СПЕЦІАЛЬНІ РОЗДІЛИ

ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4

Реалізація операцій у скінченних полях характеристики 2

(нормальний базис)

1. 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

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 елементу;

6) піднесення елемента поля до квадрату;

7) піднесення елемента поля до довільного степеня (не вище 2m □ 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).

Хід роботи

Написавши бібліотеку для роботи з елементами в поліноміальному базисі, визначеному моїм варіантом проведемо тести для визначення коректності роботи нашої бібліотеки.

Демонстрація роботи.

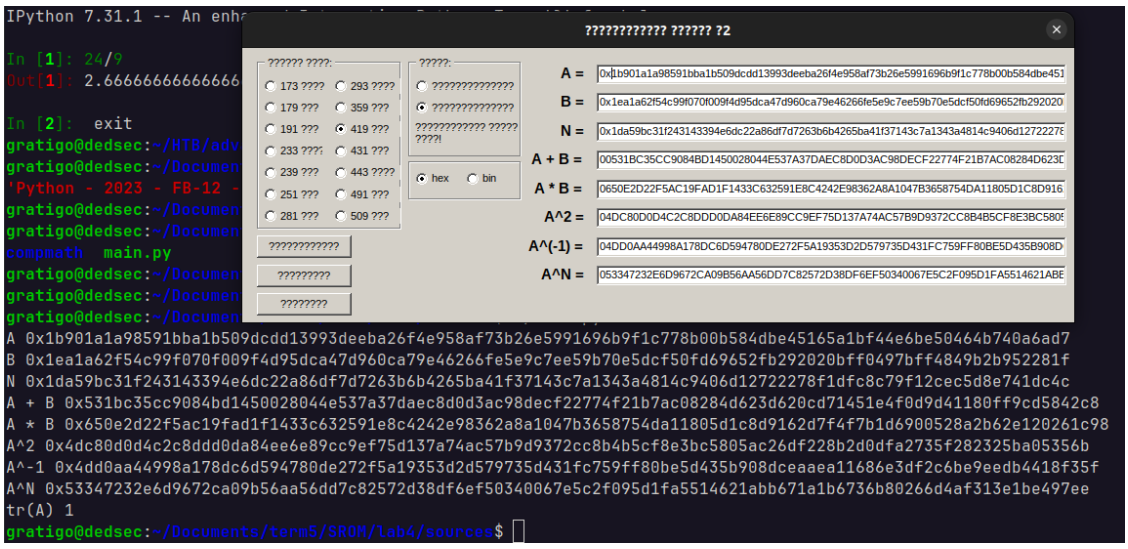
gratigo@dedsec: ~/Documents/term5/SRO... × gratigo@dedsec: ~/Documents/term5/SRO... ×

```python
#!/usr/bin/python3
from compmath.gf import *
from random import getrandbits
import time

def main() -> None:
    fld = GF()
    BITS = fld.m
    A,B,N = getrandbits(BITS),getrandbits(BITS),getrandbits(BITS)
    a,b,n = fld(A),fld(B),fld(N)
    print("A",a)
    print("B",b)
    print("N",n)
    print("A + B",a+b)
    print("A * B",a*b)
    print("A^2",a**2)
    print("A^-1",a.inv())
    print("A^N",a**n)
    print("tr(A)",a.trace())



if __name__ == "__main__":
    main()
```



Весь функціонал є, правильно і швидко

```
gratigo@dedsec:~/Documents/term5/SROM/lab4/sources$ time ./main.py
A 0x1be0ebe928fdbcf35a2857a7f540d4556b7c19e18694a69b5372533b562c0e7c52c1fbb167491b8af3b46f543f388f55046415277
B 0x4fb241a8d82171288f184d44377ba4b790d13c01e065c85d34d39419e2e1fb2647bd925f66fae1baa9658746c393a52f2b299d084
N 0x7dac3cd3d13ff1fd3eba39c10d16a48401a6b24c55ce9312cb5181324677d73beeab12dc43266c52d634c6266ae14493de5820bcf
A + B 0x5452aa41f0dccddbd5301ae3c23b70e2fbad25e066f16ec667a1c722b4cdf55a157c69ee01b3fa305ad1e812fcab2a7a2f4d882f3
A * B 0x2062d0f06a65958d8fe0e4f4c8319c73420c8a82bd106b4be9c7e53581d83734853af4b0f3db90182a108600d86be933f8e190310
A^2 0x4df075f4947ede79ad142bd3faa06a2ab5be0cf0c34a534da9b9299dab16073e2960fdd8b3a48dc579da37aa1f9c47aa82320a93b
A^-1 0x6040d735a2591f60e85060248ed651b82b25b0086dd4be949eabc076230d2f99766a77cade0b2a66afe961d7d3fcd1116549cee85
A^N 0x4b954eb55a7919fa5c02ee8880ed20d9d246ec9cb3471880af7b91c2244a57546dce6ab8bbbdc44e07872ba5d24d305f08a759c17
tr(A) 0

real    0m3,274s
user    0m3,264s
sys     0m0,005s
```