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

addition (ns)	multiplication (ns)	to power (ms)	inverse (ms)	to square (ns)
358.64	36.04	4436.34	443.31	433.93

Табл. 1: Середній час виконання операцій

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
    - $zero$: 0000000000000000000000000000000000000000000000000000000000000000
  - результат: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c

3.2 Multiplication Tests

- Multiplication Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
  - результат: f1032ceec873b9ad89ad868839c48d2b1453ab9791233f597161cec4abc
- To Square Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
  - результат: 27e0e47b91ec845422caabdb9d8ec99aed8aca3570e69e31c5a03f54096
- To Power Of Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
  - результат: 7fe807e61c75fb7aa1e9fc4b09c1a549d500440ac7e572cfccb1b0be36a4

3.3 Utilities Tests

- Trace Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
  - результат: для 'a' = 116, для 'b' = 117
- Inverse Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
  - результат для 'a': 204bdb3f7f6afbc1d432c39c34cb28b3967369e91df764019b5cb3b89880
  - результат для 'b': 24c4831dc75e12a14d3cbc9332ec8a71eb5d697f79091b2bd98f309fd677

3.4 Complex Tests

- Distributivity Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
    - b: 6c6e49eca4f2b4b5684cc678e5b1449500a6ae03b4e732eaacdec175ccd
    - c: 09d7f58ff5398570a5ba840d9f0fc5c806f5353788a4c0b8488e4e62d2a
  - результат: True
- Neutral Test:
  - вхід:
    - a: 4fc1c8f723d908a8459557b73b1d9335db15946ae1cd3c638b407ea812c
  - результат: 1