Отчет по лабораторной работе №6

Дисциплина: Математические основы защиты информации и информационной безопасности

Подмогильный Иван Александрович, НПМмд-02-22

Содержание

List of Figures

List of Tables

1 Цель работы

Ознакомится и реализовать алгоритм разложения чисел на множители.

2 Задание

Реализовать программно алгоритм, реализующий p-метод Полларда.

3 Выполнение лабораторной работы

3.1 Шаг 1

Ознакомился с предоставленными теоретическими данными.Написал функцию 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
```

Figure 3.1: Реализация алгоритма, реализующего p-метод Полларда

3.2 Шаг 2

Написал мэйн функцию

```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 3.2: main

3.3 Шаг 3

Нашёл нетривиальный делитель

```
/home/pi/education/pfur_masters/matOsnovyInfBez/labs/lab06/cmake-build-debug/main
1181
Process finished with exit code 0
```

Figure 3.3: Разложение на множители

4 Выводы

Ознакомился с алгоритмом, реализующем p-метод Полларда, и реализовал его программно.