

Презентация лабораторной работы 5. Вероятностные алгоритмы проверки чисел на простоту

Ильин Никита Евгеньевич

Цель выполнения лабораторной работы

Цель данной работы - научиться реализовывать алгоритмы проверки чисел на простоту.

Выполнение лабораторной работы

1. Реализуется функция алгоритма теста Ферма. (рис. (fig:001?)).

```
1 def test_ferma(a, n):
2     r = (a ** (n-1))%n
3     if r == 1:
4         print('Число n=', n, 'вероятно, простое')
5     else:
6         print('Число n=', n, 'составное')
```

✓ 0.0s

```
1 test_ferma(12, 17)
```

✓ 0.0s

Число n= 17 вероятно, простое

Figure 1: Программная реализация алгоритма теста Ферма.

Выполнение лабораторной работы

2. Реализуется функция алгоритма вычисления символа Якоби. (рис. (fig:002?)).

```
1
2 def Jakobi_symbol(a, n):
3     g = 1
4     while True:
5         if a == 0:
6             res = 0
7             break
8         if a == 1:
9             res = g
10            break
11        else:
12            k = primefactors(a)[0]
13            a1 = primefactors(a)[1]
14            if k % 2 == 0:
15                s = 1
16            if k % 2 != 0:
17                if ((n - 1) % 8) == 0 or ((n + 1) % 8) == 0:
18                    s = 1
19                if ((n - 3) % 8) == 0 or ((n + 3) % 8) == 0:
20                    s = -1
21            if a1 == 1:
22                res = g * s
23                break
24
25            if ((n - 3) % 4) == 0 or ((a1 - 3) % 4) == 0:
26                s = -s
```

Выполнение лабораторной работы

3. Программная реализация алгоритма Соловэй-Штрассена. (рис. (fig:003?)).

```
1 def solovey_strassen(a, n):
2     r = (a ** ((n - 1) / 2)) % n
3     if r != 1 and r != n - 1:
4         print('Число n=', n, 'составное')
5     s = Jakobi_symbol(a, n)
6     if (r - s) % n != 0:
7         print('Число n=', n, 'составное')
8     else:
9         print('Число n=', n, 'вероятно, простое')
10
```

6] ✓ 0.0s

```
1 solovey_strassen(12, 17)
```

7] ✓ 0.0s

Число n= 17 вероятно, простое

Выполнение

лабораторной работы

Выводы

В ходе работы были реализованы алгоритмы проверки чисел на простоту.