**СПЕЦІАЛЬНІ РОЗДІЛИ**

**ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ No3**

**Реалізація операцій у скінченних полях характеристики 2**

**(поліноміальний базис)**

**1. Мета роботи**

Одержання практичних навичок програмної реалізації обчислень у полі Галуа

характеристики 2 в поліноміальному базисі; ознайомлення з прийомами ефективної реалізації

критичних по часу ділянок програмного коду та методами оцінки їх ефективності.

**3. 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 m, 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;

m = 173

poly\_coefficients = [173, 10, 2, 1, 0]

gen = poly\_to\_GF2\_vector(poly\_coefficients)

num1 = "00110100010011010100111110100011110100001001010000001101010101000010001000100011010001111110110010110000010101010100011110111100001110010010111100111110110001101111111001110"

num2 = "01010110011010101001111011111101011110110010101000100110000111110011100101101001111110111010000010001001111000000011111110110110101000011101100000001011110111011000000101001"

Сума: 01100010001001111101000101011110101010111011111000101011010010110001101101001010101111000100110000111001101101010111100000001010100110001111011100110101000110110111111100111

Час виконання: 0.0 секунд

Добуток: 11110110111101000100110000111101001010001101110000111100000100000011101100100001010100011111011101010001101000010110101100110011100100110111011010011001011111000010100110110

Час виконання: 0.024907350540161133 секунд

Квадрат: 11110001101110110011110101010110001001101001100011101011010111000001111010101111100001111101100101100101011110011001011111001010100001100000111010000010111100110011000110110

Час виконання: 0.0018608570098876953 секунд

Слід: [0]

Час виконання: 0.41974377632141113 секунд

Обернений: 11011011110000010110110111111000110101010011110100010111000101010100010111111001010101000101001111000010011110100111010100000011001000000011110111101100110000100010000010100

Час виконання: 3.304748058319092 секунд

Степінь: 10100001101111001000101010111101101101101110110100010100110000001110101110111001010010100000010010010110101100100100010000110001101100110110101001110111101010111100111001111

Час виконання: 1.8428447246551514 секунд

Test completed