## СПЕЦІАЛЬНІ РОЗДІЛИ

## ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ

## КОМП’ЮТЕРНИЙ ПРАКТИКУМ No4

## Реалізація операцій у скінченних полях характеристики 2 (нормальний базис)

## 

## Варіант 10



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.

2. Завдання до комп’ютерного практикуму

А) Перевірити умови існування оптимального нормального базису для розширення

(степеня) поля m згідно варіанту. Реалізувати поле Галуа характеристики 2 степеня m в нормальному 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;

8) знаходження оберненого елемента за множенням;

9) конвертування (переведення) елемента поля в m-бітний рядоk;

Код програми виконаний мовою JavaScript

Перевірка коректності:

let test1 = (mul(add(first, second), third));

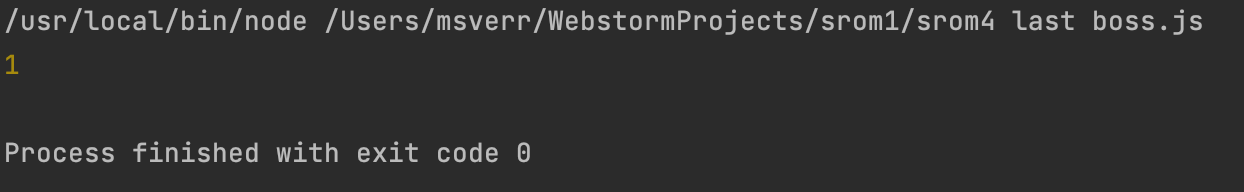
let test2 = (add(mul(second, third), mul(third, first)));

console.log(compare(test1, test2))



Функція compare виводить 0 коли на вхід подаються однакові значення, з чого робимо висновок що операції коректні

console.log(pow(t1, "11111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111"))



З чого робимо висновок про коректність модулярного множення на константу

Час виконання операцій (взято середнє значення при 10 запусках)

| Операція/значення | Мінімальне | Максимальне | Середнє |
| --- | --- | --- | --- |
| Додавання (ксор) | 0.01ms | 2ms | 0.7ms |
| Множення | 0.4ms | 5ms | 2.3ms |
| Піднесення до степеня | 167ms | 300ms | 201.02ms |
| Знаходження сліду | 112ms | 300ms | 202ms |
| Знаходження оберненого | 381ms | 738ms | 453ms |

//піднесення до степеню, співрозмірного числу, 294 знаки