

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ
Факультет физико-математических и естественных наук
Кафедра прикладной информатики и теории вероятностей

Отчёт по лабораторной работе №7.
Дискретное логарифмирование в конечном
поле

*Дисциплина: Математические основы защиты
информации и информационной безопасности*

Студент: Асеинова Елизавета, 1132236897
Группа: НФИмд-01-23
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2023

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
3.1	Ро-метод Полларда	7
3.2	Сложность алгоритма	7
4	Выполнение лабораторной работы	8
4.1	Ро-метод Полларда	8
5	Выводы	11
	Список литературы	12

Список таблиц

Список иллюстраций

4.1	Вспомогательная функция, зависящая от s, u, v	8
4.2	Вспомогательная функция. Расширенный алгоритм Евклида . . .	9
4.3	Реализация алгоритма Ро-метода Полларда для логарифмирования	9
4.4	Реализация алгоритма Ро-метода Полларда для логарифмирования	10
4.5	Результат реализации Ро-метода Полларда на примере	10

1 Цель работы

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

2 Задание

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

3 Теоретическое введение

В данной лабораторной работе предметом нашего изучения стал Ро-метод Полларда для задач дискретного логарифмирования.

3.1 Ро-метод Полларда

Ро-метод Полларда для дискретного логарифмирования (ρ -метод) — алгоритм дискретного логарифмирования в кольце вычетов по простому модулю, имеющий экспоненциальную сложность. Предложен британским математиком Джоном Поллардом в 1978 году, основные идеи алгоритма очень похожи на идеи ро-алгоритма Полларда для факторизации чисел. Данный метод рассматривается для группы ненулевых вычетов по модулю p , где p — простое число, большее 3 ([wiki:pol?](#)).

3.2 Сложность алгоритма

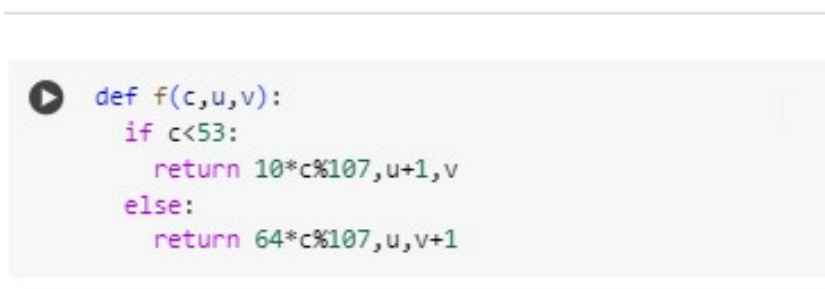
Эвристическая оценка сложности составляет $O(p^{1/2})$.

4 Выполнение лабораторной работы

В соответствии с заданием, была написана программа по воплощению алгоритма Ро-метода Полларда для задач дискретного логарифмирования.

Программный код и результаты выполнения программ представлен ниже.

4.1 Ро-метод Полларда



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

Рис. 4.1: Вспомогательная функция, зависящая от c, u, v


```

def rasshir_algorithm_Evklida(a,b):
    """
    расширенный алгоритм Евклида
    """
    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

```

Рис. 4.2: Вспомогательная функция. Расширенный алгоритм Евклида

```

def Pollard(p,a,r,b,u,v):
    """
    Метод Полларда для логарифмирования в конечном поле
    """
    c=a**u*b**v%p
    d=c
    uc=u
    vc=v
    ud=u
    vd=v
    c,uc,vc=f(c,uc,vc)
    c%=p
    d,ud,vd=f(*f(d,ud,vd))
    d%=p

```

Рис. 4.3: Реализация алгоритма Ро-метода Полларда для логарифмирования

```

while c%p!=d%p:
    ...

    условие работы цикла
    ...

    c,uc,vc=f(c,uc,vc)
    c%=p
    d,ud,vd=f(*f(d,ud,vd))
    d%=p

v=vc-vd
u=ud-uc

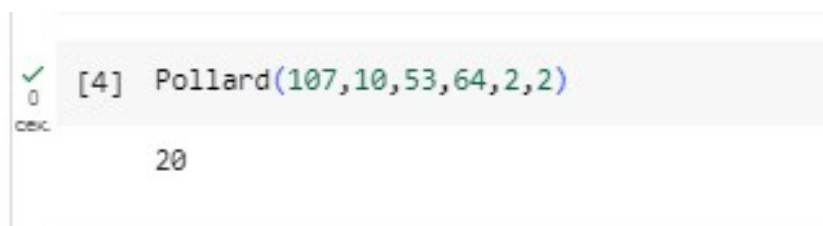
d,x,y=rasshir_algorithm_Evklida(v,r)

while d!=1:
    v/=d
    u/=d
    r/=d
    d,x,y=rasshir_algorithm_Evklida(v,r)

return x*u%r

```

Рис. 4.4: Реализация алгоритма Ро-метода Полларда для логарифмирования



```

[4] Pollard(107,10,53,64,2,2)

20

```

Рис. 4.5: Результат реализации Ро-метода Полларда на примере

5 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: в результате выполнения данной лабораторной работы нам удалось изучить алгоритм Ро-Полларда осуществить программно алгоритм, рассмотренный в описании к лабораторной работе на языке Python 3. А также получить ответ, совпадающий с ответом из инструкции.

Список литературы