Лабораторная работа №5

Вероятностные алгоритмы проверки чисел на простоту

Кубасов В.Ю.

Вводная часть

Актуальность

- Быстрое определение простых чисел является ключевым фактором в информационной безопасности

Цели и задачи

Реализовать алгоритмы:

- тест Ферма - символ якоби - тест Соловэя-Штрассена - тест Миллера-Рабина

Выполнение работы

Тест Ферма

```
println("Введите n");
n = parse(Int, chomp(readline()));

a = rand(2:n-2);

r = a ^ (n - 1) % n;
if (r == 1)
    println("Число, вероятно, простое");
else
    println("Число составное");
end;
```

Символ Якоби

```
function jackobi(n, a, g = 1)
    if (a == 1)
        return 0;
    end;
    if (a == 1)
        return g;
    end;
    k = 0;
    a1 = a;
    while (a1 % 2 == 0)
        a1 /= 2;
        k += 1;
    end;
```

Символ Якоби

```
s = 0;
if ((k % 2 == 0) || (abs(n % 8) == 1))
    s = 1;
elseif (abs(n % 8) == 3)
    s = -1
end;

if (a1 == 1)
    return g * s;
end;

if ((n % 4 == 3) && (a1 % 4 == 3))
    s = -s;
end;
```

Бинарный алгоритм Евклида

```
println("Введите n");
n = parse(Int, chomp(readline()));
a = rand(2:n-2);
r = a ^ (n - 1) % 2;
if ((r != 1) && (r != n - 1))
    println("Число n составное");
else
    s = jackobi(n, a);
    if (r % n == s)
        println("Число n составное");
    else
        println("Число, вероятно, простое");
    end;
end;
```

Тест Миллера-Рабина

```
function miller()
    println("Введите n");
    n = parse(Int, chomp(readline()));
    n_1 = n - 1;
    s = 0;
    while (n_1 % 2 == 0)
        n_1 /= 2;
        s += 1;
    end;
    r = n_1;
    a = rand(2:n-2);
    y = a^r % n;
    j = 1;
end;
```

Тест Миллера-Рабина

```
while (y != 1 && y != n - 1)
        if ((j <= s - 1) && (y != n - 1))
            y = y ^ 2 % n;
            if (y == 1)
                println("Число n составное");
                return 0;
                break;
            end;
            j += 1;
        end;
        if (y != n - 1)
            println("Число n составное");
            return 0;
            break;
```

Выводы:

Выводы:

- В ходе лабораторной работы реализовали вероятностные алгоритмы определения числа на простоту