

Міністерство освіти і науки України

НТУУ«Київський політехнічний інститут»

Фізико-технічний інститут

Спеціальні розділи обчислювальної

Лабораторна робота

Робота №4

**Виконав:**

Студент 3 курсу ФТІ

групи ФІ-03

Буржимський Р. В

**Перевірила:**

Пекарчук Н. А.

**Реалізація операцій у скінченних полях характеристики 2**

**(нормальний базис)**

**МЕТА**: 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. Варіант 3**

M=179

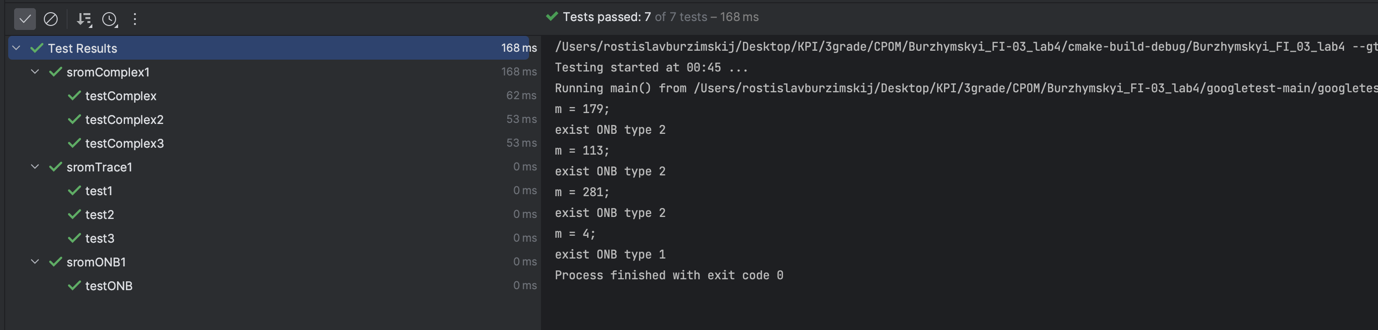
Повинні бути реалізовані такі операції:

1. знаходження константи 0 – нейтрального елемента по операції «+»;
2. знаходження константи 1 – нейтрального елемента по операції «\*»;
3. додавання елемента;
4. множення елемента;
5. піднесення елемента поля до квадрату;
6. обчислення сліду елемента
7. піднесення елемента поля до квадрату
8. піднесення елемента поля до довільного степеня (не вище 2m -1, де m –розмірність розширення);
9. конвертування (переведення) елемента поля в m -бітний рядок (строкове зображення) і навпаки, де m – розмірність розширення;

Тести

##include "gtest/gtest.h"  
#include "GF2.h"  
  
  
using namespace std;  
using namespace Field;  
  
TEST(sromComplex1,testComplex) {  
 GF2 A("3d6bacade1796866572b47c42e0a9c06858f7e881");  
 GF2 A1("3d6bacade1796866572b47c42e0a9c06858f7e881");  
  
 GF2 B("b7d34bbc0f2fc1bd486220355ae28a80695e19d0b");  
  
 GF2 C("ba2674f085c3f9f6cb67c3cd6dae5d8cfd341592b");  
  
 A += B;  
 GF2 tmp1 = C \* A;  
 GF2 tmp2 = B \* C;  
 tmp2 += (C \* A1);  
  
 EXPECT\_EQ(tmp1, tmp2);  
 std::string pow = "7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF";  
 EXPECT\_EQ((A^pow),one);  
 EXPECT\_EQ((B^pow),one);  
 EXPECT\_EQ((C^pow),one);  
  
 EXPECT\_EQ(A.inverseGF()\*A,one);  
 EXPECT\_EQ(B.inverseGF()\*B,one);  
 EXPECT\_EQ(C.inverseGF()\*C,one);  
}  
  
TEST(sromComplex1,testComplex2) {  
 GF2 A("1d1604e1854d10220cc13af0623ae471d92680345");  
 GF2 A1("1d1604e1854d10220cc13af0623ae471d92680345");  
  
 GF2 B("2ff26c39b61ca87c0c9be2fe0ef75452717e707df");  
 GF2 C("1fbc78586454cbb41ca6bbf4f65f25c7b8cb049ce");  
  
 A += B;  
 GF2 tmp1 = C \* A;  
 GF2 tmp2 = B \* C;  
 tmp2 += (C \* A1);  
  
 EXPECT\_EQ(tmp1, tmp2);  
 std::string pow = "7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF";  
 EXPECT\_EQ((A^pow),one);  
 EXPECT\_EQ((B^pow),one);  
 EXPECT\_EQ((C^pow),one);  
  
 EXPECT\_EQ(A.inverseGF()\*A,one);  
 EXPECT\_EQ(B.inverseGF()\*B,one);  
 EXPECT\_EQ(C.inverseGF()\*C,one);  
  
}  
  
TEST(sromComplex1,testComplex3) {  
 GF2 A("1e9c77c0607a981cff627d2c7754ad4a3ee9a4cd");  
 GF2 A1("1e9c77c0607a981cff627d2c7754ad4a3ee9a4cd");  
  
 GF2 B("61d2108aed8f41544b69fef9b98fc0714f48c27f1");  
 GF2 C("f293972f21bba02c2989d75b08b69ecd9e728a589");  
  
 A += B;  
 GF2 tmp1 = C \* A;  
 GF2 tmp2 = B \* C;  
 tmp2 += (C \* A1);  
  
 EXPECT\_EQ(tmp1, tmp2);  
 std::string pow = "7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF";  
 EXPECT\_EQ((A^pow),one);  
 EXPECT\_EQ((B^pow),one);  
 EXPECT\_EQ((C^pow),one);  
  
 EXPECT\_EQ(A.inverseGF()\*A,one);  
 EXPECT\_EQ(B.inverseGF()\*B,one);  
 EXPECT\_EQ(C.inverseGF()\*C,one);  
}  
  
TEST(sromTrace1,test1) {  
  
 GF2 A("a05075a1e132d524");  
 GF2 B("1a05075a1e132d524");  
 EXPECT\_EQ(A.Trace(),~B.Trace() & 1);  
}  
  
TEST(sromTrace1,test2) {  
  
 GF2 A("9cbc6dcd870c91fe483b39f9a0082628");  
 GF2 B("e9cbc6dcd870c91fe483b39f9a0082628");  
 EXPECT\_EQ(A.Trace(),~B.Trace() & 1);  
}  
TEST(sromTrace1,test3) {  
  
 GF2 A("12e7ef7de64827ebc80e2f7e5cdd425b");  
 GF2 B("12e7ef7de64827ebc80e2f7e5cdd425b1");  
 EXPECT\_EQ(A.Trace(),~B.Trace() & 1);  
}  
  
TEST(sromONB1,testONB) {  
 GF2 A("12e7ef7de64827ebc80e2f7e5cdd425b");  
 A.ONB(179,1);  
 A.ONB(113,1);  
 A.ONB(281,1);  
 A.ONB(4,1);  
}

Приклад виконання тесту

testComplex – це блокові тести на пункт Б) 

**Час виконання операцій**

|  |  |  |  |
| --- | --- | --- | --- |
| Операція  Значення | Мінімальне | Середнє | Максимальне |
| Множення | 1 мс | 2 мс | 3 мс |
| Додавання | <0мс | <0мс | <0мс |
| Оберенений | 3мс | 4 мс | 5мс |
| Піднесення до степеня | 17 мс | 16мс | 19мс |
| Трейс | <0 мс | <0 мс | мс |

\*Піднесення вимірювалося до максимального степеня(7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF)