Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

Дисципліна “Спеціальні розділи обчислювальної математики”
Комп’ютерний практикум

Робота №3. Реалізація операцій у скінченних полях характеристики 2 (поліноміальний базис)

Виконав
студент гр. ФБ-11 Подолянко Т.О.
Перевірив
Грубіян Є.О.

Київ — 2023

Робота №3. Реалізація операцій у скінченних полях характеристики 2 (поліноміальний базис)

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.

Завдання до комп'ютерного практикуму згідно з варіантом №13

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;

Розмірність поля m: 419

Генератор поля: $p(x) = x^{419} + x^{21} + x^{14} + x + 1$

Хід роботи

Завдання практикуму реалізовано мовою програмування Rust. Вихідні коди розміщено у інтернет-репозиторії GitHub за посиланням: https://github.com/timofey282228/sprzom-lab3.git.

Коректність реалізації під час виконання перевірена за допомогою тестів та вручну.

```
running 11 tests
test display::tests::display_test ... ok
test tests::deg_test ... ok
test tests::get_coef_test ... ok
test tests::modulo_test ... ok
test tests::mul_test ... ok
test tests::sqr_test ... ok
test tests::eq1 ... ok
test tests::trace_test ... ok
test tests::pow_test ... ok
test tests::eq2 ... ok
test tests::inverse_test ... ok

test result: ok. 11 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.22s
```

Оцінка часу виконання операції.

Наведено середній час виконання операцій з елементами скінченного поля. Елементи поля згенеровані випадковим чином. Для піднесення до степеню — випадкові 7-байтові числа.

```
Performance calculation example
Running 1000 experiments for each operation
Average for +: 24ns
Running 1000 experiments for each operation
Average for *: 245.924µs
Running 1000 experiments for each operation
Average for inverse: 276.4419ms
Running 1000 experiments for each operation
Average for sqr: 300.126µs
Running 1000 experiments for each operation
Average for pow: 165.880088ms
```

В якості додаткового завдання реалізовано алгоритм знаходження коренів квадратного рівняння (над полем варіанту) виду $x^2 + ax = b$. Приклад виконання:

```
     Running unittests src\lib.rs (target\release\deps\gf2-93f241e5d05daaf9.exe)

running 1 test
00000006f9123f6d9067357fcaa50610d88c43d6f4d5e0abcc2ad49cae0123366bfb044128c2c7c04188ebd95fc038bf87dc805865a0e0fc
00000003f7168e668cc366b26a3b998e778919e99a36babde2e3370c6266abbd44250ae0f599edecdfe6dce66221b3e9a623015769936d8d
test solve_sq_eq::tests::test_solve ... ok
```

Для

A =

050E04B10B1CA453CDA09E9F9EAF055A3F6EE35A162EC9E390CC67888B2FDE0EA1DD5B2A2C9E6E373F3DE18B5621FF810F0C338D71

B =

066A1CDA81DFBD5953500236E1D5264911779ECCBCBF1241AC2886FF71AB374B7DD0A28E6863801FF40507229FE65223587491D2CD

знайдено корені:

x1 =
6f9123f6d9067357fcaa50610d88c43d6f4d5e0abcc2ad49cae0123366bfb044128c2c7c04188ebd95fc038bf87dc805865a0e0fc

x2 =
3f7168e668cc366b26a3b998e778919e99a36babde2e3370c6266abbd44250ae0f599edecdfe6dce66221b3e9a623015769936d8d

Коректність розв’язку перевірена підстановкою.