Лабораторная работа №6

Разложение чисел на множители

Доборщук В.В.

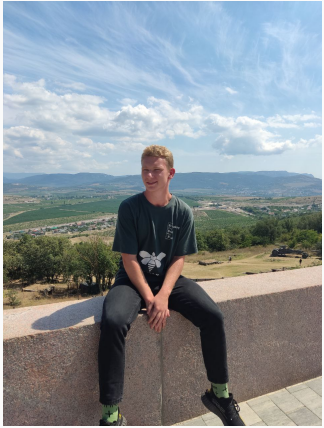
26 ноября 2022

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Доборщук Владимир Владимирович
- студент группы НФИмд-02-22, студ. билет 1132223451
- учебный ассистент кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- doborshchuk-vv@rudn.ru



Цели и задачи

Цели и задачи

Цель — Изучить алгоритмы разложения чисел на множители.

Задачи:

- Реализовать алгоритм нахождения нетривиального сомножителя p-методом Полларда

Выполнение лабораторной работы

Выполнение лабораторной работы

```
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
```

Результаты тестирования

```
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
---------
```

Результаты тестирования

```
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
---------
```

Выводы

Выводы

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