Лабораторная работа №5

Морозова Ульяна

Российский университет дружбы народов, Москва, Россия

Цель работы

Целью работы является изучение алгоритмов проверки чисел на простоту и реализация их на языке Julia.

Тест Ферма

Тест Ферма — вероятностный тест для проверки простоты натурального числа n, основанный на малой теореме Ферма. Даёт ответ о составности числа либо его несоставности лишь с некоторой вероятностью.

```
function fermat_test(n, k=10)
    println("Тестируем число $n с k = $k")

    if n <= 1
        # println("$n не является простым (n <= 1)")
        return false
    elseif n == 2 || n == 3
        # println("$n является простым числом")
        return true
    elseif n % 2 == 0
        # println("$n составное (четное число)")
        return false
    end
```

Результат его работы

```
Тест Ферма для различных чисел:
================================================
Тестируем число 7 с k = 5
7: вероятно простое
Тестируем число 11 с k = 5
12: составное
Тестируем число 14 с k = 5
14: составное
Тестируем число 15 с k = 5
15: составное
Тестируем число 35 с k = 5
35: составное
Тестируем число 548 с k = 5
548: составное
```

Тест Соловея-Штрассена и символ Якоби

Тест Соловея — Штрассена — вероятностный тест простоты, открытый в 1970-х годах Робертом Мартином Соловеем совместно с Фолькером Штрассеном. Тест опирается на малую теорему Ферма и свойства символа Якоби.

Код

```
function jacobi_symbol(a, n)

    if n % 2 == 0 || n <= 0
        throw(ArgumentError("n должно быть нечетным положительным целым"))
    end

    # Приводим a по модулю n
    a = a % n
    result = 1

    while a != 0
        # Убираем множители 2
        while a % 2 == 0
            a ÷= 2
```

Результат его работы

```
Тест Соловея-Штрассена для различных чисел:
================================================
7: вероятно простое
11: вероятно простое
13: вероятно простое
17: вероятно простое
19: вероятно простое
9: составное
10: составное
12: составное
14: составное
15: составное
35: составное
548: составное
```

Тест Миллера-Рабина

Тест Миллера — Рабина на простоту — вероятностный полиномиальный тест, который позволяет эффективно определить, является ли данное число составным. Однако с его помощью строго доказать простоту числа нельзя.

Код

```
function miller_rabin_test(n, k=10)

    # Обработка особых случаев
    if n <= 1
        return false
    elseif n == 2 || n == 3
        return true
    elseif n % 2 == 0
        return false
    end

    # Представляем n-1 в виде d * 2^s
    d = n - 1
    s = 0
```

Результаты:

```
Тестирование простого алгоритма Миллера-Рабина
================================================
1009: простое
1013: простое
10007: простое
10009: простое
1001: составное
1027: составное
10005: составное
10011: составное
```

Выводы

Мы изучили работу алгоритмов, а также реализовали их на языке Julia.