Лабораторная работа №6

Разложение чисел на множители

Кубасов В.Ю.

Содержание

# 1 Цель работы

Реализовать алгоритм дискретного логарифмирования в конечном поле

# 2 Задание

Реализовать алгоритмы:  
- Алгоритм реализующий p-метод Полларда

# 3 Выполнение лабораторной работы

## 3.1 Нахождение логарифма

from random import randint  
from sympy import mod\_inverse  
  
def f(x, a, b, p):  
 if x % 3 == 0:  
 return (x + 1) % p  
 elif x % 3 == 1:  
 return (a \* x) % p  
 else:  
 return (b \* x) % p  
  
def pollard(a, b, p):  
 u, v = randint(0, p - 1), randint(0, p - 1)  
 c = pow(a, u, p) \* pow(b, v, p) % p  
 d = c  
   
 u1, v1 = u, v  
 u2, v2 = u, v  
   
 for i in range(100\_000\_000):  
 c = f(c, a, b, p)  
 d = f(c, a, b, p)  
   
 if c % 3 == 0:  
 u1 = (u1 + 1) % (p - 1)  
 elif c % 3 == 1:  
 v1 = (v1 + 1) % (p - 1)  
   
 if d % 3 == 0:  
 u2 = (u2 + 1) % (p - 1)  
 elif d % 3 == 1:  
 v2 = (v2 + 1) % (p - 1)  
   
 if c == d:  
 num = (u1 - u2) % (p - 1)  
 den = (v2 - v1) % (p - 1)  
   
 try:  
 dev\_inv = mod\_inverse(den, p - 1)  
 x = (num \* den) % (p - 1)  
 return x  
 except ValueError:  
 return "Решений нет"  
   
 return "Решений нет"  
  
print(pollard(10, 64, 107))

# 4 Выводы:

* В ходе работы реализовали алгоритм оптимального нахождения логарифма

# Список литературы