Отчет по лабораторной работе 6

Дисциплина: Математические основы защиты информации и информационной безопасности

Подмогильный И. А.

25 ноября 2022

Российский университет дружбы народов, Москва, Россия

Прагматика выполнения лабораторной работы

Приобретение практических навыков разложения чисел на множители.

Цель выполнения лабораторной работы

Ознакомиться и реализовать программно алгоритм, реализующий p-метод Полларда.

Задачи выполнения лабораторной работы

Реализовать программно алгоритм, реализующий p-метод Полларда

```cpp
//
// Created by pi on 18.09.2022.
//

#ifndef LAB06_NUMBERDECOMPOSITIONHELPER_H
#define LAB06_NUMBERDECOMPOSITIONHELPER_H

#include <functional>
#include <GCDHelder.h>

class NumberDecompositionHelper {
    // cFunc - compressFunc
    // return -1 indicates the divider is not found
    static int pPollardMethod(const int& n, const int& c, std::function<int (int, int)>& cFunc){
        int res, a, b, d;
        a = c, b = c;
        while (true){
            a = cFunc(a, n);
            b = cFunc(b, n);
            GCDHelder::eucBinary(a - b, n, d);
            if (d > 1 && d < n){
                return d;
            }
            else if (d == n){
                return -1;
            }
        }


    }

private:
    static int compressFunc(int x, int modulo){
        return (x*x + 5) % modulo;
    }
};


#endif //LAB06_NUMBERDECOMPOSITIONHELPER_H
```

Задачи выполнения лабораторной работы

Написать функцию мэйн

```cpp
#include <iostream>
#include "src/NumberDecompositionHelper.h"
#include <GCDHelder.h>

using namespace std;

int main() {
    int a = NumberDecompositionHelper::pPollardMethod( n: 1359331,  c: 1);
    cout << a;
    return 0;
}
```

Figure 2: main

Разложить число на множители

```
/home/pi/education/pfur_masters/mat0snovyInfBez/labs/lab06/cmake-build-debug/main
1181
```

Результаты выполнения лабораторной работы

Результатом выполнения работы стала реализация алгоритма нахождения нетривиального делителя, что можно использовать для разложения числа на множители.