

# Разложение чисел на множители

## Лабораторная работа №6

---

Шутенко Виктория

17 сентября 2023

Российский университет дружбы народов, Москва, Россия

## Информация

---

- Шутенко Виктория михайловна
- студентка Магистратуры
- группы НФИмд-02-23
- Российский университет дружбы народов

## Задание лабораторной работы

---

1. Реализовать алгоритм, реализующий  $p$ -метод Полларда.

Реализация алгоритма,  
реализующего р-метод Полларда

---

# Реализация алгоритма, реализующего р-метод Полларда

```
import numpy as np

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

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

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')

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

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

## Результаты

---



Поллард 1359331

-----

a = 1, b = 1

iteration 1: a = 727, b = 659, d = 1

iteration 101: a = 221284, b = 1055655, d = 1

iteration 201: a = 738532, b = 474401, d = 1

iteration 301: a = 436715, b = 1356036, d = 1

iteration 378: a = 36811, b = 62133, d = 1151

Нетривиальный делитель 1359331: p = 1151

-----

Поллард 137

-----

a = 5, b = 5

iteration 1: a = 30, b = 33, d = 1

iteration 101: a = 12, b = 102, d = 1

iteration 201: a = 19, b = 70, d = 1

iteration 213: a = 68, b = 68, d = 137

Делитель не найден

-----

Поллард 322

-----

a = 12, b = 12

iteration 1: a = 149, b = 158, d = 1

iteration 6: a = 108, b = 258, d = 2

Нетривиальный делитель 322: p = 2

-----

## Выводы

---

1. Реализован алгоритм, реализующий  $p$ -метод Полларда.