Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

Лабораторная работа №5

По дисциплине «КМЗИ»

Тема: «Тестирование чисел на простоту и построение больших простых чисел»

Выполнил:

Студент 2 курса

Группы ИИ-21(2)

Кирилович А. А.

Проверил:

Хацкевич M. В.

Брест 2023

Цель: освоить основные программные методы тестирования чисел на простоту.

Тест Соловея-Штрассена

Код программы:

#include <bits/stdc++.h>

typedef long long LL;

LL modulo(LL base, LL exponent, LL mod)

{

LL x = 1;

LL y = base;

while (exponent > 0)

{

if (exponent % 2 == 1) x = (x \* y) % mod;

y = (y \* y) % mod;

exponent = exponent / 2;

}

return x % mod;

}

int calculateJacobian(LL a, LL n)

{

if (!a) return 0;

int ans = 1;

if (a < 0)

{

a = -a;

if (n % 4 == 3) ans = -ans;

}

if (a == 1) return ans;

while (a)

{

if (a < 0)

{

a = -a;

if (n % 4 == 3) ans = -ans;

}

while (a % 2 == 0)

{

a = a / 2;

if (n % 8 == 3 || n % 8 == 5) ans = -ans;

}

std::swap(a, n);

if (a % 4 == 3 && n % 4 == 3) ans = -ans;

a = a % n;

if (a > n / 2) a = a - n;

}

if (n == 1) return ans;

return 0;

}

bool solovoyStrassen(LL p, int iterations)

{

if (p < 2) return false;

if (p != 2 && p % 2 == 0) return false;

for (int i = 0; i < iterations; i++)

{

LL a = rand() % (p - 1) + 1;

LL jacobian = (p + calculateJacobian(a, p)) % p;

LL mod = modulo(a, (p - 1) / 2, p);

if (!jacobian || mod != jacobian) return false;

}

return true;

}

int main(int argc, char\* argv[])

{

int iterations = atoi(argv[1]);

LL num1 = atoi(argv[2]);

if (solovoyStrassen(num1, iterations)) printf("%d is prime\n",num1);

else printf("%d is composite\n",num1);

}

Вывод программы: 

**Вывод:** освоил основные программные методы тестирования чисел на простоту.