Лабораторная работа №6

Разложение чисел на множители

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Койфман Кирилл Дмитриевич Группа: НФИмд-01-25

Цель работы Получение практических навыков реализации алгоритмов, выполняющих разложение чисел на множители.

Задачи

1. Реализовать алгоритм разложения чисел на множители, использующий p-метод Полларда.
2. Проверить работоспособность реализованного алгоритма.

---

1 задание

Для решения задачи данной работы была написана программа на C++, реализующая описанный в работе алгоритм:

```
namespace functions
{
    long long function_with_compression_behavior_1(long long x, long long
n){
        return static_cast<long long>(std::pow(x, 2) + 5) % n;
    }
}
using compressing_function_t = long long(*)(long long, long long);
long long algorithmEuclid(long long a, long long b);
int algorithmPollard(long long n, long long c = 1, compressing_function_t
function = functions::function_with_compression_behavior_1){
    long long a = c;
    long long b = c;
    long long d = 0;
    std::cout << "|a\tb\td|\n---------------------------------------\n";
    while (true)
    {
        a = function(a, n);
        b = function(b, n);
        b = function(b, n);
        d = algorithmEuclid(std::abs(a - b), n);
        std::cout << a << '\t' << b << '\t' << d << '\n';
        if (d > 1 && d < n)
            return d;
        else if (d == n)
            return -1;
        else if (d == 1)
```

```
            continue;
        }
    }
```

---

2 задание

Протестируем работу реализованного алгоритма:

```
int main()
{
    long long chosenValue = 1'359'331;
    long long result = algorithmPollard(chosenValue);
    std::cout << "Chosen value: " << chosenValue << '\n';
    if (result > 0)
    {
        std::cout << "\nDivider = " << result << std::endl;
        std::cout << "Result tests: \n[1]" << chosenValue << " / " <<
result << " = " << chosenValue / result
            << "\n[2]" << result << " * " << chosenValue / result << " = "
<< result * (chosenValue / result) << std::endl;
    }
    else
    {
        std::cout << "\nDivider was not found!" << std::endl;
    }
    return 0;
}
```

---

2 задание

```
|a      b       d|
---------------------------------------
6       41      1
41      123939  1
1686    391594  1
123939  438157  1
435426  582738  1
391594  1144026 1
1090062 885749  1181
Chosen value: 1359331

Divider = 1181
Result tests:
[1]1359331 / 1181 = 1151
[2]1181 * 1151 = 1359331
```

Спасибо за внимание!