Отчёт по лабораторной работе №7

Аветисян Давид Артурович

7 декабря 2024

РУДН, Москва, Россия

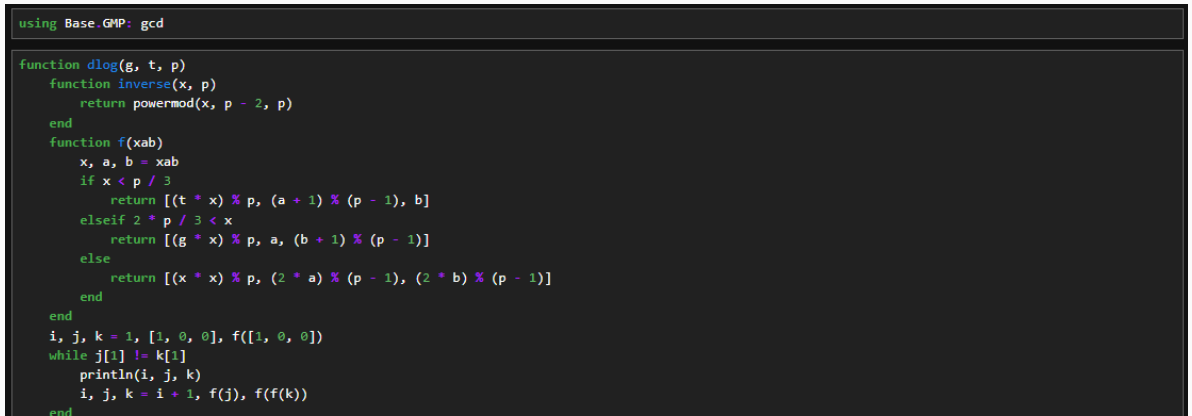
Цель работы

Познакомиться с дискретным логарифмированием в конечном поле.

Выполнение лабораторной работы

В данной программе:

- 1 строка: подключение библиотеки для нахождения НОД.
- 3 строка: задание функции.
- 4-16 строки: задание внутренней функции для вывода результатов.
- 17 строка: задание начальных значений.
- 18 строка: начало вычисления, пока не получим равенство.
- 19-36 строки: запуск основного алгоритма, который с помощью вычисления остатков от деления и формул, представленных в теории лабораторной работы, формирует таблицу ответов.
- 39 строка: запуск функции



```
using Base.GMP: gcd

function dlog(g, t, p)
    function inverse(x, p)
        return powermod(x, p - 2, p)
    end
    function f(xab)
        x, a, b = xab
        if x < p / 3
            return [(t * x) % p, (a + 1) % (p - 1), b]
        elseif 2 * p / 3 < x
            return [(g * x) % p, a, (b + 1) % (p - 1)]
        else
            return [(x * x) % p, (2 * a) % (p - 1), (2 * b) % (p - 1)]
        end
    end
    i, j, k = 1, [1, 0, 0], f([1, 0, 0])
    while j[1] != k[1]
        println(i, j, k)
        i, j, k = i + 1, f(j), f(f(k))
    end
```

Выполнение лабораторной работы

Мы можем видеть результат на рисунке ниже. Программа работае верно.

```
39  dlog(10,64,107)
```

```
1[1, 0, 0][64, 1, 0]
2[64, 1, 0][101, 3, 0]
3[30, 2, 0][69, 6, 2]
4[101, 3, 0][27, 24, 8]
5[47, 3, 1][61, 26, 8]
6[69, 6, 2][81, 52, 17]
7[53, 12, 4][83, 104, 36]
8[27, 24, 8][61, 104, 38]
9[16, 25, 8][81, 102, 77]
10[61, 26, 8][83, 98, 50]
11[83, 52, 16][61, 98, 52]
12[81, 52, 17][81, 90, 105]
020
```

Выводы

Я познакомился с дискретным логарифмированием в конечном поле и реализовал p-метод Полларда.