Лабораторная работа №6

Разложение чисел на множители

Цель работы

Реализация (\rho)-метода Полларда для факторизации составного числа (n).

Теоретическая часть

Задача разложения числа на множители заключается в поиске нетривиального делителя составного числа (n). Один из эффективных методов — (\rho)-метод Полларда, который основан на использовании простой функции (f(x) = (x^2 + 1) \mod n).

Описание алгоритма:

1. Задаётся начальное значение (c = 1), (a = c), (b = c).
2. Далее итеративно вычисляются:
    - (a \leftarrow f(a) \mod n),
    - (b \leftarrow f(f(b)) \mod n),
    - (d \leftarrow \text{НОД}(|a - b|, n)).
3. Если (d = n), то алгоритм перезапускается с другим значением (c).
4. Если (1 < d < n), то (d) — нетривиальный делитель числа (n).

Практическая часть

1. Реализация алгоритма

```
from math import gcd

def pollards_rho(n, f=lambda x: (x**2 + 1) % n):
    """
    Реализация алгоритма Полларда для факторизации числа.

    Параметры:
        n (int): Составное число для разложения на множители.
        f (function): Функция для итерации, по умолчанию f(x) = (x^2 + 1) mod n.

    Возвращает:
        int: Нетривиальный делитель числа n или None, если факторизация не
удалась.
    """
    c = 1  # Начальное значение
    a = c
    b = c
    while True:
```

```
        a = f(a)  # Одно обновление a
        b = f(f(b))  # Два обновления b
        d = gcd(abs(a - b), n)  # НОД(|a - b|, n)
        if d == n:  # Неудача, нужно перезапустить с новым c
            return None
        if d > 1:  # Успех, найден нетривиальный делитель
            return d

# Пример: Факторизация числа 1359331
n = 1359331
factor = pollards_rho(n)
if factor:
    print(f"Нетривиальный делитель числа {n}: {factor}.")
    print(f"Другой делитель: {n // factor}.")
else:
    print(f"Не удалось найти делитель для числа {n}.")
```

2. Разложение числа

Для примера разложим число n=1359331,как указано в задании. 1.Подставляем n=1359331 в алгоритм. 2.После выполнения ρ-метода Полларда находим:

- Нетривиальный делитель d=1181.
- Второй делитель n/d=1151.

```
Нетривиальный делитель числа 1359331: 1181.
Другой делитель: 1151.
```

Итоговое разложение: 1359331=1181×1151

```
Вывод
В ходе лабораторной работы реализован ρ-метод Полларда для разложения числа на
множители. Программа успешно нашла разложение числа n = 1359331 на множители 1181
и 1151. Метод применим к другим составным числам, для чего достаточно заменить
значение n в коде.
```