

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего
образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ
компьютерной безопасности и
криптографии

Проверка чисел на простоту с помощью критерия Вильсона

ЛАБОРАТОРНАЯ РАБОТА

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Серебрякова Алексея Владимировича

Научный руководитель

доцент, к. п. н.

подпись, дата

А. С. Гераськин

Саратов 2022

Описание алгоритма

Теорема Вильсона — теорема [теории чисел](#), которая утверждает, что

Если p — простое число, то число $(p - 1)! + 1$ делится на p . Обратно: если $(p - 1)! + 1$ делится на p , то p — простое число.

Код программы

```
#include <bits/stdc++.h>
#include <iostream>

using namespace std;

int validated_input()
{
    int s = 0;
    while (!(cin >> s))
    {
        cin.clear();
        cin.ignore(numeric_limits<streamsize>::max(), '\n');
        printf("! Неверный ввод. Повторите ввод, начиная с первого неверного элемента.\n");
    }

    return s;
}

int factmod(int n, int p)
{
    printf("\nПроверка теоремы Вильсона для нашего случая:\n  %d! + 1 (mod %d)\n  ", n, p);
    int res = 1;
    while (n > 1)
    {
        res = (res * ((n / p) % 2 ? p - 1 : 1)) % p;
        for (int i = 2; i <= n % p; ++i)
            res = (res * i) % p;
        n /= p;
    }
    printf("(p-1)! (mod p) = %d! (mod %d)\n", res % p, p);

    return res % p;
}

void test(int p){

    (factmod(p - 1, p) + 1) % p == 0 ?
        printf("\nОтвет: p - простое число\n") :
        printf("\nОтвет: p - не простое число\n");

}

int main()
{
    setlocale(0, "");
    int p;

    printf("\nТеорема Вильсона: Число p простое, если (p-1)! делится на p. Обратное тоже верно.\n");
```

```

printf("\nВведите число p: ");
p = validated_input();

test(p);

return 0;
}

```

Пример запуска программы

● * Executing task: /bin/bash -c ./build/Debug/outDebug

Теорема Вильсона: Число p простое, если $(p-1)!$ делится на p . Обратное тоже верно.

Введите число p : 731

Проверка теоремы Вильсона для нашего случая:

$730! + 1 \pmod{731}$

$(p-1)! \pmod{p} = 0! \pmod{731}$

Ответ: p - не простое число

* Terminal will be reused by tasks, press any key to close it.

● * Executing task: /bin/bash -c ./build/Debug/outDebug

Теорема Вильсона: Число p простое, если $(p-1)!$ делится на p . Обратное тоже верно.

Введите число p : 32465431

Проверка теоремы Вильсона для нашего случая:

$32465430! + 1 \pmod{32465431}$

$(p-1)! \pmod{p} = 0! \pmod{32465431}$

Ответ: p - не простое число

* Terminal will be reused by tasks, press any key to close it.