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 №2**

**Дисциплина: Криптографические протоколы**

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

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

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

Лабораторная работа №2

**Задание №13**. Реализовать программный продукт решения квадратичного сравнения с указанием промежуточных результатов. Программа должна показывать случаи, когда решения существуют, находить количество решений или указывать, что нахождение затруднительно.

**Квадратичные сравнения**

Квадратичное сравнение — это уравнение вида:

где a и m — целые числа, m > 1. Решением такого сравнения является целое число x, которое при возведении в квадрат дает остаток a при делении на m.

**Условия существования решений**

1. **Символ Лежандра.** Для простого модуля p символ Лежандра (a/p) определяется как:

mod p

Возможные значения:

• 1: решение существует.

• −1: решение не существует.

• 0: a делится на p.

1. **Критерий Эйлера.** Если p – нечетное простое число, то:

Это позволяет проверить, существует ли решение.

1. **Китайская теорема об остатках.** Если модуль m составной, то его можно разложить на простые множители m = p1^k1 p2^k2 … pn^kn. Решение квадратичного сравнения по модулю m сводится к решению системы сравнений: , для всех i.

**Алгоритм решения**

• Проверить, что a и m взаимно просты.

• Для простого модуля p:

Вычислить символ Лежандра.

Если символ Лежандра равен 11, найти решения перебором.

• Для составного модуля:

Разложить m на простые множители.

Решить сравнение для каждого простого множителя.

Объединить решения с помощью китайской теоремы об остатках.

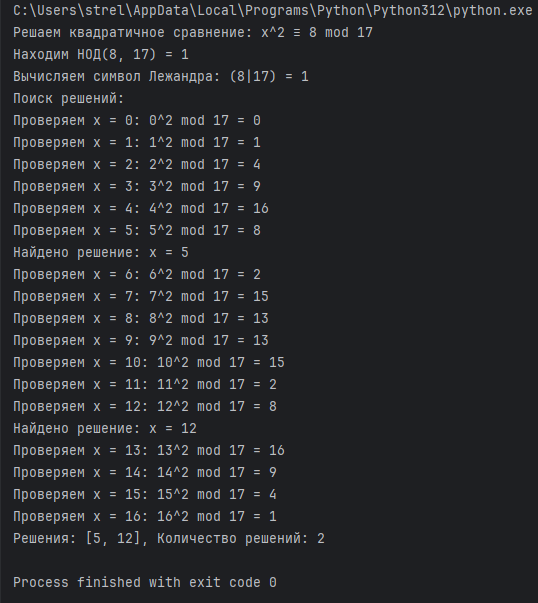
****

Рисунок 1 – Результат работы алгоритма