

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 елемента;
- 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:

[illegible]

Функція додавання:

addition:

$$\begin{array}{l} 1110000111110001010111001101011111010101100000001000010110000110110101010011 \\ 1010011001111110110001000000100110111100010101100110111100000011000101000101 \\ 01111100110010011001010100100111010100101 + \\ 1001101111000101011001101101001000110001010000010111110011001001100101010010 \\ 0111010100100000011001 = \\ 1110000111110001010111001101011111010101100000001000010110000110110101010011 \\ 1010011001111110110011011100011000010010110000111001001000010111001011000010 \\ 01000110010111101011110001111001010111110 \end{array}$$

11110001111100010101110011010111110

1011000000010000101100001101101010100

1110100110011111101100110111000110000

1001011000011100100100001011100101100

0010010001100101111010111100011110010

10111110

A + B =

Функція множення:

multiplication:

1110000111110001010111001101011111010101100000001000010110000110110101010011
 1010011001111110110001000000100110111100010101100110111100000011000101000101
 01111100110010011001010100100111010100101 *

1001101111000101011001101101001000110001010000010111110011001001100101010010
 011101010010000011001 =

1110011100100100011100100011101110001110100000001011011000010000011010000101
 1101000100001101000001100010011101110011101011011001101000000100111011111011
 11100001101001110111000001010100011111010001010111011101000101000010000001
 01

10100010100001000000101

1110011100100100011100100011101110001

1101000000010110110000100000110100001

0111010001000011010000011000100111011

1001110101101100110100000010011101111

1011111000011010011101110000010101000

1111110100010101110111101000101000010

00000101

(A * B) mod M =

Функція піднесення до квадрату:

square:

1110000111110001010111001101011111010101100000001001101111000000110001010001
 010111110011100100111010100101 ** 2 =

110001110110101000101000110000110101010101010111110010101011010110110110110

1011000110001011101111100100111101110000101101000100011000100110101010110111
001101001000000001110111111011001111101101001111011001011001

000000000101011111111
1/1
^
v
x

$(A^2) \bmod M =$

1101111101000011001001001100001110001
0111101011110101100110100111000100100
0111101100111011100101101111011011101
0111110011101011001010110111001111001
1011001110010110001010110011000101111
010110101100001010110011000000000010
10111111111

Функція піднесення до довільного степеня:

power:

1110000111110001010111001101011111010101100000001000010110000110110101010011
1010011001111110110001000000100110111100010101100110111100000011000101000101
01111100110010011001010100100111010100101 ^ 1001 =
1000001001100000110110101110000011110101101011010000100010001001010110111110
1110110111100100001101110010110001110100111011110101001001000101111100001011
1011100010101110010110110001111111110010000011110101000110100111100111111001
10

11010011110011111100110
1/1
^
v
x

$(A^B) \bmod M =$

1000001001100000110110101110000011110
1011010110100001000100010010101101111
1011101101111001000011011100101100011
1010011101111010100100100010111110000
1011101110001010111001011011000111111
1111001000001111010100011010011110011
111100110

Контроль коректності:

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

```
10 ##### TEST: (a + b) * c = a * c + c * b
11
12 a = '111000011001101'
13 b = '111000011001101'
14 c = '1001101111'
15 sum1_1 = add_in_field(a[::-1], b[::-1])[:, -1]
16 prod1_1 = multiply_in_field(sum1_1[:, -1], c[:, -1])[:, -1]
17
18 prod2_1 = multiply_in_field(a[:, -1], c[:, -1])[:, -1]
19 prod2_2 = multiply_in_field(c[:, -1], b[:, -1])[:, -1]
20 sum2_1 = add_in_field(prod2_1[:, -1], prod2_2[:, -1])[:, -1]
21
22 print('TEST:', prod1_1, '=', sum2_1)
```

main x

C:\Users\User\PycharmProjects\srom_lab3\venv\Scripts\python.exe

TEST: 10001001010000010111000110 = 10001001010000010111000110