Отчет по лабораторной работе номер 7

Хамбалеев Булат Галимович

Содержание

List of Tables

List of Figures

1 Цель работы

Реализовать алгоритм p-метода Полларда для задач дискретного логарифмирования.

2 Задание

Задание подразумевает реализацию алгоритма ρ-метода Полларда для задач дискретного логарифмирования.

3 Выполнение работы

1. Реализуем функцию алгоритма.(рис. 1)

```
def inverse(x, m):
    a, b, u = 0, m, 1
    while x > 0:
        x, a, b, u = b % x, u, x, a - b // x * u
    if b == 1: return a % m
    return 0

def dlog(g,t,p):

    from fractions import gcd
    def f(xab):
        x, a, b = xab[0], xab[1], xab[2]
        if x < p/3:
            return [(t*x)%p, (a+1)%(p-1), b]
        if 2*p/3 < x:
            return [(g*x)%p, a, (b+1)%(p-1)]
        return [(x*x)%p, (2*a)%(p-1), (2*b)%(p-1)]
    i, j, k = 1, [1,0,0], f([1,0,0])
    while j[0] != k[0]:
        print(i, j, k)
        i, j, k = i+1, f(j), f(f(k))
    print(i, j, k)
    d = gcd(j[1] - k[1], p - 1)
    if d == 1: return ((k[2]-j[2])%(p-1) * inverse((j[1]-k[1])%(p-1),p-1)) % (p-1)
    m, l = 0, ((k[2]-j[2])%((p-1)/d) * inverse((j[1]-k[1])%((p-1)/d),(p-1)/d)) % ((p-1)/d)
    while m <= d:
        print(m, l)
        if pow(int(g),int(l),int(p)) == t:
            return l
        m, l = m+1, (l+((p-1)/d))%(p-1)
    return False
```

Figure 3.1: рис.1. Алгоритм.

2. Проверим работу алгоритма.

```
        return False


    dlog(83,555,997)
```

```
1 [1, 0, 0] [555, 1, 0]
2 [555, 1, 0] [4, 2, 1]
3 [949, 2, 0] [805, 4, 1]
4 [4, 2, 1] [904, 5, 2]
5 [226, 3, 1] [64, 6, 3]
6 [805, 4, 1] [798, 14, 6]
7 [16, 4, 2] [185, 28, 14]
8 [904, 5, 2] [666, 29, 15]
9 [257, 5, 3] [837, 58, 32]
10 [64, 6, 3] [442, 58, 34]
11 [625, 7, 3] [4, 116, 69]
12 [798, 14, 6] [805, 118, 69]
13 [432, 14, 7] [904, 119, 70]
14 [185, 28, 14] [64, 120, 71]
15 [981, 29, 14] [798, 242, 142]
16 [666, 29, 15] [185, 484, 286]
17 [443, 29, 16] [666, 485, 287]
18 [837, 58, 32] [837, 970, 576]
0 46.0
1 129.0
<ipython-input-30-d6d6896c46bf>:24: DeprecationWarning: fractions.gcd() is deprecated. Use math.gcd() instead.
  d = gcd(j[1] - k[1], p - 1)
129.0
```

Figure 3.2: рис.2. Проверка.

4 Библиография

1. ТУИС РУДН

5 Выводы

Во время выполнения лабораторной работы я на практике реализовал алгоритм p-метода Полларда.