Презентация лабораторной работы 5. Вероятностные алгоритмы проверки чисел на простоту

Бармина Ольга

Цель выполнения лабораторной работы

Цель выполнения лабораторной работы

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

Выполнение лабораторной работы

1. Реализуется функция алгоритма теста Ферма

```
a = 29
b = 49
```

```
def ferm(a, n):
    r = (a**(n-1))%n
    if r == 1:
        return 'probably, prime'
    else:
        return 'not prime'
```

```
ferm(8,a)
```

```
'probably, prime'
```

```
ferm(8,b)
```

```
'not prime'
```

Figure 1: Программная реализация алгоритма теста Ферма.

Выполнение лабораторной работы

2. Реализуется функция алгоритма вычисления символа Якоби

```
from sympy import primefactors

def jacobi(a, n):
    g = 1
    while True:
        if a == 0:
            return 0
        elif a == 1:
            return g
        else:
            k = primefactors(a)[0]
            if len(primefactors(a)) == 1:
                a1 = a
            else:
                a1 = primefactors(a)[1]
            if k%2 == 1:
                if (n-1)%8 == 0 or (n+1)%8 == 0:
                    s = 1
                if (n-3)%8 == 0 or (n+3)%8 == 0:
                    s = -1
            else:
                s = 1
            if a1 == 1:
                return g*s
            if (n-3)%4 == 0 or (a1-3)%4 == 0:
                s = -s
            a = n%a1
            n = a1
            g = g*s
```

```
jacobi(8, a)
```

```
-1
```

```
jacobi(8, b)
```

```
1
```


Figure 2: Алгоритм вычисления символа Якоби

3. Программная реализация алгоритма Соловэй-Штрассена

```
def sol_st(a, n):
    r = (a**((n-1)/2))%n
    if r != 1 and r != n-1:
        return 'not prime'
    s = jacobi(a, n)
    if (r-s)%n != 0:
        return 'not prime'
    else:
        return 'probably prime'
```

```
sol_st(8, a)
```

```
'probably prime'
```

```
sol_st(8, b)
```

```
'not prime'
```

Figure 3: Программная реализация алгоритма Соловэй-Штрассена

Выполнение лабораторной работы

4. Программная реализация алгоритма Миллера-Рабина

```python
def mil_rab(a, n):
    s = primefactors(n-1)[0]
    if len(primefactors(n-1)) == 1:
        r = n-1
    else:
        r = primefactors(n-1)[1]
    y = (a**r)%n
    if y != 1 and y != n-1:
        j = 1
        while j <= s-1 and y != n-1:
            y = (y**2)%n
            if y == 1:
                return 'not prime'
            j += 1
        if y != n-1:
            return 'not prime'
    return 'probably prime'
```

```python
mil_rab(8, a)
```

```
'probably prime'
```

```python
mil_rab(8, b)
```

```
'not prime'
```

Figure 4: Алгоритм Миллера-Рабина.

Выводы

Выводы

В ходе работы были реализованы алгоритмы проверки чисел на простоту.