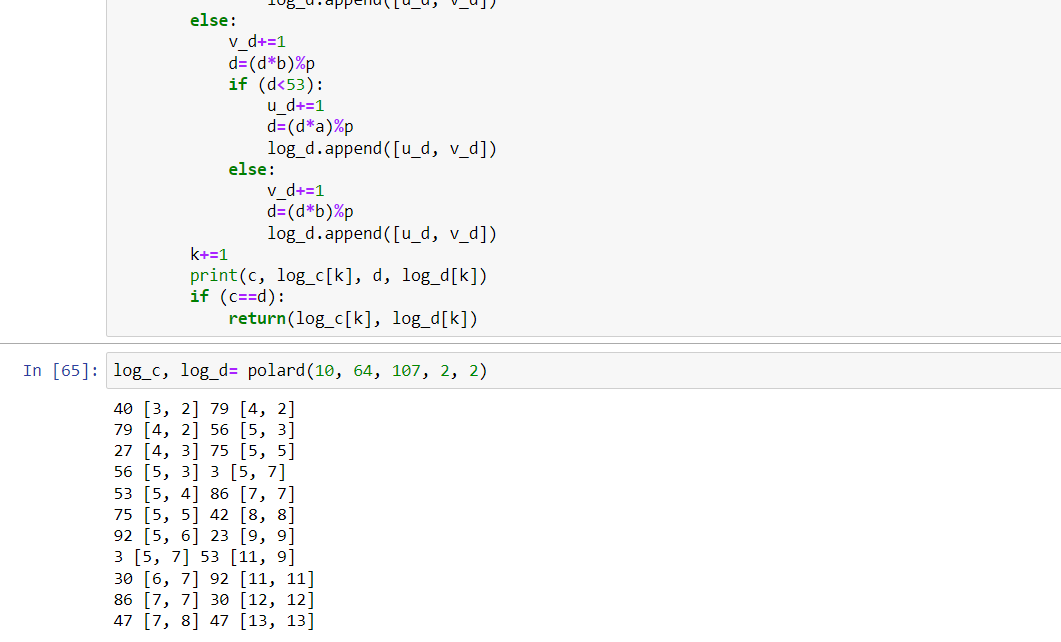


Figure 2: Реализация шагов 1 и 2 алгоритма, реализующего p-метод Полларда для задач дискретного логарифмирования

## 4.2 Шаг 2

Реализовала 3 шаг алгоритма, написав функцию *poisk*. Код функции и результат ее использования представлен на Рисунке 3 (рис. - fig. 3). Полученный ответ совпадает с ответом, представленным в теоретических материалах.

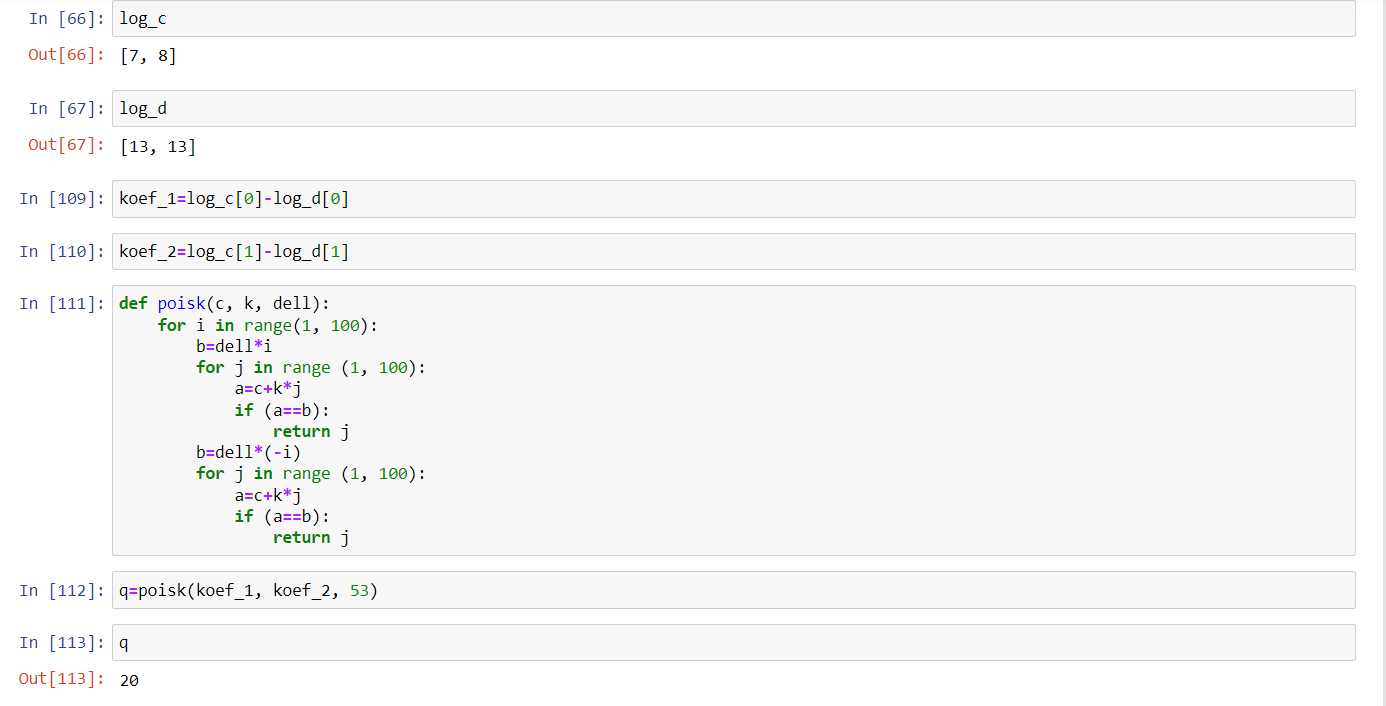


Figure 3: Реализация 3 шага алгоритма

# 5 Выводы

Я ознакомилась с алгоритмом, реализующем p-метод Полларда для задач дискретного логарифмирования, и реализовала его программно. Результаты работы находятся в [репозитории на GitHub](https://github.com/ZlataDyachenko/workD), а также есть [скринкаст выполнения лабораторной работы](https://www.youtube.com/watch?v=Zj6k0AjUHYA).