

Міністерство освіти і науки України

НТУУ«Київський політехнічний інститут»

Фізико-технічний інститут

Спеціальні розділи обчислювальної

Лабораторна робота №3

**Виконав:**

Студент 3 курсу ФТІ

групи ФІ-03

Недождій М. А.

**Перевірила:**

Пекарчук Н. А.

## 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.

2. 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;

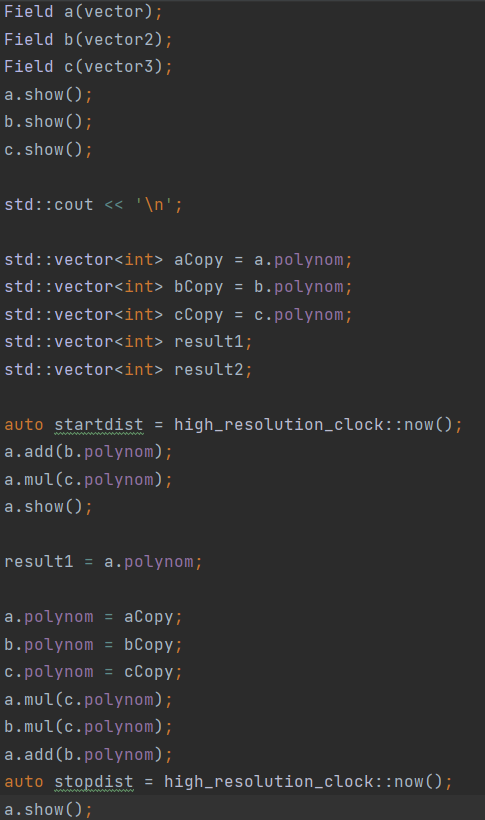
6) піднесення елемента поля до квадрату;

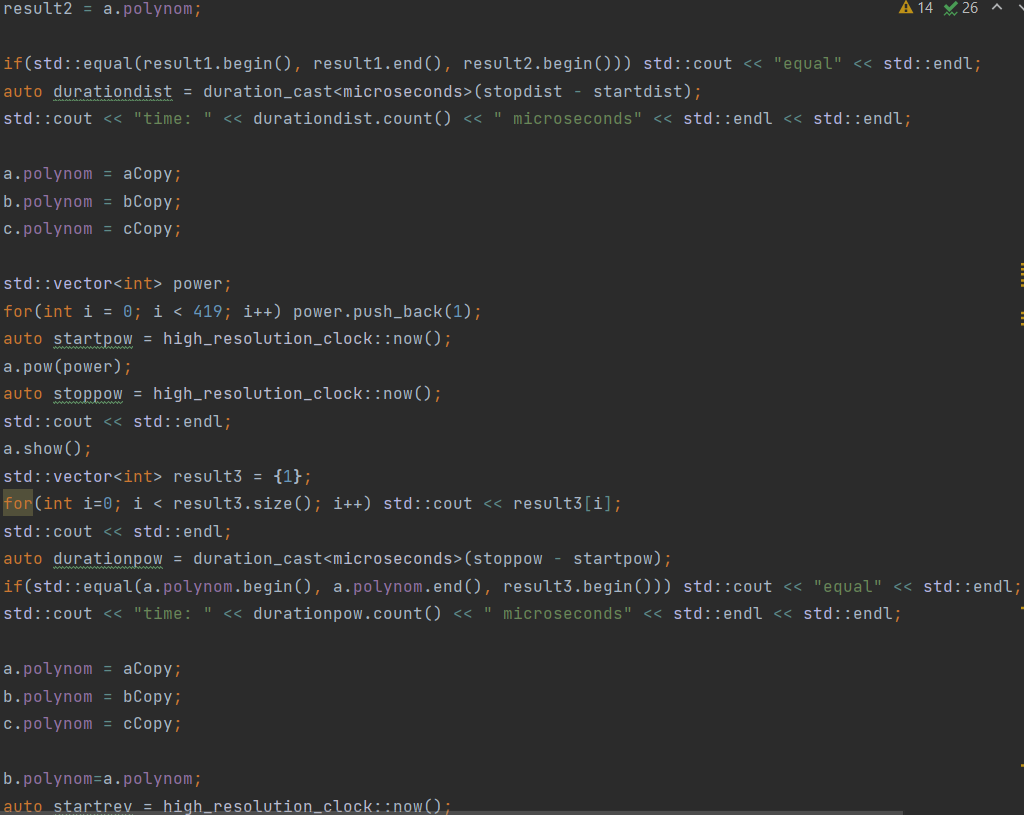
7) піднесення елемента поля до довільного степеня (не вище 2^m -1 , де m – розмірність розширення);

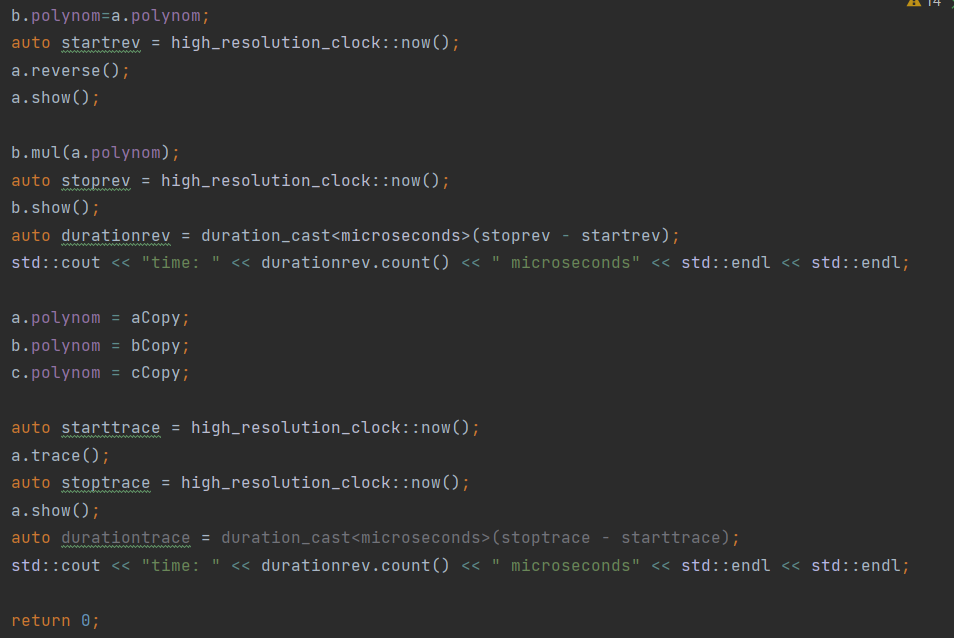
8) знаходження оберненого елемента за множенням;

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

Код програми виконаний мовою C++, залито на GitHub







Дані на вхід для перевірки дистрибутивності, піднесеня в степінь розширення, добутку елемента і оберненого, пошук сліду за mod x^419+x^21+x^14+x+1:

a:

10111101100101000010100110100111001100110110110101001010011111100111101001010001111110001010110110001010011011010110000001100101110011010011010100111000110100000100010101101101001011100010001011100100011110011101101001111011101011001111110100100010100011110100001100001100010100101000000101001001111110010110100010110001011100100011010001110011001110100111011110100110

b:

11000011000110001010100111000100000011100100010100001010111110000011100001101101001001100111111001101001010110111000101010001000100110011100101000100101111111000000000101011100100000010000010001111011010011011011100010010110001111110011011100110000101111101011101010110001100010001000101111111010011000111001110111100110101100011010100101101001110010110011000010011110

c:

10011010000100100000000001011110101100110000100110000000000010100011101100000000010101100000000100101001011000101110010001011101011011100111110001001111100001111110000111111001000001010110011000010111011111110000001111100111111001010011011001101101101101010100000000010011101110001111111100100001010000101101110111111100010101100101111011110001000111010011110010001010

Текст у консолі:

10111110101001110001000000101110011011100010001111001100101100000011000110101010010011100101111100000110111001110110111101110000001001000011110110110001101110001001011000000110110111011010010000011101111000011100001111100011011111100001000110011111110001011100111111101011010110000000000010101011111110010111010111100011001010000111001010010011101011010111011011010100011011101100110111001111111101011000000110010010100

10111110101001110001000000101110011011100010001111001100101100000011000110101010010011100101111100000110111001110110111101110000001001000011110110110001101110001001011000000110110111011010010000011101111000011100001111100011011111100001000110011111110001011100111111101011010110000000000010101011111110010111010111100011001010000111001010010011101011010111011011010100011011101100110111001111111101011000000110010010100

equal

time: 12865 microseconds

a^(2^419-1)

1

1

equal

time: 2688905 microseconds

степінь, у яку підносять для отримання оберненного

11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111110

a^(-1)

1110111010111011010011110101011100011011110001100111101011010001000011111001000110001001101110000100001111001000100000100101011000101110101110001111111101000100111100111001110011010100110100011010100100001110101111100111000101111011001011001101110110101111101011000011110110101111001101000001110010110100110111010100010011001001001000111101011000010101111100100011111110011000001000011100110100001111000011001001100010

a\*a^(-1)

1

time: 2598310 microseconds

trace:

0

time: 2598310 microseconds

**Час виконання операцій у мікросекундах**

|  |  |  |  |
| --- | --- | --- | --- |
| Операція  Значення | Мінімальне | Середнє | Максимальне |
| Дистрибутивність | 12865 | 17848 | 22831 |
| Піднесення в макс степінь. | 2688905 | 2764017 | 2839130 |
| Множення на обернений | 2598310 | 2744347 | 2890384 |
| Пошук сліду | 2598310 | 2744347 | 2890384 |