

СПЕЦІАЛЬНІ РОЗДІЛИ ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ

Комп'ютерний практикум №4

Реалізація операцій у скінченних полях характеристики 2

(нормальний базис)

ФБ-23 Моїсеєнко Дмитро

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.

Варіант 3 – як в попередній лабораторній роботі $m=179$

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 « \square »;
- 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 $2m \square 1$, 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.

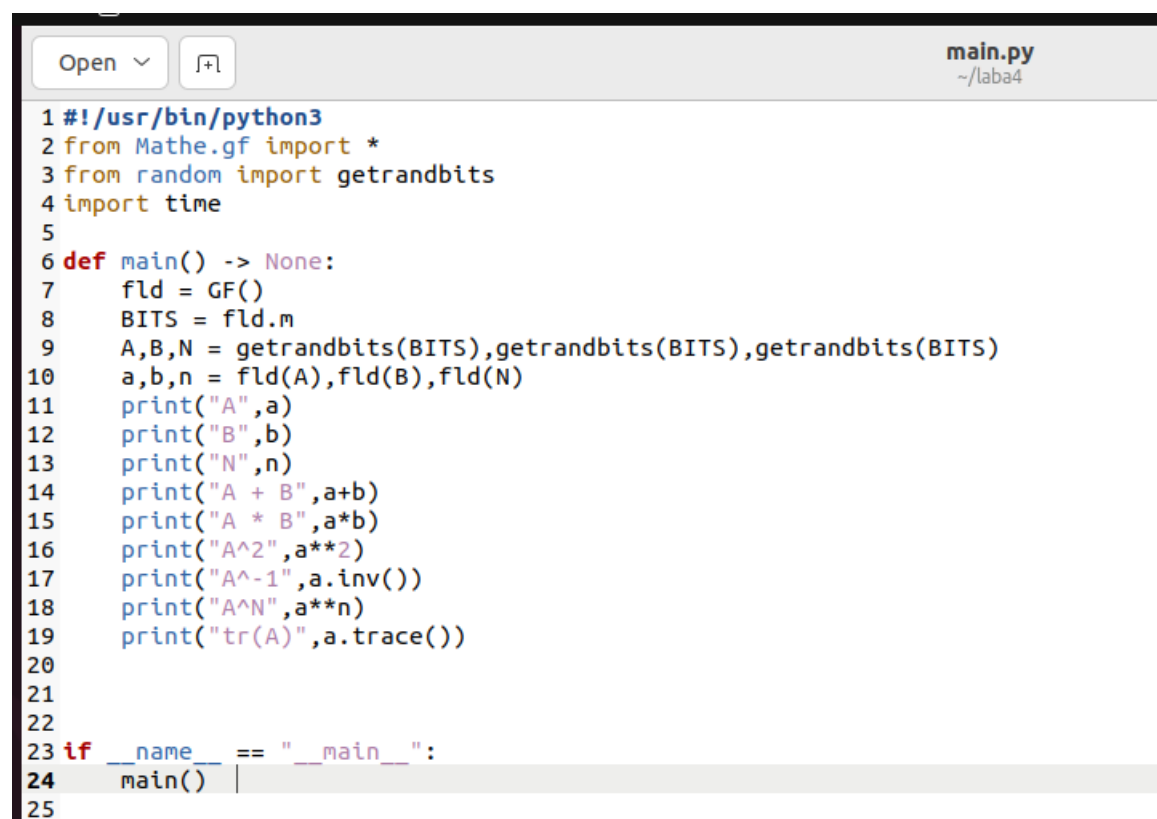
Під час конвертування елементів поля у бітові рядки потрібно враховувати конвенції щодо зображень елементів поля (зокрема, порядок бітів).

Хід роботи:

Напишемо програму бібліотеку для роботи з елементами нормального базису при визначенні довільного мого варіанту та визначити коректність роботи нашої бібліотеки.

Реалізація програмної роботи:

Код *main.py*:



```
1 #!/usr/bin/python3
2 from Mathe.gf import *
3 from random import getrandbits
4 import time
5
6 def main() -> None:
7     fld = GF()
8     BITS = fld.m
9     A,B,N = getrandbits(BITS),getrandbits(BITS),getrandbits(BITS)
10    a,b,n = fld(A),fld(B),fld(N)
11    print("A",a)
12    print("B",b)
13    print("N",n)
14    print("A + B",a+b)
15    print("A * B",a*b)
16    print("A^2",a**2)
17    print("A^-1",a.inv())
18    print("A^N",a**n)
19    print("tr(A)",a.trace())
20
21
22
23 if __name__ == "__main__":
24     main()
25
```

Застосовав tkinter:

