Лабораторная работа №6. Разложение чисел на множители.

Alexander S. Baklashov

22 November, 2023

RUDN University, Moscow, Russian Federation

Цель работы

Цель работы

Рассмотреть и реализовать алгоритм, реализующий p-метод Полларда и реализовать метод квадратов.

Реализуем ρ-Метод Полларда

In [1]:

```python
from math import gcd

def f(x, n):
    # Функция для вычисления f(x) (mod n)
    return (x**2 + 5) % n

def find_divisor(n,c):
    a, b = c, c
    while True:
        # Шаг 2: Вычислить a <- f(a) (mod n), b <- f(b) (mod n)
        a = f(a, n)
        b = f(f(b, n), n)

        # Шаг 3: Найти НОД(a - b, n)
        d = gcd(abs(a - b), n)

        # Шаг 4: Проверить результат
        if 1 < d < n:
            # Делитель найден
            return d
        elif d == n:
            # Делитель не найден
            return "Делитель не найден"


c = 1
n = 1359331
result = find_divisor(n,c)
print("Нетривиальный делитель числа", n,"=",result)
```

```
Нетривиальный делитель числа 1359331 = 1181
```

Figure 1: ρ-Метод Полларда

Метод квадратов

Реализуем метод квадратов

In [2]:

```python
from math import isqrt

def square_factorization(n):
    a = isqrt(n) + 1  # ближайшее целое квадратному корню из n
    b2 = a**2 - n

    while not is_square(b2):
        a += 1
        b2 = a**2 - n

    b = isqrt(b2)
    return a + b, a - b  # разложение числа на множители

def is_square(x):
    return isqrt(x)**2 == x


n = 1359331
factors = square_factorization(n)
print(f"Разложение числа {n} на множители: {factors}")
```

```
Разложение числа 1359331 на множители: (1181, 1151)
```

Figure 2: Метод квадратов

Вывод

Вывод

В ходе данной лабораторной работы я рассмотрел и реализовал следующие алгоритмы:

- p-метод Полларда;
- Метод квадратов.