Лабораторная работа №6

Разложение чисел на множители. Метод Полларда

- 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

Объект и предмет исследования

- Объект исследования - Алгоритмы разложения чисел на множители
- Предмет исследования - p-метод Полларда, факторизация больших чисел, псевдослучайные последовательности

Цели и задачи

- Цель работы: Программная реализация p-метода Полларда на языке программирования python
- Задачи: реализовать программно алгоритм разложения чисел на множители
- продемонстрировать работу алгоритма

Теоретическая часть

Метод полларда - вероятностный алгоритм для нахождения нетривиальных делителей. Основан на поиске циклов в псевдослучайных последовательностях. Использует “черепаху” и “зайца” для обнаружения делителей

Процесс выполнения работы

Реализация метода Полларда по разложению чисел на множители используя язык программирования 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)
```

Результат работы программы с заданным n = 135931

```
n = 135931
 i       a               b               d
1        6       41      1
1        41      123981  1
1        1686    87869   1
1        123981  68427   1
1        74955   38171   1
1        87869   120409  1
1        80366   112191  1
1        68427   41677   1
1        111039  75074   1
1        38171   24431   1
1        116788  11306   1
1        120409  13584   1
1        62757   19528   1
1        112191  74435   1
1        17679   83231   1
1        41677   105389  181

 Нетривиальный делитель: 181 и 751
```

Вывод

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