СПЕЦІАЛЬНІ РОЗДІЛИ ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ

Лабораторна 3

Терпило Софія

ФБ-06

Завдання до комп’ютерного практикуму:

А) Реалізувати поле Галуа характеристики 2 степеня m в поліноміальному базисі з операціями:

1) знаходження константи 0 – нейтрального елемента по операції «+»;

2) знаходження константи 1 – нейтрального елемента по операції «»;

3) додавання елементів;

4) множення елементів;

5) обчислення сліду елементу;

6) піднесення елемента поля до квадрату;

7) піднесення елемента поля до довільного степеня (не вище 2^m - 1, де m – розмірність розширення);

8) знаходження оберненого елемента за множенням;

9) конвертування (переведення) елемента поля в m -бітний рядок (строкове зображення) і навпаки, де m – розмірність розширення;

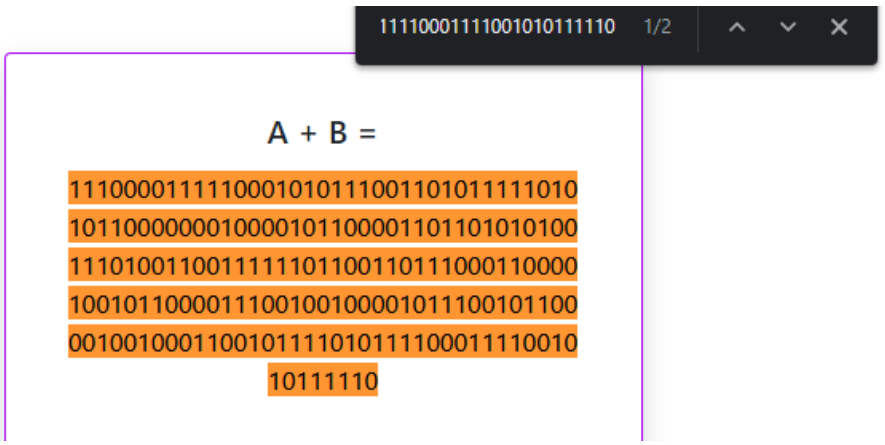
Хід роботи:

Мій варіант мав поле розмірності 233, що задається рівнянням x^233 + x^9 + x^4 + x + 1.

Генератор поля відповідає такому представленню:
100000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000001
000010011

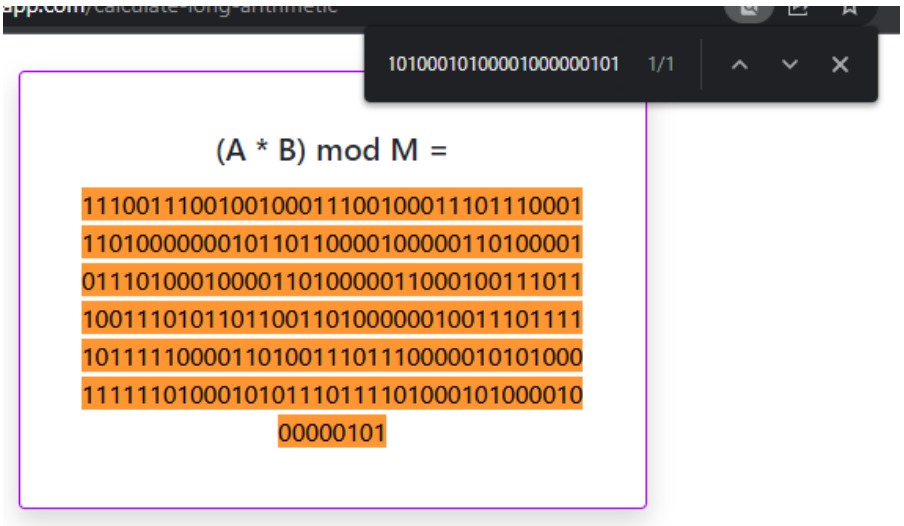
Функція додавання:

addition:
111000011111000101011100110101111101010110000000100001011000011011010101010011
1010011001111110110001000000100110111100010101100110111100000011000101000101
01111100110010011001010100100111010100101 +
1001101111000101011001101101001000110001010000010111110011001001100101010010
0111010100100000011001 =
111000011111000101011100110101111101010110000000100001011000011011010101010011
1010011001111110110011011100011000010010110000111001001000010111001011000010
0100011001011110101111000111100101011110



Функція множення:

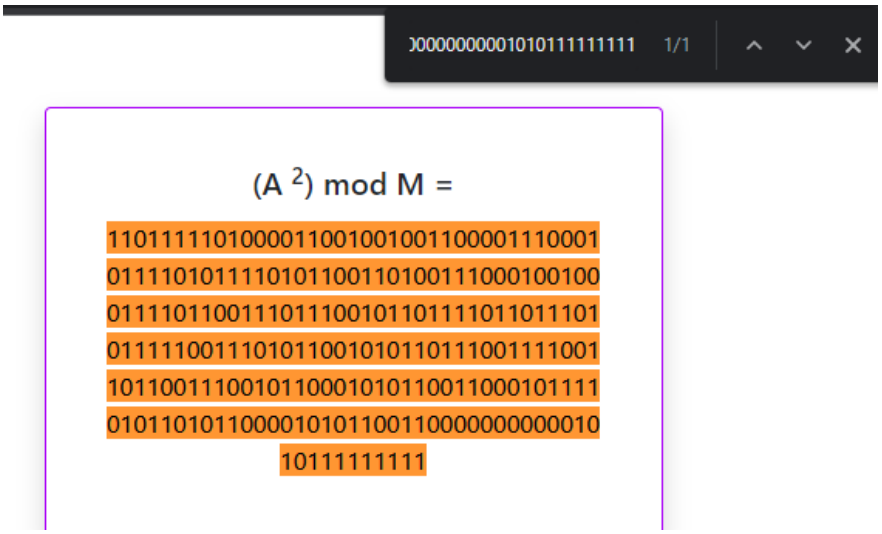
multiplication:
11100001111100010101110011010111110101011000000010000101100001101101010100111011000111111011000100000010011011110001010110011011110000001100010100010101111100110010011001010100100111010100101 *
10011011110001010110011011010010001100010100000101111100110010011001010100100111010100000011001 =
11100111001001000111001000111011100011101000000010110110000100000110100001011101000100001101000001100010011101110011101011011001101000000100111011111011111000011010011101110000010101000111111010001010111011110100010100001000000101



Функція піднесення до квадрату:

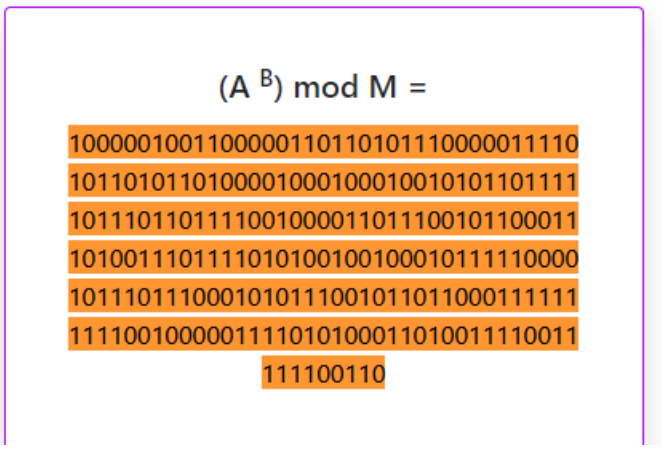
square:
11100001111100010101110011010111110101011000000010011011110000001100010100010101111100110010011101010010100101 ** 2 =
11000111011010100010100011000011010101010101011111100101010110101101101101101101

10110001100010111011111100100111101110000101101000100011000100110101010110111
00110100100000000111011111101100111110110100111101100101100 1



Функція піднесення до довільного степеня:

power:
11100001111100010101110011010111110101011000000010000101100001101101010100111
01001100111111011000100000010011011110001010110011011110000001100010100010101
01111100110010011001010100100111010100101 ^ 1001 =
10000010011000001101101011100000111101011010110100001000100010010101101111101
11011011110010000110111001011000111010011101111010100100100010111110000101111
01110001010111001011011000111111111100100000111101010001101001111001111110010
10



Контроль коректності:

1) (a + b) * c = a * c + c * b