

Отчёт по лабораторной работе №5

Вероятностные алгоритмы проверки чисел на простоту

Шутенко Виктория Михайловна

Содержание

1	Цель работы	4
2	Ход работы	5
2.1	Реализация теста Ферма	5
2.2	Реализация символа Якоби	5
2.3	Реализация теста Соловья-Штрассена	7
2.4	Реализация теста Миллера-Рабина	8
2.5	Тестирование	9

Список иллюстраций

2.1	Тестирование	10
2.2	Тестирование	11

1 Цель работы

Приобрести практические навыки работы с вероятностными алгоритмами проверки чисел на простоту.

2 Ход работы

2.1 Реализация теста Ферма

```
def fermats(n: int):  
    if n < 5:  
        print("N should be greater or equal to 5")  
        return  
  
    a = np.random.choice(range(2, n-1))  
  
    if (a**(n-1)) % n == 1:  
        return "Число " + str(n) + ", вероятно, простое"  
    else:  
        return "Число " + str(n) + " составное"
```

2.2 Реализация символа Якоби

```
def yakobi(n: int, a: int):  
    if n < 3:  
        print("Число n должно быть больше или равно 3")  
        return None  
  
    if a < 0 or a >= n:
```

```
print("Число a должны быть на интервале [0;n)")  
return None
```

```
g = 1
```

```
while a != 0 and a != 1:
```

```
    k = 0
```

```
    a_1 = a
```

```
    while divmod(a_1, 2)[1] != 1:
```

```
        a_1 = divmod(a_1, 2)[0]
```

```
    while (2**k)*a_1 != a:
```

```
        k += 1
```

```
s = 1
```

```
if k % 2 == 0:
```

```
    s = 1
```

```
else:
```

```
    if (n == 1 % 8) or (n == -1 % 8):
```

```
        s = 1
```

```
    elif (n == 3 % 8) or (n == -3 % 8):
```

```
        s = -1
```

```
if a_1 == 1:
```

```
    return g * s
```

```
if (n == 3 % 4) and (a_1 == 3 % 4):
```

```
    s = -s
```

```

a = n % a_1
n = a_1
g = g * s

if a == 0:
    return 0
else:
    return g

```

2.3 Реализация теста Соловья-Штрассена

```

def soloway_shtrassen(n: int):
    if n % 2 == 0 or n < 5:
        return "Число " + str(n) + " составное"

    a = np.random.randint(2, n-1)
    r = int((a**((n-1)/2)) % n)

    if r != 1 and r != (n - 1):
        return "Число " + str(n) + " составное"

    s = yakobi(n, a)
    if r == s % n:
        return "Число " + str(n) + " составное"
    else:
        return "Число " + str(n) + ", вероятно, простое"

```

2.4 Реализация теста Миллера-Рабина

```
def miller_rabin(n: int):  
    if n % 2 == 0 or n < 5:  
        return "Число " + str(n) + " составное"  
  
    r = n - 1  
    s = 0  
  
    while divmod(r, 2)[1] != 1:  
        r = divmod(r, 2)[0]  
        s += 1  
  
    a = np.random.randint(2, n-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 "Число " + str(n) + " составное"  
            j = j + 1  
        if y != n - 1:  
            return "Число " + str(n) + " составное"  
  
    return "Число " + str(n) + ", вероятно, простое"
```


2.5 Тестирование

```
def main():  
    n = [7, 11, 13, 17, 19, 23, 27, 29, 31, 33, 35]  
  
    for n_i in n:  
        print(f'\n----ЧИСЛО-{n_i}----\n')  
        print(f'Тест Ферма: {fermats(n_i)}')  
        print(f'Тест Соловья-Штрассена: {soloway_shtrassen(n_i)}')  
        print(f'Тест Миллера-Рабина: {miller_rabin(n_i)}')
```

----ЧИСЛО-7----

Тест Ферма: Число 7, вероятно, простое

Тест Соловья-Штрассена: Число 7, вероятно, простое

Тест Миллера-Рабина: Число 7, вероятно, простое

----ЧИСЛО-11----

Тест Ферма: Число 11, вероятно, простое

Тест Соловья-Штрассена: Число 11 составное

Тест Миллера-Рабина: Число 11, вероятно, простое

----ЧИСЛО-13----

Тест Ферма: Число 13, вероятно, простое

Тест Соловья-Штрассена: Число 13, вероятно, простое

Тест Миллера-Рабина: Число 13, вероятно, простое

----ЧИСЛО-17----

Тест Ферма: Число 17, вероятно, простое

Тест Соловья-Штрассена: Число 17 составное

Тест Миллера-Рабина: Число 17, вероятно, простое

----ЧИСЛО-19----

Тест Ферма: Число 19 составное

Тест Соловья-Штрассена: Число 19 составное

Тест Миллера-Рабина: Число 19, вероятно, простое

Рис. 2.1: Тестирование

----ЧИСЛО-23----

Тест Ферма: Число 23, вероятно, простое
Тест Соловья-Штрассена: Число 23 составное
Тест Миллера-Рабина: Число 23, вероятно, простое

----ЧИСЛО-27----

Тест Ферма: Число 27 составное
Тест Соловья-Штрассена: Число 27 составное
Тест Миллера-Рабина: Число 27 составное

----ЧИСЛО-29----

Тест Ферма: Число 29 составное
Тест Соловья-Штрассена: Число 29 составное
Тест Миллера-Рабина: Число 29, вероятно, простое

----ЧИСЛО-31----

Тест Ферма: Число 31 составное
Тест Соловья-Штрассена: Число 31 составное
Тест Миллера-Рабина: Число 31, вероятно, простое

----ЧИСЛО-33----

Тест Ферма: Число 33 составное
Тест Соловья-Штрассена: Число 33 составное
Тест Миллера-Рабина: Число 33 составное

----ЧИСЛО-35----

Тест Ферма: Число 35 составное
Тест Соловья-Штрассена: Число 35 составное
Тест Миллера-Рабина: Число 35 составное

Рис. 2.2: Тестирование