P-метод Полларда для задач дискретного логорифмирования.

Меньшов Иван Сергеевич

24 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цель работы

Цель работы

Изучить алгоитм реализующий P-метод Полларда для задач дискретного логорифмирования.

Выполнение лабораторной работы

P-метод Полларда для задач дискретного логорифмирования

Вход: Простое число p, число a порядка r по модулю p, целое число b, 1 < b <p; отображение f, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.

Выход. Показатель x, для которого $a^x = b \pmod p$, если такой показатель существует.

P-метод Полларда для задач дискретного логорифмирования

1. Выбрать произвольные целые числа u, v и положить $c = a^u b^v \pmod p$, $d = c$.
2. Выполнять $c = f(c) \pmod p$, $d = f(f(d)) \pmod p$, вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r, до получения равенства $c = d \pmod p$.
3. Приравняв логарифмы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат: x или “Решений нет”

Контрольные пример - код

```python
a = 10
b = 64
p = 107
u_0 = 2
v_0 = 2


def f(c, a, b, p):
    if c < (p // 2):
        return a * c
    else:
        return b * c


c = (a ** u_0 * b ** v_0) % p
d = c

while True:
    c = f(c, a, b, p) % p
    d = f(f(d, a, b, p) % p, a, b, p) % p
    print(c, d)
    if c == d % p:
        break
```

Figure 1: P-метод Полларда для задач дискретного логорифмирования python

Контрольные пример - работа программы

Figure 2: P-метод Полларда для задач дискретного логорифмирования работа алгоритма

Выводы

Результаты выполнения лабораторной работы

Мной было изучен алгоитм реализующий P-метод Полларда для задач дискретного логорифмирования. К сожаленю данный алгоритм нуждается в доработке - этот вывод был сделан преподавателем на семинаре.