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

Алгоритм Диксона

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. _____ А. С. Гераськин

подпись, дата

Саратов 2022

Описание алгоритма

Алгоритм Диксона – алгоритм факторизации, использующий в своей основе идею Лежандра, заключающуюся в поиске пары целых чисел x и y таких, что $x^2 = y^2 \pmod n$ и x != +-y (mod n).

Метод Диксона является обобщением метода Ферма.

Код программы

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

using namespace std;

typedef vector<int> vect;
typedef vector<pair<int, int>> vect_pair;

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 gcd(int a, int b)
{
   return b == 0 ? a : gcd(b, a % b);
}

bool test(int x, int y, int n)
{
   return (x * x - y * y) % n == 0 && (x + y) % n != 0 && (x - y) % n != 0;
}

int dix(int n)
{
   vect base({2, 3, 5, 7});
   vect_pair result;
   int init(sqrt(n)), len(base.size()), left, right;

   for (int i = init; i < n; i++)
      for (int j = 0; j < len; j++)
      {
         left = (i * i) % n;
         right = (base[j] * base[j]) % n;

         if (left == right)
            result.push_back(make_pair(i, base[j]));
      }
```

```
    len = result.size();

    for (int i = 0; i < len; i++)
        if (test(result[i].first, result[i].second, n))
            if (result[i].first != 1)
            {
                return n / result[i].first;
                break;
            }
    return -1;
}

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

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

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

        return 0;
}
```

Пример запуска программы