

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

**Факторизация Ферма**

**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

Метод факторизации Ферма находит разложение числа на 2 сомножителя.

❑ Вход: Натуральное нечетное число  $n > 1$

❑ Выход: Натуральный делитель  $a$ .

1. Вычислить наименьшее целое число  $s$  такое, что  $s^2 \geq \sqrt{n}$ , т.е.  $s = \lceil \sqrt{n} \rceil$ .
2. Если  $s^2 = n$ , то  $a = s$  и завершить алгоритм.
3. Взять  $x = s$ ,  $l = x^2 - n$  и счетчик шагов  $k = 0$ .
4. Если  $l$  является полным квадратом, то вычислить  $y = \sqrt{l}$ ,  $a = x + y$  и закончить алгоритм.
5. Вычислить  $k = k + 1$ ,  $x = x + 1$ ,  $l = x^2 - n$ . Перейти к пункту 4.

Другой делитель числа  $n$  равно  $b = n/a$ .

## Код программы

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

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;
}

bool isSqr(int n)
{
    float f(sqrt(n));

    return f == int(f);
}

int fact(int n)
{
    int a, s(ceil(sqrt(n))), x(s), l(x * x - n), k(0), y;

    if (n % 2 == 0)
    {
        printf("\nЧисло %d четное.\n\n", n);
```

```

        return -1;
    }

    if (s * s == n)
    {
        a = s;
        return a;
    }

    while (true)
    {
        if (isSqr(l))
        {
            y = sqrt(l);
            a = x + y;
            return a;
        }
        k++;
        x++;
        l = x * x - n;
    }
}

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

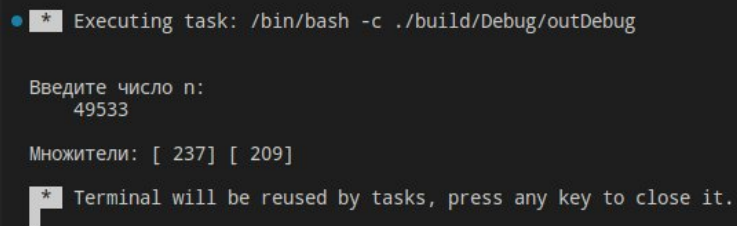
    printf("\nВведите число n:\n  ");
    n = validated_input();

    printf(fact(n) == -1 ?
        "\nПрекращение работы\n\n"
        : "\nМножители: [%4d] [%4d]\n\n", fact(n), n / fact(n));

    return 0;
}

```

## Пример запуска программы



```

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

Введите число n:
49533

Множители: [ 237] [ 209]

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

```