Лабораторная работа №5

Математические основы защиты информации и информационной безопасности

Полиенко Анастасия Николаевна

25 октября 2023

Российский университет дружбы народов, Москва, Россия

НПМмд-02-23

Вероятностные алгоритмы проверки чисел на простоту

Цель лабораторной работы

Изучить вероятностные алгоритмы проверки чисел на простоту

Задачи лабораторной работы

Реализовать алгоритм Евклида в четырёх его вариациях:

Реализовать четыре теста на определение простоты чисел:

1. Тест Ферма
2. Символ Якоби
3. Тест Соловэя-Штрассена
4. Тест Миллера-Рабина

Ход лабораторной работы

Тест Ферма

```
n = int(input()) #>5
a = np.random.randint(2, n-2)
r = a ** (n - 1) % n
if r == 1:
    print("число n. вероятно, простое")
else:
    print("число n составное")
```

Рис. 1: Код

Символ Якоби

```
def ka(a):
    k = 0
    while a % 2 == 0:
        k += 1
        a /= 2
    return k, a

def jacobi(n, a):
    g = 1
    while True:
        if a == 0:
            return 0
        if a == 1:
            return g
        k, a_1 = ka(a)
        if k % 2 == 0:
            s = 1
        else:
            if n % 8 == 1 or n % 8 == -1:
                s = 1
            elif n % 8 == 3 or n % 8 == -3:
                s = -1
        if a_1 == 1:
            return g * s
        if n % 4 == 3 and a_1 % 4 == 3:
            s = -s
        a = n % a_1
        n = a_1
        g = g * s

n = int(input()) #>3 нечётное
a = int(input()) #0<a<n
jacobi(n, a)
```

Тест Соловэя-Штрассена

```
n = int(input()) #>=5 нечётное
a = np.random.randint(2, n-2)
r = a ** ((n - 1)/2) % n
if r != 1 and r != (n-1):
    print("Число n составное")
else:
    s = jacobi(n, a)
    if r % n == s:
        print("число n составное")
    else:
        print("число n, вероятно, простое")
```

Рис. 3: Код

Тест Миллера-Рабина

```
n = int(input()) #>=5 нечётное
s, r = ka(n - 1)
a = np.random.randint(2, n-2)
y = a ** r % n
flag = False
if y != 1 and y != (n - 1):
    j = 1
    while j <= (s - 1) and y != (n - 1):
        y = y ** 2 % n
        if y == 1:
            flag = True
        j += 1
    if y != (n - 1):
        flag = True
if flag:
    print("Число n составное")
else:
    print("Число n, вероятно, простое")
```

Выводы

Изучила вероятностные алгоритмы проверки чисел на простоту.