

Дискретное логарифмирование в конечном поле

Лабораторная работа №7

Данилова А.С.

- Изучить теоретическую часть о дискретном логарифмировании;
- Реализовать алгоритм программно.

Ро-алгоритм — предложенный Джоном Поллардом в 1975 году алгоритм, служащий для факторизации (разложения на множители) целых чисел. Алгоритм наиболее эффективен при факторизации составных чисел с достаточно малыми множителями в разложении.

Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны.

```
1 using Random
2
3 function mod_exp(base, exp, mod)
4     result = 1
5     base = base % mod
6     while exp > 0
7         if exp % 2 == 1
8             result = (result * base) % mod
9         end
10        exp = div(exp, 2)
11        base = (base * base) % mod
12    end
13    return result
14 end
15
16 function pollard(g, h, p)
17     function f(x)
18         return (mod_exp(g, x[1], p) * mod_exp(g, x[2], p) % p, (x[1] + 1) % (p - 1), (x[2] + 1) % (p - 1))
19     end
20
21     x0 = (0, 0)
22     x1 = f(x0)
23     x2 = f(f(x0))
24
```

Рис. 1: Код

```
25     while true
26         if mod_exp(g, x1[1], p) == h
27             return x1[1]
28         end
29         if mod_exp(g, x2[1], p) == h
30             return x2[1]
31         end
32
33         if x1 == x2
34             return "Не удалось найти логарифм"
35         end
36
37         x1 = f(x1)
38         x2 = f(f(x2))
39     end
40 end
41
42 println("g: ")
43 g = parse{Int, readline()}
44 println("h: ")
45 h = parse{Int, readline()}
46 println("p: ")
47 p = parse{Int, readline()}
48 result = pollard(g, h, p)
49 println("Логарифм: ", result)
```

Рис. 2: Код

$$3^x \equiv 13 \pmod{17}.$$

Рис. 3: Пример задачи

```
Activating new project at `C:\Users\nastd\.julia\environments\v1.11`  
g:  
3  
h:  
13  
p:  
17  
Логарифм: 4  
* Terminal will be reused by tasks, press any key to close it.
```

Рис. 4: Результат

Мы изучили теоретическую часть о дискретном логарифмировании в конечном поле и реализовали алгоритм на языке программирования Julia.