МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КУБГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчет**

**по практическому заданию №2**

**по курсу**

**«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»**

Работу выполнил

Студент 49 группы

Пинский Д. А.

Преподаватель:

Крамаренко А.А.

Краснодар 2025

**Цель работы:** Реализовать программный продукт нахождения множества квадратичных вычетов и множества квадратичных невычетов по заданному простому модулю с пояснением всех промежуточных шагов решения задачи.

**Теория:**

Квадратичные вычеты — числа a, для которых существует решение уравнения , где p – нечеткое простое число.

Критерий Эйлера:

Для простого p> 2 и целого a, не кратного p:

Количество вычетов и невычетов по модулю p всегда равно p-1/2.

**Ход работы;**

1. Проверяем число на простоту.
2. Вычисляем показатель степени p-1/2.
3. Применяем критерий Эйлера

Вычисляем

Определяем тип (вычет\не вычет).

1. Выводим результат

**Пример:**

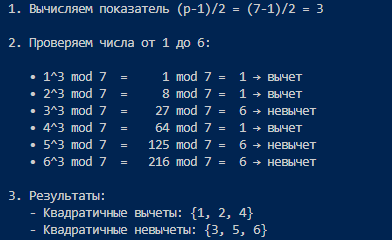


Рисунок 1 – пример работы программы

Листинг программы:

def task(p):

    """Находит и выводит квадратичные вычеты/невычеты с пояснениями"""

    if p <= 2 or not all(p % i != 0 for i in range(2, int(p\*\*0.5)+1)):

        print(f"Ошибка: {p} не является простым числом")

        return None, None

    print(f"Анализ квадратичных вычетов для простого модуля p = {p}\n")

    exponent = (p-1) // 2

    residues = set()

    non\_residues = set()

    print(f"1. Вычисляем показатель (p-1)/2 = ({p}-1)/2 = {exponent}\n")

    print(f"2. Проверяем числа от 1 до {p-1}:\n")

    for a in range(1, p):

        calculation = f"{a}^{exponent} mod {p}"

        power = a \*\* exponent

        mod\_result = power % p

        result\_type = "вычет" if mod\_result == 1 else "невычет"

        print(f" {calculation:10} = {str(power):>5} mod {p} = {mod\_result:2} {result\_type}")

        if mod\_result == 1:

            residues.add(a)

        else:

            non\_residues.add(a)

    print(f"\n3. Результаты:")

    print(f"   Квадратичные вычеты: {residues}")

    print(f"   Квадратичные невычеты: {non\_residues}")

    return residues, non\_residues

if \_\_name\_\_ == "\_\_main\_\_":

    a = int(input("Введите  a: "))

    task(a)