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:
студент групи ІА-23:
Лядський Д.С.

Перевірив:
Шимкович Л.Л.

Київ 2024

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

Хід роботи:

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

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC
1	Елемент	Елемент 1	Елемент 2	Елемент 3	Елемент 4	Елемент 5	Елемент 6	Елемент 7	Елемент 8	Елемент 9	Елемент 10	лемент 1	лемент 1	лемент 1	лемент 1	лемент 1	лемент 1	лемент 1	лемент 1	лемент 1	лемент 2	лемент 2	лемент 2	лемент 2	лемент 2	лемент 2	лемент 2	лемент 2	лемент 28
2	1	1																											
3	2	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
4	3	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
5	4	4	16	6	24	9	7	28	25	13	23	5	20	22	1														
6	5	5	25	9	16	22	23	28	24	4	20	13	7	6	1														
7	6	6	7	13	20	4	24	28	23	22	16	9	25	5	1														
8	7	7	20	24	23	16	25	1																					
9	8	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
10	9	9	23	4	7	5	16	28	20	6	25	22	24	13	1														
11	10	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
12	11	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
13	12	12	28	17	1																								
14	13	13	24	22	25	6	20	28	16	5	7	4	23	9	1														
15	14	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
16	15	15	22	11	20	10	5	17	23	26	13	21	25	27	28	14	7	18	9	19	24	12	6	3	16	8	4	2	1
17	16	16	24	7	25	23	20	1																					
18	17	17	28	12	1																								
19	18	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
20	19	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
21	20	20	23	25	7	24	16	1																					
22	21	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
23	22	22	20	5	23	13	25	28	7	9	24	6	16	4	1														
24	23	23	7	16	20	25	24	1																					
25	24	24	25	20	16	7	23	1																					
26	25	25	16	23	24	20	7	1																					
27	26	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
28	27	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
29	28	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=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 p- просте число, вибрати w- первісний елемент поля GF(p), перевірити
   і довести факт його первісності при p=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 = 2^{2*28+6} = 2^6 =6 (mod 29)

4^46 ≡ 24 (mod 29) => 4^46 = (2^2)^46 = 2^92 = 2^{3*28+8} = 2^8 = 24

4^52 ≡ 23 (mod 29)

9^31 ≡ (mod 29) => 9^31 = (5^3)^31 = 5^93 = 5^{3*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 = $14^{11*28+2}$ = 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 = 5^{2*28+6} = 5^6 = 7 (mod 29)

$16^{46} \equiv 25 \pmod{29}$

$16^{52} \equiv 7 \pmod{29}$

Для b=23, c=25:

$23^{31} \equiv 16 \pmod{29}$

$23^{46} \equiv 20 \pmod{29}$

$23^{52} \equiv 16 \pmod{29}$

$25^{31} \equiv 23 \pmod{29}$

$25^{46} \equiv 24 \pmod{29}$

$25^{52} \equiv 23 \pmod{29}$

6 - d ≡ b^(-1)(mod29); d ≡ c^(-1)(mod29); (w^j є GF(29)
Використаємо властивість: $b * b^{-1} = 1 (\mathrm{mod}\ p)$ та властивість формальної 1 за т. Ферма: $w^{p-1} = 1 (\mathrm{mod}\ p)$.
$b = 4 = 21^{10} \rightarrow d \equiv b^{-1}(\mathrm{mod}29) \rightarrow 21^{-10} = 1 * 21^{-10} = 21^{28} * 21^{-10} = 21^{18} = 22 \pmod{29}$
$c = 9 = 26^{2} \rightarrow d \equiv c^{-1}(\mathrm{mod}29) \rightarrow 26^{-2} = 1 * 26^{-2} = 26^{28} * 26^{-2} = 26^{26} = 13 \pmod{29}$
$b = 13 = 26^{26} \rightarrow d \equiv b^{-1}(\mathrm{mod}29) \rightarrow 26^{-26} = 1 * 26^{-26} = 26^{28} * 26^{-26} = 8^{2} = 9 \pmod{29}$
$c = 16 = 26^{12} \rightarrow d \equiv c^{-1}(\mathrm{mod}29) \rightarrow 26^{-12} = 1 * 26^{-12} = 26^{28} * 26^{-12} = 26^{16} = 20 \pmod{29}$
$b = 23 = 2^{20} \rightarrow d \equiv b^{-1}(\mathrm{mod}29) \rightarrow 2^{-20} = 1 * 2^{-20} = 2^{28} * 2^{-20} = 2^{8} = 24 \pmod{29}$
$c = 25 = 2^{16} \rightarrow d \equiv c^{-1}(\mathrm{mod}29) \rightarrow 2^{-16} = 1 * 2^{-16} = 2^{28} * 2^{-16} = 2^{12} = 7 \pmod{29}$

7 - Дано p- просте число, вибрати w- первісний елемент поля GF(p), перевірити і довести факт його первісності при p=139; 271;617
p=139, w=4→
$(p - 1) = 139 - 1 = 138$
Знаходимо критичні степені: m = 2,3,6,23,46,69,138
Підносимо w в ці степені.
$3^{2} (\mathrm{mod}\ 139) = 9;$
$3^{3} (\mathrm{mod}\ 139) = 27;$
$3^{6} (\mathrm{mod}\ 139) = 34;$
$3^{23} (\mathrm{mod}\ 139) = 43;$
$3^{46} (\mathrm{mod}\ 139) = 42;$
$3^{69} (\mathrm{mod}\ 139) = 138;$
$3^{138} (\mathrm{mod}\ 139) = 1;$
Очевидно, що w^m (mod p) ≠ 1 на критичному степені, отже ми довели, що

w = 3 – первісний елемент.

2. p=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.

7^2(mod 271) = 49;

7^3(mod 271) = 72;

7^5(mod 271) = 5;

7^6(mod 271) = 35;

7^9(mod 271) = 81;

7^{10}(mod 271) = 25;

7^{15}(mod 271) = 125;

7^{18}(mod 271) = 57;

7^{27}(mod 271) = 10;

7^{30}(mod 271) = 178;

7^{45}(mod 271) = 28;

7^{54}(mod 271) = 100;

7^{90}(mod 271) = 242;

7^{135}(mod 271) = 1;

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

3. p=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.

6^2(mod 617) = 36;

6^4(mod 617) = 62;

6^7(mod 617) = 435;

6^8(mod 617) = 142;

6^{11}(mod 617) = 439;

6^{14}(mod 617) = 423;

6^{22}(mod 617) = 217;

6^{28}(mod 617) = 616;

6^{44}(mod 617) = 197;

6^{56}(mod 617) = 1;

Очевидно, що w^m (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..