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 №3**

**Дисциплина: Криптографические протоколы**

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

Направление подготовки: 02.03.02 Фундаментальная информатика и информационные технологии

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

Лабораторная работа №3

**Задание №13**. Реализовать интерактивный калькулятор в поле Галуа с заданным пользователем образующим многочленом (сложение, умножение, деление, НОД, таблица умножения).

**Поле Галуа (GF)** – это конечное поле, содержащее конечное число элементов. В данном случае рассматривается поле Галуа GF(2^n), где элементы представляются в виде многочленов степени не выше n−1 с коэффициентами из {0,1}.

**Образующий многочлен** – это неприводимый многочлен степени n, используемый для построения поля. Операции в поле выполняются по модулю этого многочлена.

**Операции в поле Галуа**:

* **Сложение** – побитовая операция XOR.
* **Умножение** многочленов с последующим приведением по модулю образующего многочлена.
* **Деление** многочленов с нахождением частного и остатка.
* Нахождение **наибольшего общего делителя** двух многочленов.
* **Таблица**, показывающая результат умножения всех элементов поля.

Ниже представлены результаты работы программы.

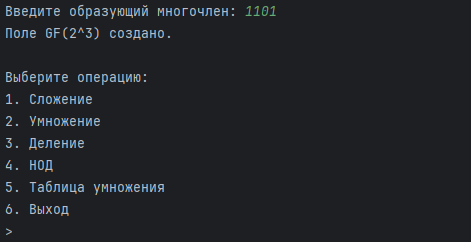


Рисунок 1 – Задаем образующий многочлен и выбираем операцию

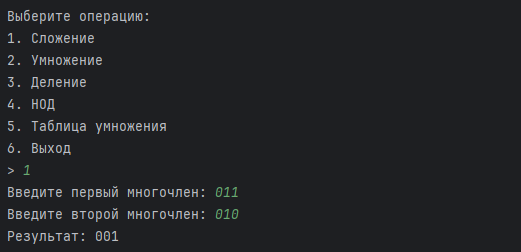


Рисунок 2 – Выполнение операции сложения

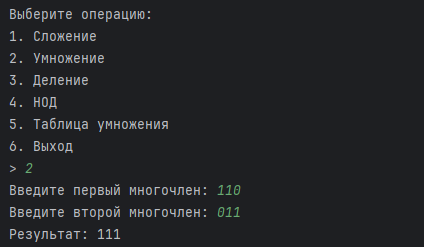


Рисунок 3 – Выполнение операции умножения

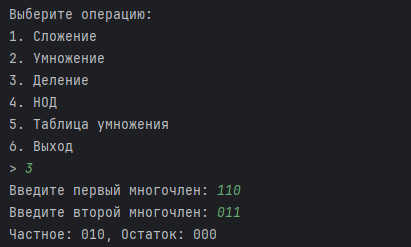


Рисунок 4 – Выполнение операции деления

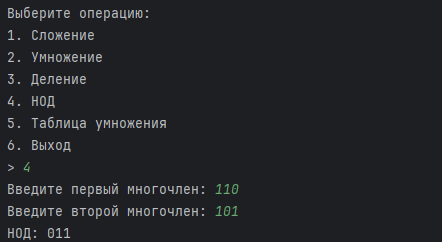


Рисунок 5 – Нахождение наибольшего общего делителя

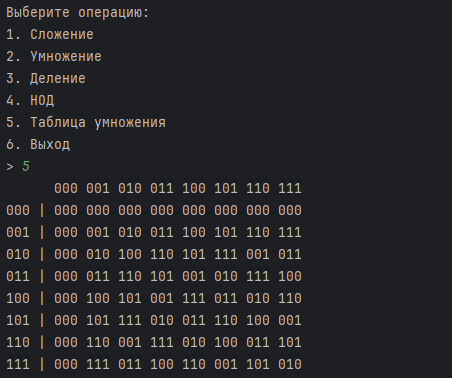


Рисунок 6 – Вывод таблицы умножения