1 Реалізація

Клас GaloisField представляє елементи поля Галуа зі степенем 239. Він включає в себе арифметичні операції, такі як додавання, множення, піднесення до степеня, знаходження обернених чисел та сліду. Клас також підтримує ініціалізацію з бітового набору, шістнадцяткового рядка та випадкову генерацію бітів.

2 Середній час роботи операцій

Розмір	**Додавання (ns)**	**Множення (ns)**	**Піднесення до степеня (ms)**	**Обернення (ms)**
16	128.57	45312.8	178.07	352.46
32	126.45	79633.6	191.5	357.66
64	116.43	155148	196.44	349.45
128	123.15	333578	226.35	356.46
239	148.22	792021	285.47	379.63

Табл. 1: Середній час виконання операцій

!!! В таблиці фігурує змінна *'розмір'*, для неї я генерував випадкові бітові послідновності, тобто, якщо розмір 16, то це означає, що потенційно лише перші 16 бітів послідовності можуть бути 1, а всі інші 0.

3 Тестування класу GaloisField

Ці тести перевіряють функціональність операцій у класі GaloisField.

3.1 Addition Tests

- Addition Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
  - результат: 23af811b872bbc1d2dd991cfdeacd7a0dbb33a69552a0e89279ebfddde1
- Neutral Element Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - $zero$: 000000000000000000000000000000000000000000000000000000000000000000000000
  - результат: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c

3.2 Multiplication Tests

- Multiplication Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
  - результат: 28f0923c10c934e09527bfa23cd7e2b853b3b2f3e0b3ec7aea2152073287
- Neutral Element Test:
  - вхід:

        * a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
        * one: 0000000000000000000000000000000000000000000000000000000000000001
    - результат: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c

- To Square Test:
    - вхід:
        * a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - результат: 50b6456108378713c37d3039cf1792aec1b5f9dfbebbc0a6c770a75d693e

- To Power Of Test:
    - вхід:
        * a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
        * b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
    - результат: 17c762a0c47b27abcd6d274ad5b5c738ff5ac768d320f24514b1f483ddaa

3.3 Utilities Tests

- Trace Test:
    - вхід:
        * a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
        * b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
    - результат: для 'a' = 0, для 'b' = 1

- Inverse Test:
    - вхід:
        * a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
        * b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
    - результат для 'a': 5832c6cdadb2067298e6c340ce3eadf6810ed043badeb297a8219eebc277
    - результат для 'b': 3d4b7cbaf4dec964719450d456eb5c6074b00df53fa4e11d19b248328389

3.4 Complex Tests

- Distributivity Test:
    - вхід:
        * a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
        * b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
        * c: 09d7f58ff5398570a5ba840d9f0fc5c806f5353788a4c0b8488e4e62d2a
    - результат: True

- Neutral Test:
    - вхід:
        * a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - результат: 1