Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования   
**Национальный исследовательский университет «МЭИ»**

**Лабораторная работа №11**

по курсу«**Методы и средства защиты информации**»

Выполнил:

студент группы А-07-18

Востриков Р.В.

Вариант 8

Москва  
2020

**1. Задание**

Задание 1  
Написать программу для умножения двух полиномов над полем Zp. В программу вводится простое число p. Полиномы задаются коэффициентами и степенью.

Задание 2

Определим поле GF(8) как расширение GF(23) простого поля GF(2) по модулю неприводимого многочлена . Ненулевые элементы поля в этом случае – многочлены над GF(2) со степенями не выше второй:

Пусть – корень неприводимого многочлена p(x). Проверить, что он является примитивным элементом поля. Т.к. любой примитивный элемент является корнем .

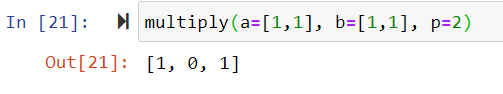
Подсчитать α11.

**2. Описание результатов**

Задание 1

Была составлена программа, вычисляющая произведение двух полиномов над полем Zp. На вход программы подаются массивы коэффициентов, записанных в порядке возрастания степеней, двух полиномов и простое число p. Результат работы программы: произведение полиномов над полем Zp в виде массива коэффициентов.

Результат работы программы на примере из задания:



Задание 2

Проверим примитивность вычислив степени 0-6:

По определению примитивным элементом называется элемент поля, степени которого образуют все ненулевые элементы поля. Мы получили все ненулевые элементы поля, следовательно α – примитивный элемент

Так как в данном поле 7 ненулевых элементов – многочленов над GF(2), то вычислить можно следующим образом:

Результат тот же, что и при вычислении по определению:

**3. Код программы (к заданию 1)**

# функция умножения многочленов над полем Zp

# коэффициенты записываются в порядке возрастания степеней

def multiply(a, b, p = 2):

res = [0]\*(len(a)+len(b)-1) # результат имеет длину соответствующую степени deg(a)+deg(b)

for pow\_ai,ai in enumerate(a):

for pow\_bi,bi in enumerate(b):

res[pow\_ai+pow\_bi] += ai\*bi

for i in range(len(res)):

res[i] %= p

return res

**4. Вывод**

В ходе данной лабораторной работы было рассмотрено введение в теорию конечных полей и работа с полиномами над полями. Также был составлен алгоритм вычисления произведения двух полиномов над полем 𝑍𝑝 , и написана программа, реализующая данный алгоритм.