Лабораторная работа №6

Разложение чисел на множители

Кубасов В.Ю.

Вводная часть

Актуальность

- Нахождение логарфима - времязатратный процесс. Необходим алгоритм дискретного быстрого нахождения логарифма

Цели и задачи

Реализовать алгоритмы:

- Алгоритм реализующий p-метод Полларда

Выполнение работы

Нахождение логарифма по методу Полларда:

```
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
```

Нахождение логарифма по методу Полларда:

```
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)
```

Выводы:

Выводы:

- В ходе лабораторной работы реализовали алгоритм нахождения дискретного логарифма