Разложение чисел на множители

Бакундукизе Эжид Принц НФИмд-01-21

21 сентября, 2022, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение задачи дискретного логарифмирования в конечном поле.

Выполнение лабораторной работы

Задача дискретного логарифмирования

Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x, удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы.

ρ-алгоритм Поллрада

- Вход. Простое число p, число a порядка r по модулю p, целое число bб $1 < b < p$; отображение f, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.
- Выход. показатель x, для которого $a^x = b(mod p)$, если такой показатель существует.

1. Выбрать произвольные целые числа u, v и положить $c = a^u b^v (mod p), d = c$
2. Выполнять $c=f(c)(mod p), d=f(f(d))(mod p), вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r, до получения равенства $c = d(mod p)$
3. Приняв логарифмы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат x или РЕШЕНИЯ НЕТ.

Пример работы алгоритма

```
In [70]: p = 107
         a = 10
         b = 64
         r = 53
         u = 2
         v = 2


         print('Результат ', Pol(p, a, r, b, u, v))

Результат  20.0
```

Figure 1: Работа алгоритма

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения данной лабораторной работы мы познакомились с дискретным логарифмированием в конечном поле, программно реализовали алгоритм Полларда.