Презентация по лабораторной работе №5

Вероятностные алгоритмы проверки чисел на чистоту

Саргсян А. Г.

05 ноября 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель: Изучить алгоритмы проверки числа на простоту

Задачи:

- Реализовать алгоритм теста Ферма;
- Реализовать алгоритм теста Соловэя-Штрассена;
- Реализовать алгоритм теста Миллера-Рабина.

Теста Ферма

```
: using Random

function fermat_test(n::Int)
    # Проверка на условие входа
    if n < 5 || n % 2 == 0
        return "Входное число должно быть нечётным и больше или равно 5"
    end

    # Шаг 1: Выбрать случайное целое число a, 2 ≤ a ≤ n - 2
    a = rand(2:n-2)

    # Шаг 2: Вычислить r = a^(n-1) % n
    r = powermod(a, n-1, n)  # эффективное возведение в степень по модулю

    # Шаг 3: Проверка результата
    if r == 1
        return "Число n, вероятно, простое"
    else
        return "Число n составное"
    end
end
n=7
println(n,": ",fermat_test(n))
n=9
println(n,": ",fermat_test(n))
```

```
7: Число n, вероятно, простое
9: Число n составное
```

Рис. 1: Тест Ферма

Алгоритм теста Соловэя-Штрассена

```
jacobi (generic function with 1 method)
```

```julia
# Тест Соловэя-Штрассена
function solovay_strassen_test(n::Int, k::Int)
    if n < 2
        return false
    elseif n == 2
        return true
    elseif n % 2 == 0
        return false
    end

    for _ in 1:k
        a = rand(2:n-2)  # Случайное число в диапазоне [2, n-2]
        x = jacobi(a, n)
        if x == 0 || powermod(a, (n-1) ÷ 2, n) != (x % n + n) % n
            return "Число n составное"
        end
    end

    return "Число n, вероятно, простое"
end

n = 61  # Число для проверки
k = 5   # Количество итераций
println(n, ":", solovay_strassen_test(n, k))
```

```
61:Число n, вероятно, простое
```

Рис. 2: Тест Соловэя-Штрассена

Алгоритм теста Миллера-Рабина

```julia
function miller_rabin_test(n::Int, k::Int)

    if n < 2
        return false
    elseif n == 2
        return true
    elseif n % 2 == 0
        return false
    end

    # Представить n - 1 в виде 2^s * d, где d нечетно
    d = n - 1
    s = 0
    while d % 2 == 0
        d ÷= 2
        s += 1
    end

    # Повторить тест k раз для повышения надежности
    for _ in 1:k
        a = rand(2:n-2)  # Случайное число a в диапазоне [2, n-2]
        x = powermod(a, d, n)  # a^d % n

        if x == 1 || x == n - 1
            continue  # Продолжить, если x == 1 или x == n - 1
        end

        composite = true
        for _ in 1:(s - 1)
            x = powermod(x, 2, n)  # x = x^2 % n
            if x == n - 1
                composite = false
                break
            end
        end

        if composite
            return "Число n составное"
        end
    end

    return "Число n, вероятно, простое"
end

n = 61
k = 5
println(n,":", miller_rabin_test(n, k))
```

```
61:Число n, вероятно, простое
```

Выводы

Я реализовал алгоритмы проверки числа на простоту.