Лабораторная работа №5

Вероятностные проверки чисел на простоту

Выполнила:

Манаева Варвара Евгеньевна, НФИмд-01-24, 1132249514

Для проверки будем использовать числа 441 (21^2) и 443 (простое)

1. Тест Ферма

In [1]:
```
function testFerma(n)
    if n < 5
        return "Incorrect input."
    end
    a = rand(2:n-2)
    r = powermod(a, n-1, n)
    if r == 1
        return "Число " * string(n) * ", вероятно, простое."
    else
        return "Число " * string(n) * " составное."
    end
end
```

Out[1]: testFerma (generic function with 1 method)

In [2]:
```
display(testFerma(441))
display(testFerma(443))
```

```
"Число 441 составное."
"Число 443, вероятно, простое."
```

2. Символ Якоби

In [3]:
```
function YacobySymbol(n, a)
    if n < 3 || a >= n || a < 0
        return "Incorrect input."
    end
    g = 1
    a1 = 0
    k = 0
    s = 0
    while a1 != 1
        if a == 0
            return 0
        elseif a == 1
            return 1
        end
        a1 = a
```

```
        k = 0
        while a1 % 2 == 0
            k += 1
            a1 = round(Int64, a1 / 2)
        end

        if k % 2 == 0 || (k % 2 == 1 && (n % 8 == 1 || n % 8 == 7))
            s = 1
        elseif k % 2 == 1 && (n % 8 == 3 || n % 8 == 5)
            s = -1
        end
        if a1 == 1
            return g*s
        end

        if n % 4 == 3 && a % 4 == 3
            s = -s
        end

        a = n % a1
        n = a1
        g *= s
    end
end
```

Out[3]: YacobySymbol (generic function with 1 method)

In [4]:
```
YacobySymbol(443, 359)
```

Out[4]: 1

3. Тест Соловэя-Штрассена

In [5]:
```
function testSoloveyaShtrassena(n)
    if n < 5
        return "Incorrect input."
    end
    a = rand(2:n-2)
    r = powermod(a, round(Int64, (n-1)/2), n)
    if r != 1 && r != n-1
        return "Число " * string(n) * " составное."
    else
        s = YacobySymbol(n, a)
        if r == s && r != NaN
            return "Число " * string(n) * " составное."
        end
        return "Число " * string(n) * ", вероятно, простое."
    end
end
```

Out[5]: testSoloveyaShtrassena (generic function with 1 method)

In [6]:
```
display(testSoloveyaShtrassena(4463429))
display(testSoloveyaShtrassena(443))
```

```
"Число 4463429 составное."
"Число 443, вероятно, простое."
```

4. Тест Миллера-Робина

In [7]:
```
function testMilleraRobina(n)
    if n < 5
        return "Incorrect input."
    end
    r = n-1
    s = 0
    while r % 2 == 0
        s += 1
        r = round(Int64, r / 2)
    end
    a = rand(2:n-2)
    y = powermod(a, r, n)
    if y != 1 && y != n-1
        j = 1
        while j < s-1 && y != n-1
            y = y^2 % n
            if y == 1
                "Число " * string(n) * " составное."
            end
            j += 1
        end
        if y != n-1
            "Число " * string(n) * " составное."
        else
            "Число " * string(n) * ", вероятно, простое."
        end
    else
        return "Число " * string(n) * ", вероятно, простое."
    end
end
```

Out[7]:
```
testMilleraRobina (generic function with 1 method)
```

In [8]:
```
display(testMilleraRobina(4463429))
display(testMilleraRobina(443))
```

```
"Число 4463429 составное."
"Число 443, вероятно, простое."
```