Информационная безопасность. Отчет по лабораторной работе № 5

Вероятностные алгоритмы проверки чисел на простоту

Мухамеджанов Исматулло Иззатуллоевич

Содержание

List of Figures

List of Tables

1 Цель работы

Освоить на практике применение вероятностные алгоритмы проверки чисел на простоту

2 Указание к работе

Тест Ферма Символ Якоби Тест Соловея-Штрассена Тест Миллера-Рибена # Выполнение лабораторной работы 1. Тест Ферма Вход. Нечетное целое число n >= 5. Выход. «Число n, вероятно, простое» или «Число n составное».

Выбрать случайное целое число a, 2 <= a <= n — 2. Вычислить r = a ^ n-1 (mod n). При r = 1 результат: «Число n, вероятно, простое». В противном случае результат: «Число n составное».

2. Алгоритм вычисления символа Якоби. Положить g +- 1.

   При п = 0 результат: 0. При п = 1 результат: g. Представить п в виде о 2'n , где число о нечетное. При четном k положить s ‹= 1, при нечетном k положить s +- 1, если n - 1 (mod 8); положить s —1, если п п -33 (mod 8). При m = 1 результат: ф- s. Если п ж 3 (mod 4) и о ж 3 (mod 4), то s +- —s. Положить п +— п (mod m), п +- a , g +- g- s и вернуться на шаг 2.

3. Алгоритм реализующий тест Соловея-Штрассена Вход. Нечетное целое число п й 5. Выход. «Число п, вероятно, простое» или «Число п составное».

   Выбрать случайное целое число п, 2 N п < п — 2. ВычислиТЬ г с- д 2 (mod п). При г Т 1 и г Т п — 1 результат: «Число п составное». Вычислить символ Якоби s +- ( ). При г ж s {mod п) резулътат: «Число п составное». В противном случае результат: «Число п, вероятно, простое». На сегодняшний день для проверки чисел на простоту чаще всего используется тест Миллера-Рабина, основанный на следующем наблюдении. Пусть число п нечетное и

п — 1 — 2Sr, где г — нечетное. Если п простое, то для любого п й 2, взаимно простого с п, выполняется условие п*** 1 {mod p).

4. Алгоритм реализующий тест Миллера-Рабина. Вход. Нечетное целое число п й 5. Выход. «Число n, вероятно, простое» или «Число n составное».

Представить n — 1 в виде n — 1 = 2’r, где число г нечетное. Выбрать случайное целое число п, 2 й п < п — 2.

Вычислить у +- a^(mod п). При у У 1 и у Т п — 1 вьшолнить следующие действия. Положить J +- 1. Если J й s - 1 и у Т п — 1, то Положить у ‹= у2 (mod п). При у = 1 результат: «Число п составное». Положить J +- J -1- 1. При у Т п — 1 результат: «Число п составное». Результат: «Число п, вероятно, простое».

Тест Ферма

```
import random
import math

def test_ferm(n):
    if n == 1:
        return "Number is prime"
    number = random.randint(2,  n - 2)
    r = math.pow(number, n - 1) % n
    if r == 1:
        return "Number is prime"
    return "Number is not prime"

test_ferm(9)
```

[4] Python

... 'Number is not prime'

Figure 2.1: Программа (1)

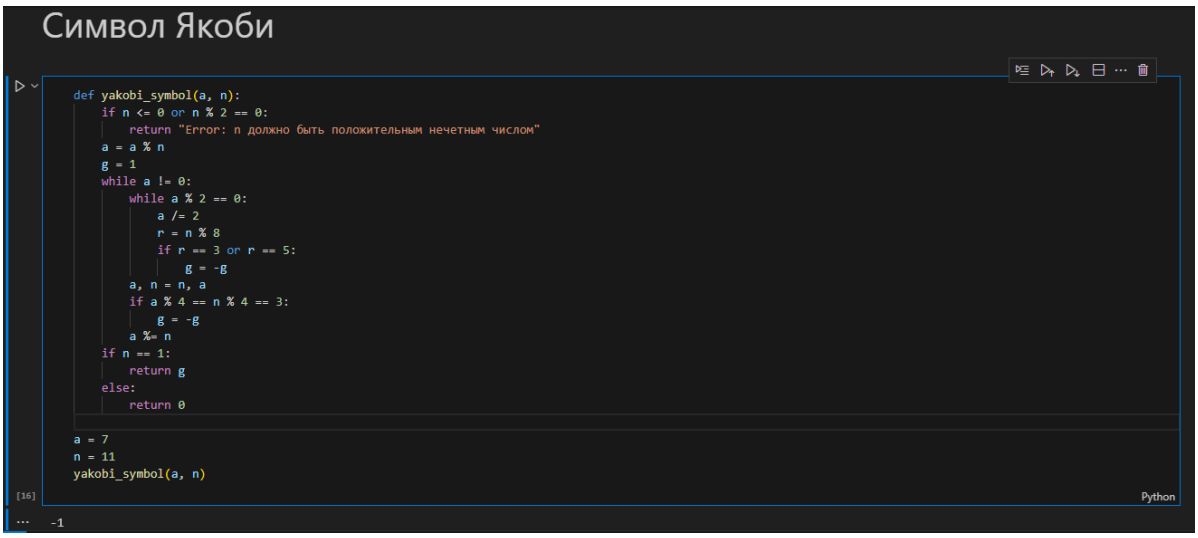

Figure 2.2: Программа (2)

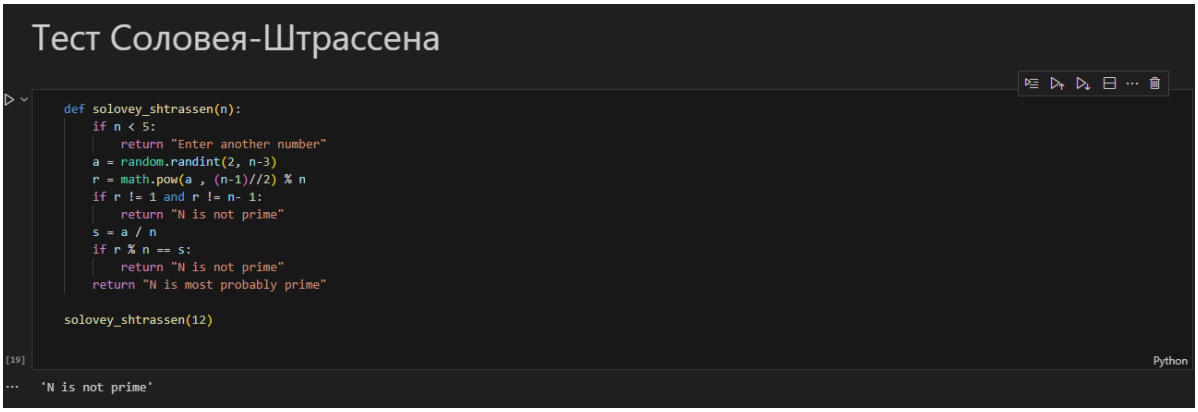

Figure 2.3: Программа (3)

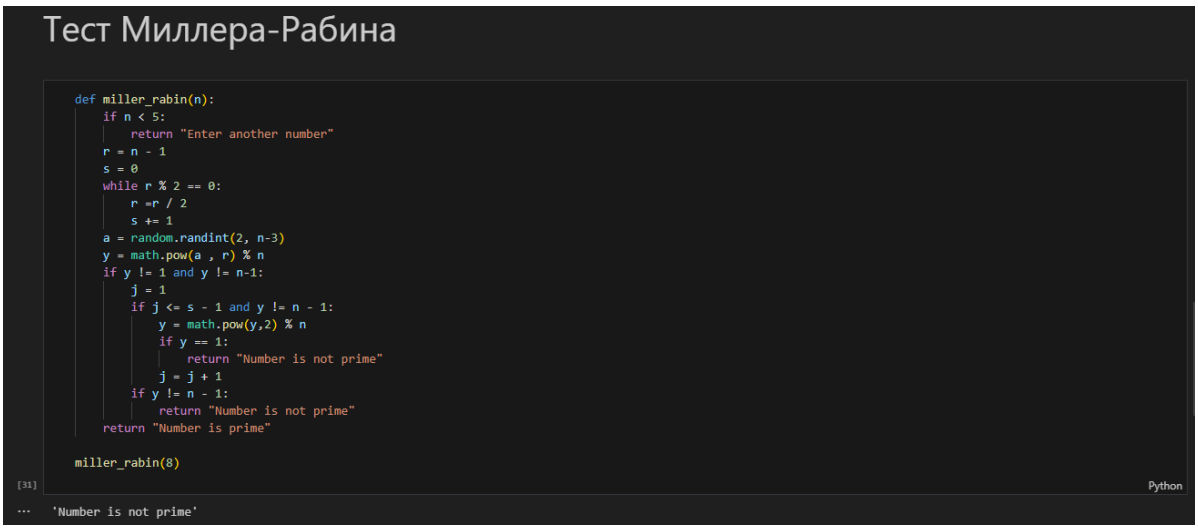

Figure 2.4: Программа (4)

3 Выводы

Освоены алгоритмы проверки чисел на простоту

4 Список литературы

1. Методические материалы курса