Отчёт по лабораторной работе №7  
Дискретное логарифмирование в конечном поле

Студент: Леонова Алина Дмитриевна, 1032212306

Группа: НФИмд-01-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

# 1 Цель работы

Целью данной работы является ознакомление с -методом Полларда для задач дискретного логарифмирования и его реализация на выбранном языке программирования.

# 2 Задание

* Реализовать алгоритм программно.
* Получить у преподавателя задание, содержащее числа , , и вычислить логарифм.

# 3 Теоретическое введение

Задача дискретного логарифмирования, как и задача разложения на множители, применяется во многих алгоритмах криптографии с открытым ключом. Предложенная в 1976 году У. Диффи и М. Хеллманом для установления сеансового ключа, эта задача послужила основой для создания протоколов шифрования и цифровой подписи, доказательств с нулевым разглашением и других криптографических протоколов.

## 3.1 Алгоритм, реализующий –Метод Полларда для задач дискретного логарифмирования.

Вход. Простое число , число порядка по модулю , целое число , 1 < < ; отображение , обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.

Выход. Показатель , для которого , если такой показатель существует.

1. Выбрать произвольные целые числа , и положить .
2. Выполнять , вычисляя при этом логарифмы для и как линейные функции от по модулю , до получения равенства .
3. Приравняв логарифмы для и , вычислить логарифм решением сравнения по модулю . Результат: или “Решений нет”.

## 3.2 Пример

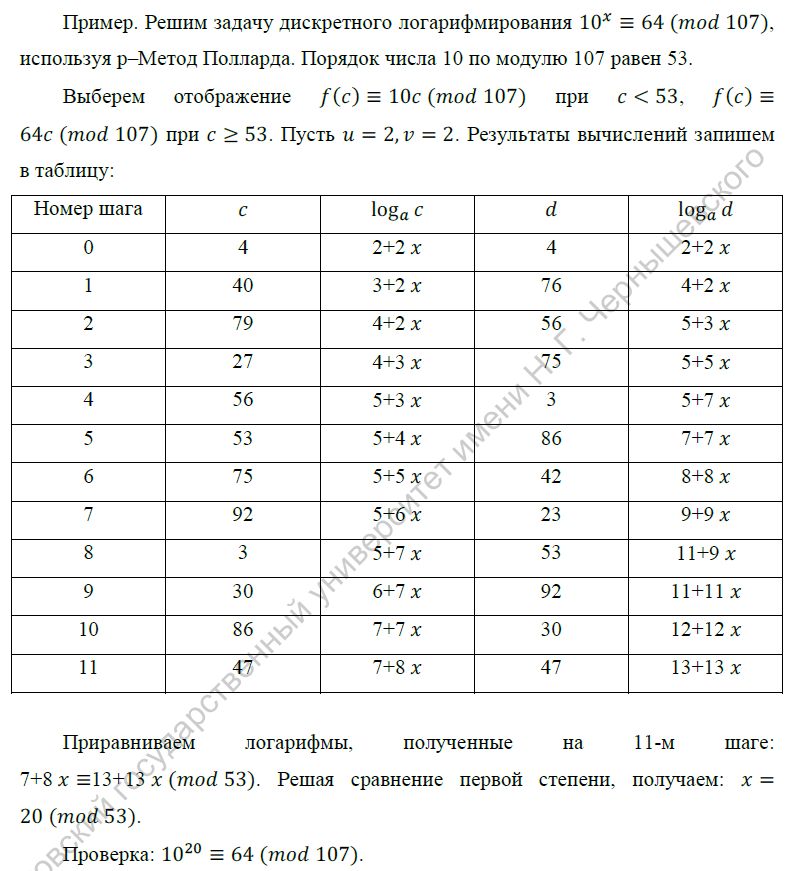


Figure 1: Пример из задания

Для проверки правильности реализации в задании дан пример (см. рис. 1) [1].

# 4 Выполнение лабораторной работы

## 4.1 Промежуточные функции

Функция для вычисления НОД(a,b) расширенным алгоритмом Евклида, взятая с небольшими изменениями из 4 лабораторной работы:

# Расширенный алгоритм Евклида  
# d = НОД(a,b) = ax + by  
def nod3(a, b):  
 if a == 0 or b == 0:  
 return max(a, b)  
 if a == 1 or b == 1:  
 return 1  
 if abs(a) < abs(b):  
 a, b = abs(b), abs(a)  
  
 x, y = [1,0], [0,1]  
 a\_, b\_ = a, b  
   
 while b\_ != 0:  
 a\_, b\_, p = b\_, a\_ % b\_, a\_ // b\_  
   
 x[0], x[1] = x[1], x[0] - p\*x[1]  
 y[0], y[1] = y[1], y[0] - p\*y[1]  
   
 d = a\_  
 #print(a,'\*',x[1],' + ',b,'\*',y[1],' = ',d)  
 return d, abs(y[0]), abs(x[0])

Далее функция для вычисления значения соответствующей функции в зависимости от :

# Функция  
def f(c, u, v):  
 if c < r:  
 return a\*c % p, u+1, v  
 else:  
 return b\*c % p, u, v+1

Функция для печати промежуточных шагов:

def pr(c,uc,vc,d,ud,vd):  
 print(' ',c,' ',uc,' + ',vc,'x ', d,' ',ud,'+',vd,'x')

## 4.2 p-метод Полларда для задач дискретного логарифмирования

с использованием расширенного алгоритма Евклида:

def Pollard\_log(a, p, r, b, u, v):  
 c = a\*\*u \* b\*\*v % p  
 d = c  
 uc, vc = u, v  
 ud, vd = u, v  
  
 print(' c log\_c d log\_d')  
 print('--------------------------------------')  
 pr(c,uc,vd,d,ud,vd)   
  
 c, uc, vc = f(c, uc, vc)  
 c %= p  
 d, ud, vd = f(\*f(d, ud, vd))  
 d %= p  
 pr(c,uc,vd,d,ud,vd)  
   
 while c%p != d%p:  
 c, uc, vc = f(c, uc, vc)  
 c %= p  
 d, ud, vd = f(\*f(d, ud, vd))  
 d %= p  
 pr(c,uc,vd,d,ud,vd)  
   
 v = vc - vd  
 u = ud - uc  
   
 d, x, y = nod3(v, r)  
   
 while d != 1:  
 v /= d  
 u /= d  
 r /= d  
 d, x, y = nod3(v, r)  
 pr(c,uc,vd,d,ud,vd)  
   
 return x\*u % r

## 4.3 Проверка работы алгорима

Проверка работы алгорима на примере из задания:

print('p-метод Полларда ля задач дискретного логарифмирования')  
a = 10  
p = 107  
r = 53  
b = 64  
u = 2  
v = 2  
print(Pollard\_log(a, p, r, b, u, v))

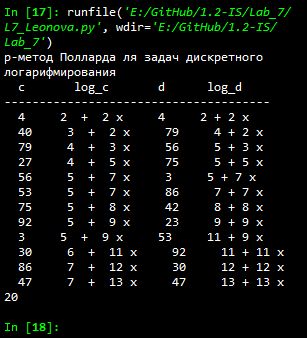


Figure 2: Результат выполнения L7\_Leonova.py

Результат выполнения программы, проверка реализации p-метод Полларда для задач дискретного логарифмирования на заданном примере (см. рис. 2).

# 5 Выводы

Цель лабораторной работы была достигнута, -метод Полларда для задач дискретного логарифмирования был реализован на языке программирования Python и проверен на заданном примере.

# Список литературы

1. Бубнов С.А. Лабораторный практикум по основам криптографии [Электронный ресурс]. Саратовский государственный университет имени Н.Г.Чернышевского, 2012. URL: <http://elibrary.sgu.ru/uch_lit/656.pdf>.