

Отчёт по лабораторной работе №6

Разложение чисел на множители

Федюшина Ярослава Андреевна

Содержание

| | |
|---------------------------------------|----------|
| Цель работы | 4 |
| Задание | 5 |
| Выполнение лабораторной работы | 6 |
| Код на Python | 7 |
| Вывод | 8 |

Список иллюстраций

| | | |
|---|----------------------------------|---|
| 1 | Код Алгоритма Полларда | 7 |
|---|----------------------------------|---|

Цель работы

Изучение задачи разложения на множители, изучение р-алгоритма Полларда.

Задание

Реализовать рассмотренный алгоритм программно.

Выполнение лабораторной работы

Код на Python

```
import math
import random
from math import gcd

def pollard_rho(n):
    c = random.randint(1, n - 1)
    a = b = random.randint(1, n - 1)

    def f(x):
        return (x * x + c) % n

    while True:
        a = f(a)
        b = f(f(b))
        d = gcd(abs(a - b), n)

        if d != 1 and d != n:
            return d
        elif d == n:
            return "Делитель не найден"

n = 1359331
result = pollard_rho(n)
print(f"Нетривиальный делитель числа {n}: {result}")
```

✓ 0.0s

Нетривиальный делитель числа 1359331: 1181

Рис. 1: Код Алгоритма Полларда

Вывод

В ходе выполнения данной лабораторной работы мы изучили задачу разложения на множители, изучили р-алгоритм Полларда и успешно реализовали на языке программирования Python.