

Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Факультет інформатики та обчислювальної техніки Кафедра інформаційних систем та технологій

Лабораторна робота №3

з дисципліни «Безпека інформаційних систем»

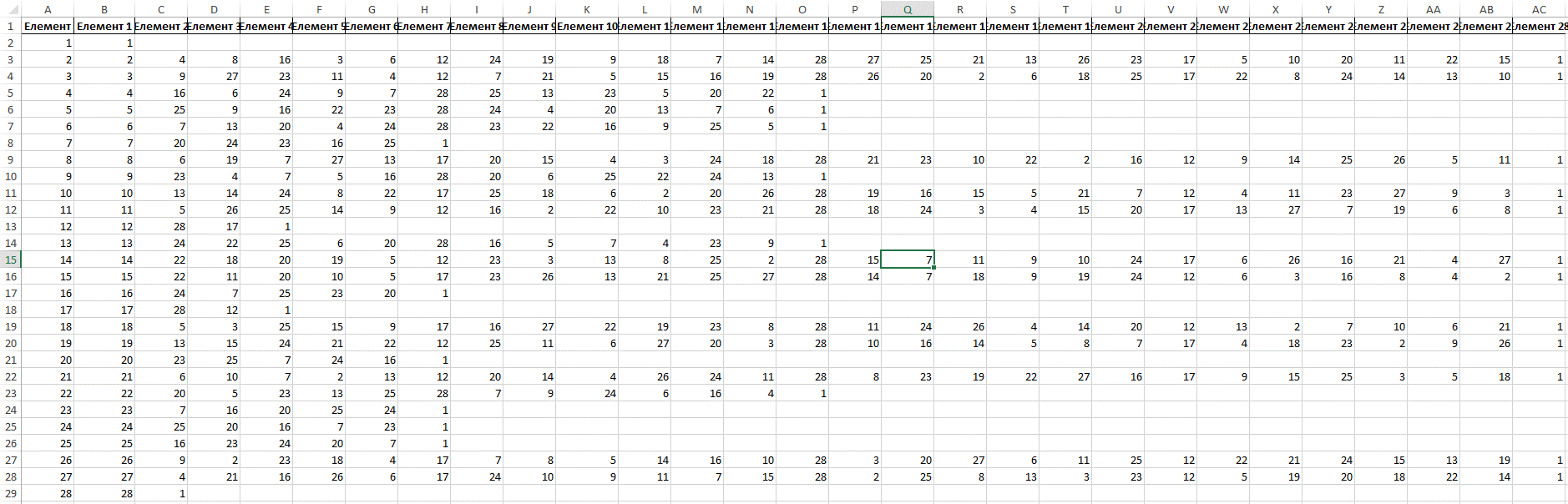
|  |  |
| --- | --- |
| Виконав: | Перевірив: |
| студент групи ІА-23:  Лядський Д.С. | Шимкович Л.Л. |
|  |  |

Київ 2024

|  |
| --- |
| Дослідження арифметичної системи GF(p). Скінченні поля Галуа. |
|  |

**Хід роботи:**

Завдання №1.  Побудувати таблицю мультиплікативних циклів елементів  М29 із GF(29).



Завдання№2.  Виконати наступні операції над елементами поля  GF(p), де р=29; для обчислень брати різні первісні елементи з таблиці мультиплікативних циклів елементів М29 із GF(29).

b,c,d є GF(29),   1.b=4, c=9;    2. b=13, c=16;    3. b=23, c=25.

1. b+c≡d
2. b -c≡d
3. b\*c≡d(mod29),   (w^j є GF(29)
4. b : c≡d(mod29),   (w^j є GF(29))
5. b^m≡d(mod29),   c^m≡d(mod29).    m= 31, 46, 52.
6. d≡b^(-1)(mod29);   d≡c^(-1)(mod29);     (w^j є GF(29).
7. Дано р- просте число, вибрати  w- первісний елемент поля GF(p), перевірити

і довести факт його первісності при  р=139;  271; 617.

**1 – 4** :Виконаємо операції:

Для b=4, c=9:

4 + 9 ≡ 13 (mod 29)

4 - 9 ≡ 24 (mod 29) => 4 – 9 = 4 + 29 – 9 = 24 (mod29)

4 \* 9 ≡ 36 ≡ 7 (mod 29) => 4 \* 9 = 2^2 \* 2^10 = 2^12 (mod29) = 7 (mod29)

4 / 9 ≡ 4 \* 9^(-1) ≡ 4 \* 13 ≡ 52 ≡ 23 (mod 29) => 4 : 9 = 2^2 : 2^10 = 2^-8 = 1 \* 2^-8 = 2^28 \* 2^-8 = 2^20(mod29) = 23

Для b=13, c=16:

13 + 16 ≡ 0 (mod 29)

13 - 16 ≡ 26 (mod 29)

13 \* 16 ≡ 208 ≡ 8 (mod 29)

13 / 16 ≡ 13 \* 16^(-1) ≡ 13 \* 20 ≡ 260 ≡ 27 (mod 29)

Для b=23, c=25:

23 + 25 ≡ 19 (mod 29)

23 - 25 ≡ 27 (mod 29)

23 \* 25 ≡ 575 ≡ 14 (mod 29)

23 / 25 ≡ 23 \* 25^(-1) ≡ 23 \* 7 ≡ 161 ≡ 16 (mod 29)

**5.** Піднесення до степеня m: Для b=4, c=9:

4^31 ≡ 6 (mod 29) => 4^31 = (2^2)^31 = 2^62 = 22\*28+6 = 2^6 =6 (mod 29)

4^46 ≡ 24 (mod 29) => 4^46 = (2^2)^46 = 2^92 = 23\*28+8 = 2^8 = 24

4^52 ≡ 23 (mod 29)

9^31 ≡ (mod 29) => 9^31 = (5^3)^31 = 5^93 = 53\*28+9 = 5^9 = 4 (mod 29)

9^46 ≡ 7 (mod 29)

9^52 ≡ 25 (mod 29)

Для b=13, c=16:

13^31 ≡ 22 (mod 29) => 13^31 = (14^10)^31 = 14^310 = 1411\*28+2 = 14^2 = 22 (mod 29)

13^46 ≡ 25 (mod 29)

13^52 ≡ 7 (mod 29)

16^31 ≡ 7 (mod 29) => 16^31 = (5^2)^31 = 5^62 = 52\*28+6 = 5^6 = 7 (mod 29)

16^46 ≡ 25 (mod 29)

16^52 ≡ 7 (mod 29)

Для b=23, c=25:

23^31 ≡ 16 (mod 29)

23^46 ≡ 20 (mod 29)

23^52 ≡ 16 (mod 29)

25^31 ≡ 23 (mod 29)

25^46 ≡ 24 (mod 29)

25^52 ≡ 23 (mod 29)

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

Використаємо властивість: b\* b-1 = 1(mod p) та властивість формальної 1 за т. Ферма: wp-1 = 1(mod p).

b = 4 = 2110 → d ≡ b-1(mod29) → 21-10 = 1 \* 21-10= 2128 \* 21-10 = 2118 = 22 (mod 29)

c = 9 = 262 → d ≡ c-1(mod29) → 26-2 = 1 \* 26-2 = 2628 \* 26-2 = 2626 = 13 (mod 29)

b = 13 = 2626 → d ≡ b-1(mod29) → 26-26 = 1 \* 26-26 = 2628 \* 26-26 = 82 = 9 (mod 29)

c = 16 = 2612 → d ≡ c-1(mod29) → 26-12 = 1 \* 26-12 = 2628 \* 26-12 = 2616 = 20 (mod 29)

b= 23 = 220 → d ≡ b-1(mod29) → 2-20 = 1 \* 2-20 = 228 \* 2-20 = 28 = 24 (mod 29)

c= 25 = 216 → d ≡ c-1(mod29) → 2-16 = 1 \* 2-16 = 228 \* 2-16 = 212 = 7 (mod 29)

**7** - Дано р- просте число, вибрати w- первісний елемент поля GF(p), перевірити і довести факт його первісності при р=139; 271;617

р=139, w=4→

(p −1) = 139 - 1 = 138

Знаходимо критичні степені: m = 2,3,6,23,46,69,138

Підносимо w в ці степені.

32(mod 139) = 9;

33(mod 139) = 27;

36(mod 139) = 34;

323(mod 139) = 43;

346(mod 139) = 42;

369(mod 139) = 138;

3138(mod 139) = 1;

Очевидно, що 𝑤𝑚 (mod p) ≠ 1 на критичному степені, отже ми довели, що

w = 3 – первісний елемент.

2. р=271, w=7

(p −1) = 271 - 1 = 270

Знаходимо критичні степені: m = 2,3,5,6,9,10,15,18,27,30,45,54,90,135,270

Підносимо w в ці степені.

72(mod 271) = 49;

73(mod 271) = 72;

75(mod 271) = 5;

76(mod 271) = 35;

79(mod 271) = 81;

710(mod 271) = 25;

715(mod 271) = 125;

718(mod 271) = 57;

727(mod 271) = 10;

730(mod 271) = 178;

745(mod 271) = 28;

754(mod 271) = 100;

790(mod 271) = 242;

7135(mod 271) = 1;

Очевидно, що 𝑤𝑚 (mod p) = 1 на критичному степені отже ми довели, що w = 7– не первісний елемент.

3. р=617, w=6

(p −1) = 617- 1 = 616

Знаходимо критичні степені: m = 2,4,7,8,11,14,22,28,44,56,77,88,154,308,616

Підносимо w в ці степені.

62(mod 617) = 36;

64(mod 617) = 62;

67(mod 617) = 435;

68(mod 617) = 142;

611(mod 617) = 439;

614(mod 617) = 423;

622(mod 617) = 217;

628(mod 617) = 616;

644(mod 617) = 197;

656(mod 617) = 1;

Очевидно, що 𝑤𝑚 (mod p) = 1 на критичному степені отже ми довели, що w = 6– не первісний елемент.

**Висновок:** Отже, на цій лабораторній роботі ми розглянули Дослідження арифметичної системи GF(p) та Скінченні поля Галуа..