\metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction} \makeatletter \beamer@ignorenonframefalse \makeatother

Лабораторная работа №6

Разложение чисел на множители. Метод Полларда

АВТОР
Кюнкриков Д.С. -

ПРИНАДЛЕЖНОСТЬ
Российский университет дружбы народов, Москва, Россия
-

Информация

Докладчик

- Кюнкриков Даниил Саналович
- студент уч. группы НПИмд-01-24
- Российский университет дружбы народов
- 1132249574@pfur.ru
- https://github.com/DanzanK/2025-2026_math-sec/tree/main

Вводная часть

Актуальность

- Реализация p - метода Полларда для разложения чисел на множители

Объект и предмет исследования

- p - метода Полларда
- Факторизация больших чисел
- Псевдослучайные последовательности
- Веб-сервис GitHub
- Язык разметки Markdown
- Язык программирования python

Цели и задачи

- Реализовать p - метода Полларда на языке программирования python.
- Проанализировать поведение алгоритма на заданных числах

Метод Полларда

- Вероятностный алгоритм для нахождения нетривиальных делителей
- Основан на поиске циклов в псевдослучяайной последовательности
- Использует “черепаху” и “зайца” для обнаружения делителей

Алгоритм

1. Выбор псевдослучайной функции f(x) = (x^2 + c) mod n
2. 2.Инициализация a = b = 1
3. На каждом шаге итерации:
    - a = f(a) (step 1)
    - b = f(f(b)) (step 2)
    - d = НОД(|a - b|, n) (где НОД - Наибольший общий делитель)
4. Ессли 1 < d < n - найден нетривиальный делитель

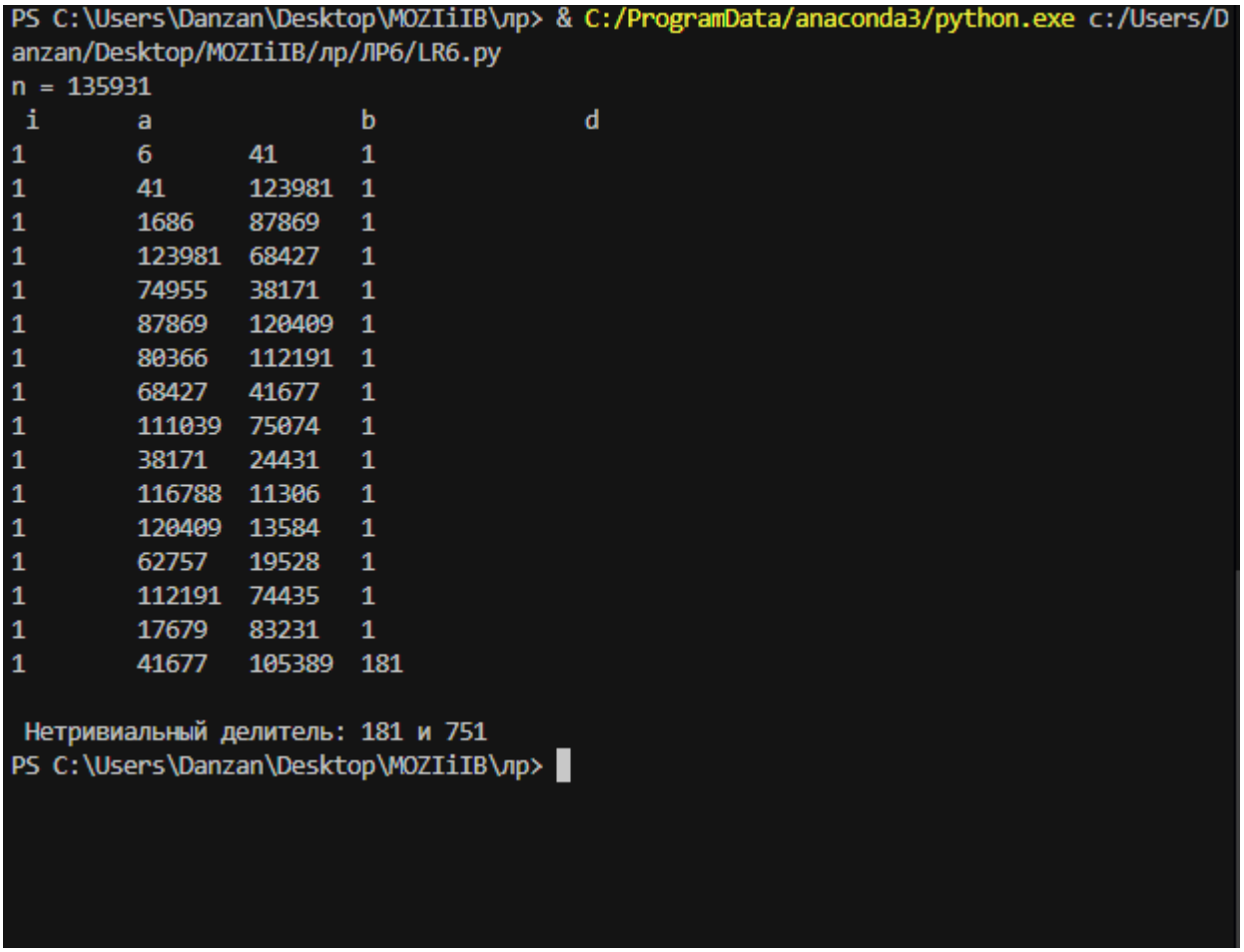
Процесс выполнения работы

Реализация метода Полларда по разложению чисел на множителя используя язык программирования python

```python
import math
def pollard(n: int):
    a = 1
    b = 1
    i = 1

    def f(x:int) -> int:
        return(x*x+5) % n
    print(" i\t a\t\t b\t\t d")

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

        print(f"{i}\t {a}\t {b}\t {d}")
        if i < d < n:
            print(f"\n Нетривиальный делитель: {d} и {n // d}")
            break
        if d == n:
            print(" Попытка найти делитель провалилась")
            break

if __name__ == "__main__":
    n_str = input("n = ").strip()
    n = int(n_str)
    pollard(n)
```

Результаты

- Успешно реализованы все задачи, поставленные для выполнения лабораторной работы



Вывод

Реализован p-метод Полларда по на языке программирования python по разложению чисел на множители