Математические основы защиты информации и информационной безопасности

Колчева Юлия Вячеславовна

9 Ноября 2024

РУДН, Москва, Россия

Лабораторная работа 5

Тест Ферма

In [16]:

```
using Random
num = 20
k = 10

function Ferma(n, k)
    for i in 1:k
        a = rand(1:n-1)
        if (a^(n - 1) % n != 1)
            return "Число составное"
        end
    end
    return "Число простое"
end

println(Ferma(num, k))
```

```
Число составное
```

Рис. 1: Реализация программы

Символ Якоби

In [14]:

```
function jacobi(a, n)
    if !(n > a > 0 && n % 2 == 1)
        return 0
    end
    s = 1
    while a != 0
        while a % 2 == 0
            a /= 2
        end
        k = n % 8
        if k == 3 || k == 5
            s = -s
        end
        a, n = n, a
        if a % 4 == 3 && n % 4 == 3
            s = -s
        end
        a %= n
    end
    if n == 1
        return s
    else
        return 0
    end
end
println("Символ Якоби ", jacobi(7, 33))
```

```
Символ Якоби -1
```

Рис. 2: Реализация программы

Тест Соловэя-Штрассена

In [4]:

```
using Random

function S_Sh(n, k)
    for i in 1:k
        a = rand(2:(n - 3))
        r = a^((n - 1) ÷ 2) % n
        if r != 1 && r != n - 1
            return "Число составное"
        end
        s = jacobi(n, a)
        if r == s % n
            return "Число составное"
        end
    end
    return "Число простое"
end

println(S_Sh(num, k))
```

```
Число составное
```

Рис. 3: Реализация программы

Тест Миллера-Рабина

```
3  function miller_rabin(n, k)
4      if n == 2
5          return "Число простое"
6      end
7      if n % 2 == 0
8          return "Число составное"
9      end
10     r, s = 0, n - 1
11     while s % 2 == 0
12         r += 1
13         s ÷= 2
14     end
15     for _ in 1:k
16         a = rand(2:(n - 1))
17         x = powermod(a, s, n)
18         if x == 1 || x == n - 1
19             continue
20         end
21         for _ in 1:(r - 1)
22             x = powermod(x, 2, n)
23             if x == n - 1
24                 break
25             else
26             return "Число составное"
27             end
28         end
29     end
```

Рис. 4: Реализация программы

Выводы всех программ

In [17]:

```
1 println(Ferma(num, k))
2 println("Символ Якоби ", jacobi(7, 33))
3 println(S_Sh(num, k))
4 println(miller_rabin(num, k))
```

```
Число составное
Символ Якоби -1
Число составное
Число составное
```

Рис. 5: Вывод программ

Выводы

- Познакомилась с вероятностными алгоритмами проверки чисел на простоту
- Реализовала алгоритмы на практике.

Спасибо за внимание!