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 №3**

**по курсу**

**«КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ»**

Работу выполнил

Студенты 46 группы

Нагалевский А.М.

Преподаватель:

Крамаренко А.А.

Краснодар 2024

**Постановка задачи.**

Реализовать интерактивный калькулятор в поле Галуа с заданным пользователем образующим многочленом (сложение, умножение, деление, НОД, возведение в степень и таблица умножения).

Сначала разберемся что из себя представляет поле Галуа.

Поле Галуа (или конечное поле) — это математическая структура, которая состоит из конечного набора элементов, обладающих свойствами поля: сложение, вычитание, умножение и деление (за исключением деления на ноль). Поле Галуа обычно обозначается как GF(q), где q - простое число, которое называется порядком поля.

Ключевой аспект полей Галуа заключается в том, что они имеют конечное количество элементов. Это означает, что арифметические операции в этих полях выполняются по модулю числа q.

Существует два основных способа построения полей Галуа:

1. Поле Галуа GF(p), где p - простое число.
2. Расширенное поле Галуа GF(2^m), где m - положительное целое число.

Давайте рассмотрим, как выполняются операции в полях Галуа:

1. **Сложение и вычитание**: Операции сложения и вычитания в полях Галуа выполняются так же, как и в обычных полях. Результат сложения или вычитания двух элементов также должен принадлежать к этому полю.
2. **Умножение**: Умножение в полях Галуа может быть выполнено с использованием таблицы умножения, которая определена для каждого поля. Это таблица, в которой указан результат умножения каждого элемента поля на каждый другой элемент.
3. **Деление**: Деление в полях Галуа может быть выполнено как умножение на обратный элемент. Обратный элемент для каждого элемента определен в поле Галуа.
4. **Возведение в степень**: Возведение в степень в полях Галуа может быть выполнено путем многократного умножения.
5. **Наибольший общий делитель (НОД)**: Для полей Галуа с простым числом элементов вычисление НОД может быть выполнено аналогично алгоритму Евклида для целых чисел. В случае расширенных полей Галуа этот процесс более сложный и требует использования расширенного алгоритма Евклида.

Далее будут представлены примеры работы калькулятора.

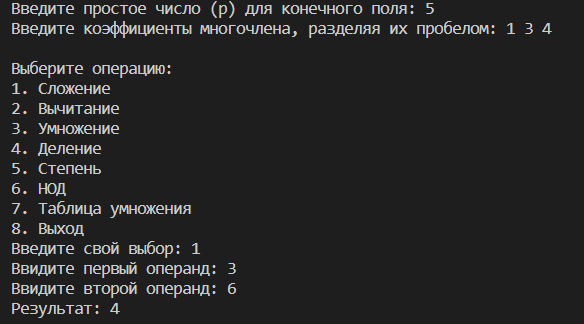


Рисунок 1 – Сложение

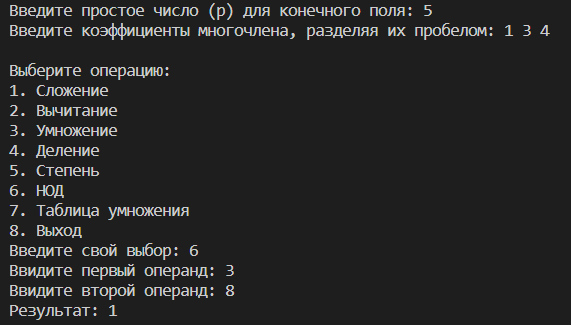


Рисунок 2 – НОД

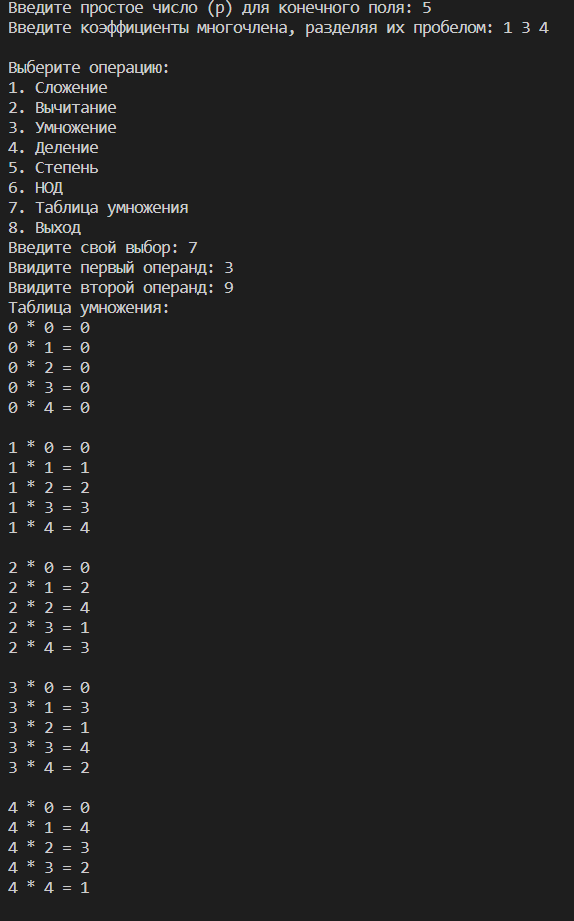


Рисунок 3 – Таблица умножения

**Текст программы:**

**Файл LR3.py:**

def add(x, y, p):

    return (x + y) % p

def subtract(x, y, p):

    return (x - y) % p

def multiply(x, y, p):

    return (x \* y) % p

def division(x, y, p):

    gcd\_xy = gcd(x, y)

    if gcd\_xy != 1:

        raise ValueError("Деление невозможно в конечном поле!")

    return (x \* pow(y, p - 2, p)) % p

def power(x, n, p):

    return pow(x, n, p)

def gcd(x, y):

    while y != 0:

        x, y = y, x % y

    return x

def multiplication\_table(p):

    print("Таблица умножения:")

    for i in range(p):

        for j in range(p):

            print(f"{i} \* {j} = {multiply(i, j, p)}")

        print()

def main():

    try:

        p = int(input("Введите простое число (p) для конечного поля: "))

        polynomial = input("Введите коэффициенты многочлена, разделяя их пробелом: ").split()

        polynomial = [int(coeff) for coeff in polynomial]

        while True:

            print("\nВыберите операцию:")

            print("1. Сложение")

            print("2. Вычитание")

            print("3. Умножение")

            print("4. Деление")

            print("5. Степень")

            print("6. НОД")

            print("7. Таблица умножения")

            print("8. Выход")

            choice = int(input("Введите свой выбор: "))

            if choice == 8:

                print("Выход...")

                break

            if choice > 8 or choice < 1:

                print("Ввидите номер операции из представленных!")

                continue

            x = int(input("Ввидите первый операнд: "))

            y = int(input("Ввидите второй операнд: "))

            if choice == 1:

                result = add(x, y, p)

            elif choice == 2:

                result = subtract(x, y, p)

            elif choice == 3:

                result = multiply(x, y, p)

            elif choice == 4:

                result = division(x, y, p)

            elif choice == 5:

                result = power(x, y, p)

            elif choice == 6:

                result = gcd(x, y)

            elif choice == 7:

                multiplication\_table(p)

                continue

            print("Результат:", result)

    except ValueError:

        print("Неверный ввод. Пожалуйста, введите действительный номер операции.")

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

    main()