Лабораторная работа №6

Разложение чисел на множители

Доборщук Владимир Владимирович, НФИмд-02-22

Содержание

Список иллюстраций

Список таблиц

1 Цель и задачи работы

Цель — Изучить алгоритмы разложения чисел на множители.

Задачи:

- Реализовать алгоритм нахождения нетривиального сомножителя p-методом Полларда

2 Теоретическая информация

Все теоретическое описание дано в описании лабораторной работы.

3 Выполнение лабораторной работы

Для реализации p-метода Полларда было внесено изменение в функцию $f(x)$ - в ней у нас также выбирается случайное число от 1 до $\sqrt{n}$ и берется по модулю n.

3.1 Реалиазация и тестирование

Программный код выглядит следующим образом:

```
# Laboratory Work
# Theme: Distribution of numbers into factors
# Author: Vladimir Doborschuk

# --- Modules ---

import numpy as np

# --- Functions ---

# --- mod(a, b) ---

def mod(a ,b):
    return a % b

# --- Pollard's P-method ---
```

```
'''
n - целое число
c - начальное значение
f - сжимающая функция
'''
def pollard(n: int, c: int, f):
    d = 1
    cnt = 0
    a, b = c, c

    print(f"a = {a}, b = {b}")

    while d == 1:
        a = mod(f(a), n)
        b = mod(f(b), n)
        d = np.gcd(a - b, n)

        if mod(cnt, 100) == 0 or d != 1:
            print(f"iteration {cnt+1}: a = {a}, b = {b}, d = {d}")

        cnt += 1

    if d == n:
        print("Делитель не найден")
        return None

    return d
```

```
# --- Test ---

def pollard_test(n, c):
    print(f'Поллард {n}\n---------')
    f = lambda x: np.power(x, 2) + mod(np.random.randint(1,
 ↪  np.floor(np.sqrt(n))), n)
    p = pollard(n, c, f)

    if p != None:
        print(f'Нетривиальный делитель {n}: p = {p}')

    print(f'---------\n')

# --- Main ---

def main():
    pollard_test(1359331, 1)
    pollard_test(137, 5)
    pollard_test(322, 12)

if __name__ == "__main__":
    main()
```

При запуске получаем следующие результаты:

```
Поллард 1359331
---------
a = 1, b = 1
iteration 1: a = 281, b = 953, d = 1
iteration 101: a = 666221, b = 55317, d = 1
```

```
iteration 201: a = 1114705, b = 242518, d = 1
iteration 250: a = 1251131, b = 205946, d = 1181
Нетривиальный делитель 1359331: p = 1181
---------

Поллард 137
---------
a = 5, b = 5
iteration 1: a = 32, b = 34, d = 1
iteration 26: a = 40, b = 40, d = 137
Делитель не найден
---------

Поллард 322
---------
a = 12, b = 12
iteration 1: a = 155, b = 146, d = 1
iteration 2: a = 200, b = 78, d = 2
Нетривиальный делитель 322: p = 2
---------
```

4 Выводы

В рамках выполненной лабораторной работы мы изучили и реализовали p-метод Полларда для разложения на нетривиальные сомножители.

Список литературы