Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”
Факультет інформатики та обчислювальної техніки
Кафедра інформаційні систем та технологій

# Лабораторна робота №3

із дисципліни «Безпека інформаційних систем»

**Тема:** «Дослідження арифметичної системи GF(p). Скінченні поля Галуа»

Виконав:
Студент групи ІА-31
Самелюк А.С.

Перевірив:
Шимкович Л.Л.

Київ-2025

**Тема:** Дослідження арифметичної системи GF(p). Скінченні поля Галуа.

## Хід роботи:

**Завдання №1.** Побудувати таблицю мультиплікативних циклів елементів M29 із GF(29).

Для побудови таблиці мультиплікативних циклів елементів у полі GF(29) нам потрібно знайти порядок кожного елемента від 1 до 28 у модулі 29. Це включає обчислення множинного складу кожного елемента, поки ми не отримаємо значення, еквівалентне 1. Тобто, для кожного елемента a, шукаємо найменше j таке, що a^j ≡ 1(mod29)

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 4 | 8 | 16 | 3 | 6 | 12 | 24 | 19 | 9 | 18 | 7 | 14 | 28 | 27 | 25 | 21 | 13 | 26 | 23 | 17 | 5 | 10 | 20 | 11 | 22 | 15 | 1 |
| 3 | 9 | 27 | 23 | 11 | 4 | 12 | 7 | 21 | 5 | 15 | 16 | 19 | 28 | 26 | 20 | 2 | 6 | 18 | 25 | 17 | 22 | 8 | 24 | 14 | 13 | 10 | 1 |
| 4 | 16 | 6 | 24 | 9 | 7 | 28 | 25 | 13 | 23 | 5 | 20 | 22 | 1 | 4 | 16 | 6 | 24 | 9 | 7 | 28 | 25 | 13 | 23 | 5 | 20 | 22 | 1 |
| 5 | 25 | 9 | 16 | 22 | 23 | 28 | 24 | 4 | 20 | 13 | 7 | 6 | 1 | 5 | 25 | 9 | 16 | 22 | 23 | 28 | 24 | 4 | 20 | 13 | 7 | 6 | 1 |
| 6 | 7 | 13 | 20 | 4 | 24 | 28 | 23 | 22 | 16 | 9 | 25 | 5 | 1 | 6 | 7 | 13 | 20 | 4 | 24 | 28 | 23 | 22 | 16 | 9 | 25 | 5 | 1 |
| 7 | 20 | 24 | 23 | 16 | 25 | 1 | 7 | 20 | 24 | 23 | 16 | 25 | 1 | 7 | 20 | 24 | 23 | 16 | 25 | 1 | 7 | 20 | 24 | 23 | 16 | 25 | 1 |
| 8 | 6 | 19 | 7 | 27 | 13 | 17 | 20 | 15 | 4 | 3 | 24 | 18 | 28 | 21 | 23 | 10 | 22 | 2 | 16 | 12 | 9 | 14 | 25 | 26 | 5 | 11 | 1 |
| 9 | 23 | 4 | 7 | 5 | 16 | 28 | 20 | 6 | 25 | 22 | 24 | 13 | 1 | 9 | 23 | 4 | 7 | 5 | 16 | 28 | 20 | 6 | 25 | 22 | 24 | 13 | 1 |
| 10 | 13 | 14 | 24 | 8 | 22 | 17 | 25 | 18 | 6 | 2 | 20 | 26 | 28 | 19 | 16 | 15 | 5 | 21 | 7 | 12 | 4 | 11 | 23 | 27 | 9 | 3 | 1 |
| 11 | 5 | 26 | 25 | 14 | 9 | 12 | 16 | 2 | 22 | 10 | 23 | 21 | 28 | 18 | 24 | 3 | 4 | 15 | 20 | 17 | 13 | 27 | 7 | 19 | 6 | 8 | 1 |
| 12 | 28 | 17 | 1 | 12 | 28 | 17 | 1 | 12 | 28 | 17 | 1 | 12 | 28 | 17 | 1 | 12 | 28 | 17 | 1 | 12 | 28 | 17 | 1 | 12 | 28 | 17 | 1 |
| 13 | 24 | 22 | 25 | 6 | 20 | 28 | 16 | 5 | 7 | 4 | 23 | 9 | 1 | 13 | 24 | 22 | 25 | 6 | 20 | 28 | 16 | 5 | 7 | 4 | 23 | 9 | 1 |
| 14 | 22 | 18 | 20 | 19 | 5 | 12 | 23 | 3 | 13 | 8 | 25 | 2 | 28 | 15 | 7 | 11 | 9 | 10 | 24 | 17 | 6 | 26 | 16 | 21 | 4 | 27 | 1 |
| 15 | 22 | 11 | 20 | 19 | 5 | 17 | 23 | 26 | 13 | 21 | 25 | 27 | 28 | 14 | 7 | 18 | 9 | 19 | 24 | 12 | 6 | 3 | 16 | 8 | 4 | 2 | 1 |
| 16 | 24 | 7 | 25 | 23 | 20 | 1 | 16 | 24 | 7 | 25 | 23 | 20 | 1 | 16 | 24 | 7 | 25 | 23 | 20 | 1 | 16 | 24 | 7 | 25 | 23 | 20 | 1 |
| 17 | 28 | 12 | 1 | 17 | 28 | 12 | 1 | 17 | 28 | 12 | 1 | 17 | 28 | 12 | 1 | 17 | 28 | 12 | 1 | 17 | 28 | 12 | 1 | 17 | 28 | 12 | 1 |
| 18 | 5 | 3 | 25 | 15 | 9 | 17 | 16 | 27 | 22 | 19 | 23 | 8 | 28 | 11 | 24 | 26 | 4 | 14 | 20 | 12 | 13 | 2 | 7 | 10 | 6 | 21 | 1 |
| 19 | 13 | 15 | 24 | 21 | 22 | 12 | 25 | 11 | 6 | 27 | 20 | 3 | 28 | 10 | 16 | 14 | 5 | 8 | 7 | 17 | 4 | 18 | 23 | 2 | 9 | 26 | 1 |
| 20 | 23 | 25 | 7 | 24 | 16 | 1 | 20 | 23 | 25 | 7 | 24 | 16 | 1 | 20 | 23 | 25 | 7 | 24 | 16 | 1 | 20 | 23 | 25 | 7 | 24 | 16 | 1 |
| 21 | 6 | 10 | 7 | 2 | 13 | 12 | 20 | 14 | 4 | 26 | 24 | 11 | 28 | 8 | 23 | 19 | 22 | 27 | 16 | 17 | 9 | 15 | 25 | 3 | 5 | 18 | 1 |
| 22 | 20 | 5 | 23 | 12 | 25 | 28 | 7 | 9 | 24 | 6 | 16 | 4 | 1 | 22 | 20 | 5 | 23 | 12 | 25 | 28 | 7 | 9 | 24 | 6 | 16 | 4 | 1 |
| 23 | 7 | 16 | 20 | 25 | 24 | 1 | 23 | 7 | 16 | 20 | 25 | 24 | 1 | 23 | 7 | 16 | 20 | 25 | 24 | 1 | 23 | 7 | 16 | 20 | 25 | 24 | 1 |
| 24 | 25 | 20 | 16 | 7 | 23 | 1 | 24 | 25 | 20 | 16 | 7 | 23 | 1 | 24 | 25 | 20 | 16 | 7 | 23 | 1 | 24 | 25 | 20 | 16 | 7 | 23 | 1 |
| 25 | 16 | 23 | 24 | 20 | 7 | 1 | 25 | 16 | 23 | 24 | 20 | 7 | 1 | 25 | 16 | 23 | 24 | 20 | 7 | 1 | 25 | 16 | 23 | 24 | 20 | 7 | 1 |
| 26 | 9 | 2 | 23 | 18 | 4 | 17 | 7 | 8 | 5 | 14 | 16 | 10 | 28 | 3 | 20 | 27 | 6 | 11 | 25 | 12 | 22 | 21 | 24 | 15 | 13 | 19 | 1 |
| 27 | 4 | 21 | 16 | 26 | 6 | 17 | 24 | 10 | 9 | 11 | 7 | 15 | 28 | 2 | 25 | 8 | 13 | 3 | 23 | 12 | 5 | 19 | 20 | 18 | 22 | 14 | 1 |
| 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 | 28 | 1 |

**Завдання №2.** Виконати наступні операції над елементами поля GF(p), де p=29; для обчислень брати різні первісні елементи з таблиці мультиплікативних циклів елементів M29 із GF(29);

b,c,d є GF(29), 1.b = 4, c = 7; 2. b = 12, c = 17; 3. b = 22, c = 25.

**1. b+c≡d**

Для кожної пари b та c, обчислимо суму b + c за модулем 29:
*При b = 4 і c = 7:* d = (4 + 7) mod 29 = 11
*При b = 12 і c = 17:* d = (12 + 17) mod 29 = 0
*При b = 22 і c = 25:* d = (22 + 25) mod 29 = 18

**2. b-c≡d**

Знайдемо обернений за додаванням елемент −c для кожного значення c, а потім додамо його до b за модулем 29

*При b = 4, c = 7*
–c ≡ −7 (mod29) = 22 (mod29)
b−c ≡ 4 + 22(mod29) ≡ 26(mod29)

*При b = 12, c = 17*
−c ≡ −17(mod29) ≡ 29 − 17 = 12(mod29)
b−c ≡ 12 + 12(mod29) ≡ 24(mod29)

*При b = 22, c = 25*
−c ≡ −25(mod29) ≡ 29 − 25 = 4(mod29)
b−c ≡ 22 + 4(mod29) ≡ 26(mod29)

**3. b*c≡d(mod29), (w^j є GF(29)**

*При b=4, c=7 та w=2:* d=(4*7)mod 29 = 2^2 * 2^12 mod 29 ≡ 2^14 mod 29 = 28
*При b=12 і c=17 та w=10:* d=(12*17)mod 29 = 10^7 * 10^21 mod 29 ≡ 10^28 mod 29 [28 mod 28 = 0]= 1
*При b=22 і c=25 та w=8:* d=(22*25)mod 29 = 8^18 *8^24 mod 29 = 8^42 mod 29 [42 mod 28 = 14]= 8^14 mod 29 ≡ 28

**4. b : c≡d(mod29), (w^j є GF(29))**
При b=4, c=7 та w=8: d=(4/7)mod 29 = 8^10 / 8^4 ≡ 13 mod 29
При b=12 і c=17 та w=3: d=(12/17)mod 29 = 3^7 / 3^21 ≡ w^28 * w^-14 = 28
При b=22 і c=25 та w=21: d=(22/25)mod 29 = 21^18 /21^24 ≡ w^28 * w^-6 = 9

**5. b^m≡d(mod29), c^m≡d(mod29), m=32, 37, 43.**

*При b=4 та m=32 та w=2:* d=(4^32)mod29 = (2^2)^32 mod29 = 2^64 mod29 = 2^8 mod29 = 24
*При c=7 та m=32 та w=2:* d=(7^32)mod29 = (2^12)^32 mod29 = 2^384 mod29 = 2^20 mod29 = 23

*При b=12 та m=37 та w=15:* d=(12^37)mod29 = (15^21)^37 mod29 = 15^777 mod29 = 15^21 mod29 = 12
*При c=17 та m=37 та w=15:* d=(17^37)mod29 = (15^7)^37 mod29 = 15^259 mod29 = 15^7 mod29 = 17

*При b=22 та m=43 та w=2:* d=(22^43)mod29 = (2^26)^43 mod29 = 2^1118 mod29 = 2^26 mod29 = 22
*При c=25 та m=43 та w=2:* d=(25^43)mod29 = (2^16)^43 mod29 = 2^688 mod29 = 2^16 mod29 = 25

**6. d≡b^(-1)(mod29); d≡c^(-1)(mod29); (w^j є GF(29).**

4^(-1) ≡ (2^2)^(-1) ≡ 1 * 2^(-2) ≡ 2^28 * 2^(-2) ≡ 2^26 mod 29 ≡ 22
7^(-1) ≡ (2^12)^(-1) ≡ 1 * 2^(-12) ≡ 2^28 * 2^(-12) ≡ 2^16 mod 29 ≡ 25

12^(-1) ≡ (10^21)^(-1) ≡ 1 * 10^(-21) ≡ 18^28 * 10^(-21) ≡ 10^7 mod 29 ≡ 17
17^(-1) ≡ (11^21)^(-1) ≡ 1 * 11^(-21) ≡ 18^28 * 11^(-21) ≡ 11^7 mod 29 ≡ 12

22^(-1) ≡ (26^22)^(-1) ≡ 1 * 26^(-22) ≡ 26^28 * 26^(-22) ≡ 26^6 mod 29 ≡ 4
25^(-1) ≡ (26^20)^(-1) ≡ 1 * 26^(-20) ≡ 26^28 * 26^(-20) ≡ 26^8 mod 29 ≡ 7

**7. Дано p- просте число, вибрати w- первісний елемент поля GF(p), перевірити і довести факт його первісності при p=149; 379; 983.**

p=149, нехай w=13

Знаходимо прості дільники числа p-1=148: d = 2, 37

Для кожного m знаходимо w^m mod p

2^148/2 mod 149 ≡ 102 != 1

2^148/37 mod 149 ≡ 148 != 1

Можна вважати 13 первісним елементом

p=379, нехай w=7

Знаходимо дільники числа p-1=378: d = 2, 3, 7

Для кожного m знаходимо w^m mod p

10^378/2 mod 379 ≡ 378 !≡ 1

10^378/3 mod 379 ≡ 51  !≡ 1

10^378/7 mod 379 ≡ 125 !≡ 1

Число 7 можна вважати первісним елементом

p=983, нехай w=11

Знаходимо дільники числа p-1=982: d = 2, 491

Для кожного m знаходимо w^m mod p

3^982/2 mod 983 ≡ 121 !≡ 1

3^982/491 mod 983 ≡ 982 !≡ 1

Можна вважати 11 первісним елементом