Лабораторная работа №7. Дискретное логарифмирование в конечном поле.

Alexander S. Baklashov

30 November, 2023

RUDN University, Moscow, Russian Federation

Цель работы

Цель работы

Рассмотреть и реализовать алгоритм, реализующий ρ-метод Полларда для задач дискретного логарифмирования.

Реализуем ρ-Метод Полларда

In [1]:

```python
import time
start_time = time.time()
Flag = False

def f(c, u, v):
    if c < 53:
        return (10 * c) % 107, u + 1, v
    elif (c >= 53):
        return (64 * c) % 107, u, v + 1

p = 107  # Простое число p
a = 10   # Число a
b = 64   # Число b
r = 53   # Порядок числа a по модулю p
u = 2    # Произвольное число
v = 2    # Произвольное число

# Инициализация переменных для чисел c и d, а также их параметров u и v
uc = 2
vc = 2
ud = 2
vd = 2

# Вычисление начальных значений c и d
c = ((a ** u) * (b ** v)) % p
d = c

# Применение функции отображения f к числам c и d и их параметрам u и v
c, uc, vc = f(c, uc, vc)
d, ud, vd = f(f(d, ud, vd)[0], f(d, ud, vd)[1], f(d, ud, vd)[2])

# Цикл, выполняющий алгоритм p-метода Полларда до совпадения чисел c и d
while c % p != d % p:
    c, uc, vc = f(c, uc, vc)
    d, ud, vd = f(f(d, ud, vd)[0], f(d, ud, vd)[1], f(d, ud, vd)[2])

# Нахождение искомой степени числа a
x = 1
while (uc + vc * x) % r != (ud + vd * x) % r:
    x += 1
    elapsed_time = time.time() - start_time
    if elapsed_time > 5:
        print("Решений нет")
        Flag = True
        break

# Вывод степени числа a
if (Flag != True):
    print("x =", x)
```

```
x = 20
```

Figure 1: ρ-Метод Полларда

Вывод

Вывод

В ходе данной лабораторной работы я рассмотрел и реализовал алгоритм, реализующий ρ-метод Полларда для задач дискретного логарифмирования.