Отчёт по лабораторной работе №7

Нирдоши Всеволод Раджендер

#### **Цель работы:**

Изучение задачи дискретного логарифмирования в конечных полях и алгоритма -метода Полларда для её решения. Реализация алгоритма с использованием языка программирования Julia.

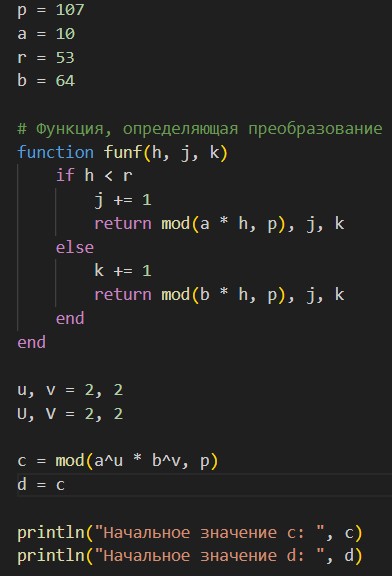
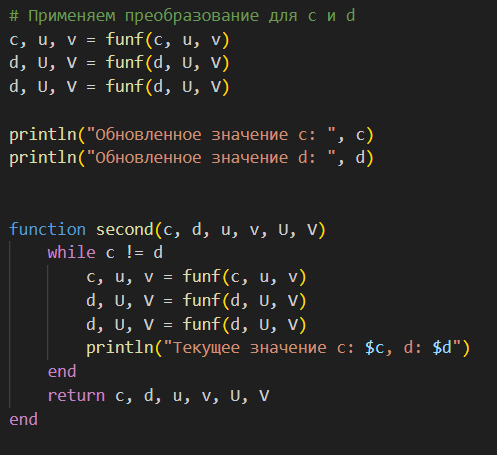
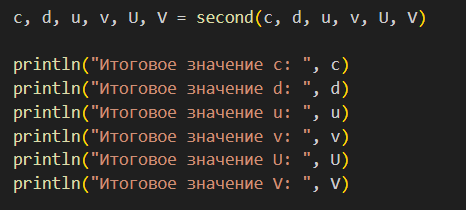
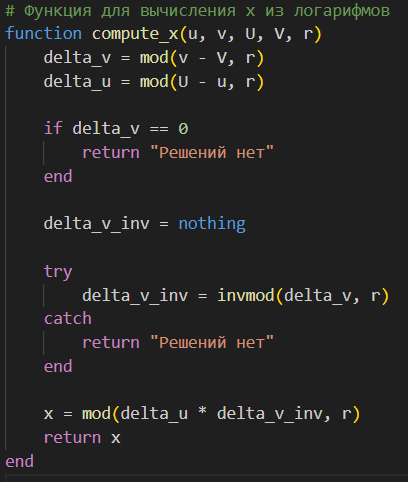
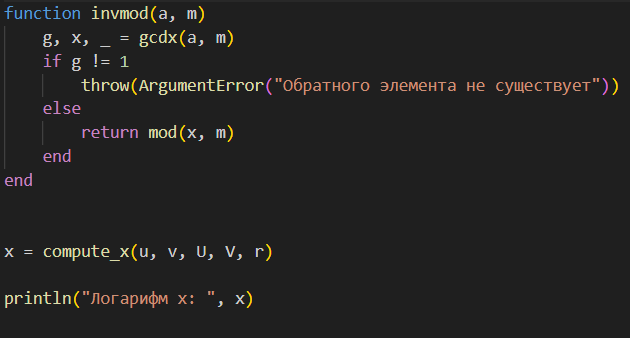
#### **Задачи:**

1. Разобраться с основами конечных полей и их свойствами, включая операции сложения, умножения и нахождения обратных элементов.
2. Изучить теоретическую основу -метода Полларда для решения задачи дискретного логарифмирования.
3. Реализовать алгоритм на языке Julia, обеспечивая корректность вычислений на каждом этапе.
4. Проверить работоспособность алгоритма на конкретных данных и проанализировать результаты.

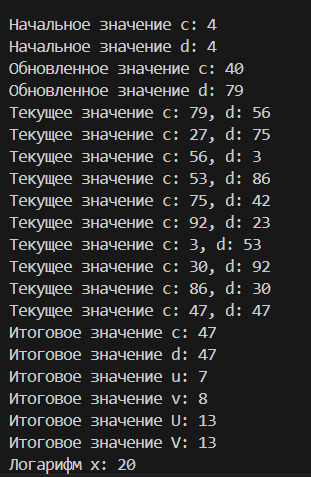
#### **Проделанная работа:**

1. **Теоретическая часть:**
   * Изучены основные свойства конечных полей и их применение в криптографии.
   * Разобрана суть задачи дискретного логарифмирования:
   * где — простое число, — основание, — значение, и — логарифм, который необходимо найти.
   * Изучен алгоритм -метода Полларда, включая использование двух указателей (медленного и быстрого) для обнаружения коллизий.
2. **Практическая часть:**
   * Реализована функция для итеративного обновления значений , , и в соответствии с определённым случайным отображением:
     + Если : обновляется показатель , связанный с основанием .
     + Если : обновляется показатель , связанный с основанием .
   * Реализован поиск коллизий между двумя указателями (медленным и быстрым).
   * Разработана функция для решения уравнения:
   * с использованием вычисления обратного элемента через расширенный алгоритм Евклида.
   * Проведена проверка правильности найденного значения путём подстановки в исходное уравнение.
3. **Тестирование алгоритма:**
   * Алгоритм протестирован на следующих данных:
   * На 11-м шаге обнаружена коллизия, и вычислено значение .

#### **Скриншоты кода**

#### **Итог**



### **Результаты работы:**

* Значение дискретного логарифма:
* Проверка:
* что подтверждает корректность алгоритма.

#### **Выводы:**

1. Алгоритм -метода Полларда успешно реализован и протестирован. Он позволяет эффективно находить дискретный логарифм в конечных полях.
2. Вычисленные значения при коллизии подтверждают корректность обновлений логарифмов в процессе работы алгоритма.
3. Реализация функций для работы с конечными полями, включая нахождение обратных элементов, показала высокую точность и стабильность.
4. Основная сложность заключалась в правильной реализации и проверке каждого шага алгоритма, включая корректность работы с модульной арифметикой.
5. Итоговый результат может быть использован для изучения задач дискретного логарифмирования и в дальнейшем применён в криптографических протоколах.