

```

1 # Лабораторная работа №5
2 # Тема: Вероятностные алгоритмы проверки чисел на простоту
3 # Выполнила: Исламова Сания
4 # Группа: НПИМд-01-24
5
6 using Random
7
8 function jacobi_symbol(a, n)
9     a == 0 && return 0
10    a == 1 && return 1
11
12    # Шаг 1: Вынести степени 2
13    e = 0
14    a1 = a
15    while iseven(a1)
16        e += 1
17        a1 ÷= 2
18    end
19
20    # Шаг 2: Множитель для степени 2
21    s = 1
22    if e % 2 == 1
23        if n % 8 == 1 || n % 8 == 7
24            s = 1
25        elseif n % 8 == 3 || n % 8 == 5
26            s = -1
27        end
28    end
29
30    # Шаг 3: Квадратичный закон взаимности
31    if n % 4 == 3 && a1 % 4 == 3
32        s = -s
33    end
34
35    # Шаг 4: Рекурсия
36    n1 = n % a1
37    if a1 == 1
38        return s
39    else
40        return s * jacobi_symbol(n1, a1)
41    end
42 end
43
44 function fermat_test()
45     println("\n=== ТЕСТ ФЕРМА ===")
46     println("Введите число для проверки:")
47     n = parse{Int, readline()}
48     println("Введите количество тестов:")
49     k = parse{Int, readline()}
50
51     for i in 1:k
52         a = rand(2:(n-2))
53         if powermod(a, n-1, n) != 1
54             println("Число $n - СОСТАВНОЕ (тест $i с основанием $a)")
55             return
56         end
57     end
58     println("Число $n - ВЕРОЯТНО ПРОСТОЕ (пройдено $k тестов)")
59 end
60

```

```

61 function solovay_strassen_test()
62     println("\n=== ТЕСТ СОЛОВЕЯ-ШТРАССЕНА ===")
63     println("Введите число для проверки:")
64     n = parse(Int, readline())
65     println("Введите количество тестов:")
66     k = parse(Int, readline())
67
68     for i in 1:k
69         a = rand(2:(n-2))
70         r = powermod(a, (n-1)÷2, n)
71         s = jacobi_symbol(a, n)
72
73         if r != 1 && r != n-1
74             println("Число $n - СОСТАВНОЕ (тест $i с основанием $a)")
75             return
76         elseif r % n != s % n
77             println("Число $n - СОСТАВНОЕ (тест $i с основанием $a)")
78             return
79         end
80     end
81     println("Число $n - ВЕРОЯТНО ПРОСТОЕ (пройдено $k тестов)")
82 end
83
84 function miller_rabin_test()
85     println("\n=== ТЕСТ МИЛЛЕРА-РАБИНА ===")
86     println("Введите число для проверки:")
87     n = parse(Int, readline())
88     println("Введите количество тестов:")
89     k = parse(Int, readline())
90
91     s, d = 0, n-1
92     while iseven(d)
93         s += 1
94         d ÷= 2
95     end
96
97     for i in 1:k
98         a = rand(2:(n-2))
99         x = powermod(a, d, n)
100
101         if x != 1 && x != n-1
102             composite = true
103             for j in 1:s-1
104                 x = (x * x) % n
105                 if x == n-1
106                     composite = false
107                     break
108                 end
109             end
110             if composite
111                 println("Число $n - СОСТАВНОЕ (тест $i с основанием $a)")
112                 return
113             end
114         end
115     end
116     println("Число $n - ВЕРОЯТНО ПРОСТОЕ (пройдено $k тестов)")
117 end
118
119 function jacobi_calculation()
120     println("\n=== ВЫЧИСЛЕНИЕ СИМВОЛА ЯКОБИ ===")

```

```

121     println("Введите число a:")
122     a = parse(Int, readline())
123     println("Введите нечетное число  $n \geq 3$ :")
124     n = parse(Int, readline())
125
126     if n < 3 || iseven(n)
127         println("Ошибка: n должно быть нечетным числом  $\geq 3$ ")
128         return
129     end
130
131     result = jacobi_symbol(a, n)
132     println("Символ Якоби ( $a/n$ ) = $result")
133
134     # Дополнительная информация
135     if result == 1
136         println("Это означает, что a является квадратичным вычетом по модулю n")
137     elseif result == -1
138         println("Это означает, что a является квадратичным невычетом по модулю n")
139     else
140         println("Это означает, что a и n не взаимно просты")
141     end
142 end
143
144 function main()
145     while true
146         println("\n" * "="^50)
147         println("ВЫБЕРИТЕ АЛГОРИТМ:")
148         println("1 - Тест Ферма")
149         println("2 - Тест Соловья-Штрассена")
150         println("3 - Тест Миллера-Рабина")
151         println("4 - Вычисление символа Якоби")
152         println("0 - Выход из программы")
153         println("="^50)
154
155         print("Ваш выбор: ")
156         choice = parse(Int, readline())
157
158         if choice == 0
159             println("Выход из программы...")
160             break
161         elseif choice == 1
162             fermat_test()
163         elseif choice == 2
164             solovay_strassen_test()
165         elseif choice == 3
166             miller_rabin_test()
167         elseif choice == 4
168             jacobi_calculation()
169         else
170             println("Неверный выбор! Попробуйте снова.")
171         end
172
173         println("\nНажмите Enter для продолжения...")
174         readline()
175     end
176 end
177
178 main()
179
180

```

