

Отчёт по лабораторной работе №7.

Дискретное логарифмирование в конечном поле

Бармина Ольга

2024 September 8th

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Целью данной лабораторной работы является ознакомление с алгоритмом, реализующим p -метод Полларда для дискретного логарифмирования, а также программное воплощение данного алгоритма.

1. Реализовать рассмотренный в инструкции к лабораторной работе алгоритм программно.
2. Подставить численное значение из примера в программный код, проверить правильность полученного ответа.

Ход выполнения и результаты

Ввод функции, зависящей от c, u, v

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

Figure 1: Вспомогательная функция, зависящая от c, u, v

Ввод функции для внедрения расш. алгоритма Евклида

```
def ext_euclid(a, b):  
    r=[]  
    x=[]  
    y=[]  
    r.append(a)  
    r.append(b)  
    x.append(1)  
    x.append(0)  
    y.append(0)  
    y.append(1)  
    i=1  
    while r[i]!=0:  
        i +=1  
        r.append(r[i-2]%r[i-1])  
        if r[i]==0:  
            d=r[i-1]  
            x=x[i-1]  
            y=y[i-1]  
        else:  
            x.append(x[i-2]-((r[i-2]//r[i-1])*x[i-1]))  
            y.append(y[i-2]-((r[i-2]//r[i-1])*y[i-1]))  
    return d, x, y
```

Figure 2: Вспомогательная функция. Расширенный алгоритм Евклида

Алгоритм, реализующий Ро-метод Полларда. Реализация

```
def pollard(p, a, b, r, u, v):  
    c = (a**u * b**v)%p  
    d = c  
  
    uc = u  
    vc = v  
    ud = u  
    vd = v  
    i = 0  
    while c%p != d%p or i==0:  
        c, uc, vc = f(c, uc, vc)  
        c %= p  
        d, ud, vd = f(*f(d, ud, vd))  
        d %= p  
        i+=1  
  
    v = vc - vd  
    u = ud - uc  
    d,x,y = ext_euclid(v,r)  
    while d!=1:  
        v/=d  
        u/=d  
        r/=d  
        d,x,y = ext_euclid(v,r)  
    return x*u*r
```


Результат проверки по данным из примера

```
pollard(107, 10, 64, 53, 2, 2)
```

```
20
```

Figure 4: Результат реализации Ро-метода Полларда на примере

В результате выполнения данной лабораторной работы нам удалось осуществить программно алгоритм, рассмотренный в описании к лабораторной работе. А также получить ответ, совпадающий с ответом из инструкции.