Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**ЛАБОРАТОРНАЯ РАБОТА №1**

**Дисциплина: Криптографические протоколы**

Работу выполнил: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.А. Спиридонов

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

Преподаватель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А.А. Крамаренко

Лабораторная работа №1

**Задание №13**. Реализовать программный продукт решения сравнений первой степени двумя способами с указанием всех промежуточных шагов вычисления (текущее значение коэффициентов расширенном алгоритме Евклида и текущее значение степеней в формуле Эйлера), программный продукт так же должен реализовывать возможность того, что сравнение не имеет решений или имеет больше одного решения. В первом случае сообщать пользователю с пояснением, во втором строить все возможные решения.

Сравнения первой степени имеют вид ax + b = 0, где a и b — коэффициенты, а x — искомое значение.

**Расширенный алгоритм Евклида.**

Алгоритм позволяет находить не только наибольший общий делитель двух чисел, но и коэффициенты, обеспечивающие линейную комбинацию двух чисел. Описание алгоритма:

1. Проверить значения коэффициентов:

* Если a = 0 и b ≠ 0, то уравнение не имеет решений.
* Если a = 0 и b = 0, то уравнение имеет бесконечное множество решений.
* Если a ≠ 0, переходим к следующему шагу.

2. Применить расширенный алгоритм Евклида для нахождения НОД и коэффициентов x0 и y0​, таких что: ax + by = NOD(a,b)

3. Подсчитать текущее значение коэффициентов и их применение к уравнению. ​

4. Проверить найденное решение.

* Если решение существует (при a ≠0), то выводим решение. ​

5. В случае большого количества решений генерируем все возможные решения, если они имеются.

**Формула Эйлера.**

Формула Эйлера связана с решением линейных уравнений и применяется для поиска всех возможных целых решений уравнений, представленных в виде ax ≡ b (mod m).

1. Убедиться, что a и b взаимно просты (с помощью НОД).

2. Применить формулу Эйлера:

* Если ax ≡ b (mod m) имеет решения, то можно выразить все решения как: x = x0 + k ⋅ (m / d), где d = НОД(a, m).

3. Вывести все возможные значения x в рамках заданного диапазона.

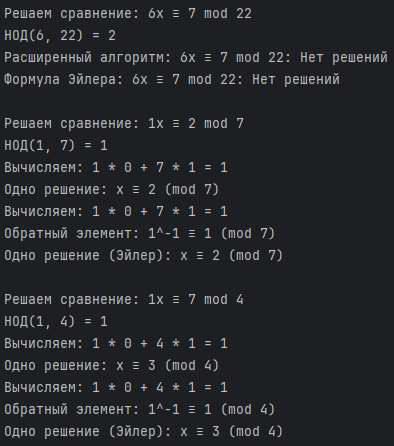


Рисунок 1 – Результат работы программы.