**СПЕЦІАЛЬНІ РОЗДІЛИ**

**ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ No4**

**Реалізація операцій у скінченних полях характеристики 2**

**(нормальний базис)**

**1. Мета роботи**

Одержання практичних навичок програмної реалізації обчислень у полі Галуа

характеристики 2 в нормальному 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

num1 = "00111000010110011010001111111111111100101001011110000010010001011011111001001011110001000101010011101100000011011111100001101110110001101000001010110100110001000010100010100"

num2 = "10111000000001010000101000010001010100001111101100001010001001101110011001111100101010101011111011011101110011001001000101111110001101110011111110001110001100111001111001011"

num3 = "00010101111010100111101110111010001111100000001011111000001000100110101000111101110111001100111000001001111001100110101011011000110111111000011100011000111101010110100100100"

Сума: 10000000010111001010100111101110101000100110110010001000011000110101100000110111011011101110101000110001110000010110100100010000111100011011110100111010111101111011011011111

Час виконання: 0.0 секунд

Добуток: 01000011100111111000000001110000110101010110001100000000001100001011100100001101010011100011011110111110011110010101111010111101010001110001110011101000011011111100001000011

Час виконання: 0.5771043300628662 секунд

Квадрат: 00011100001011001101000111111111111110010100101111000001001000101101111100100101111000100010101001110110000001101111110000110111011000110100000101011010011000100001010001010

Час виконання: 0.0 секунд

Слід: 1

Час виконання: 0.02001476287841797 секунд

Обернений: 10111110011110001001100000111110100011101011111000101110110100011000101011010000111111101100101111000001111101001111011001000111011001010011111111000000001011100110011111110

Час виконання: 9.037317276000977 секунд

Степінь: 11101010000000111111110101011111110011001111100001111101000111100011111000101000000010011010101001110101100010000011111000110001100101000011110011001110101111010101010110100

Час виконання: 49.384384632110596 секунд