

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 №4. Реалізація операцій у скінченних полях характеристики 2
(нормальний базис)

Виконав

студент гр. ФБ-11 Подолянко Т.О.

Перевірив

Грубіян Є.О.

Київ — 2023

Робота №4. Реалізація операцій у скінченних полях характеристики 2 (нормальний базис)

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.

Завдання до комп'ютерного практикуму згідно з варіантом №13

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 елемента;
- 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; Мова програмування, семантика функцій, спосіб реалізації можуть обиратись довільно. Під час конвертування елементів поля у бітові рядки потрібно враховувати конвенції щодо зображень елементів поля (зокрема, порядок бітів).

Б) Проконтролювати коректність реалізації поля для кожної операції; наприклад, для декількох a, b, c, d перевірити тотожності $(a + b) * c = b * c + c * a$, ... Додатково можна запропонувати свої тести на коректність.

В) Визначити середній час виконання операцій у полі. Підрахувати кількість тактів процесора (або інших одиниць виміру часу) на кожну операцію. Результати подати у вигляді таблиць або діаграм.

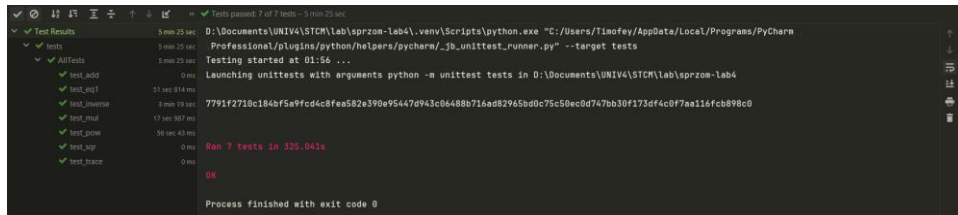
Розмірність поля m : 419

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

Хід роботи

Завдання практикуму реалізовано мовою програмування *Python*.
Вихідні коди розміщено у інтернет-репозиторії GitHub за посиланням:
<https://github.com/timofey282228/sprzom-lab4.git>.

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



The screenshot shows the PyCharm test runner interface. On the left, a tree view shows 'Test Results' expanded, with 'AllTests' and 'tests' listed. The 'tests' folder is expanded, showing seven individual test cases: 'test_add', 'test_eq1', 'test_invert', 'test_mul', 'test_pow', 'test_sqrt', and 'test_trace'. Each test case has a green checkmark indicating it passed. The 'test_add' test is highlighted. On the right, the test execution log shows the following text: 'Tests passed: 7 of 7 tests - 5 min 25 sec', 'D:\Documents\UNIV4\STCM\lab\sprzom-lab4\.venv\Scripts\python.exe "C:/Users/Timofey/AppData/Local/Programs/PyCharm Professional/plugins/python/helpers/pycharm/_jb_unittest_runner.py" --target tests', 'Testing started at 01:56 ...', 'Launching unittests with arguments python -m unittest tests in D:\Documents\UNIV4\STCM\lab\sprzom-lab4', '7791f2710c184bf5a9fcd4ccf5a582e390e95447d943c06488b716ad82965bd0c75c50ec0d747bb30f173df4cf7aa116fcb898c0', and 'Run 7 tests in 325.041s'. At the bottom, it says 'OK' and 'Process finished with exit code 0'.

Оцінка часу виконання операції.

Оцінювання не проводилося, оскільки реалізація мовою Python занадто повільна (наприклад, знаходження оберненого за алгоритмом Іто-Цудзії займає порядка 3 хв...)