4. 역원(inverse)

여기서는 **역원**에 대한 기본적인 개념을 개략적으로 살펴본다.

// 덧셈과 곱셈에서 항등원과 역원

	항등원	역원
덧셈(+)	• 덧셈에서 항등원은 **0** • 2 + 0 = 2	• 2 − 2 = **0** • 덧셈에서 **2**와 **−2**는 역원의 관계
곱셈(×)	• 곱셈에서 항등원은 **1** • 2 × 1 = 2	• 2 × 1/2 = **1** • 곱셈에서 **2**와 **1/2**은 역원의 관계

• **항등원**은 연산 결과가 다시 자신이 되도록 만드는 원소이다.
• **역원**은 연산 결과가 항등원이 되는 두 원소 관계이다.

기출문제 분석

1. 정보보호 시스템에서 사용된 보안 알고리즘 구현 과정에서 곱셈에 대한 역원이 사용된다. 잉여류 Z_{26}에서 법(modular) 26에 대한 7의 곱셈의 역원으로 옳은 것은? [2016년 지방 9급]

① 11 ② 13
③ 15 ④ 17

♤ **법 26에서 곱셈의 역원(RSA 암호시스템)**

• (d × e) mod 26 = 1

(7 × e) mod 26 = 1
↓e = 15일 때, 법 26에 대한 나머지는 1이 된다.
(7 × **15**) mod 26 = 1

• RSA 암호시스템에서 d와 e는 모듈로 Φ(n)에서 곱셈에 대한 역원 관계이다.

정답 : ③

// Z_n과 Z_n^*의 차이점

Z_n	Z_n^*
$Z_5 = \{0, 1, 2, 3, 4\}$	$Z_5^* = \{1, 2, 3, 4\}$
$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$	$Z_7^* = \{1, 2, 3, 4, 5, 6\}$
$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$	$Z_{10}^* = \{1, 3, 7, 9\}$

• Z_n : n으로 나눈 **나머지 집합**이다.

• Z_n^* : n으로 나눈 나머지에서 n과 **서로소 관계인 나머지 집합**이다.(서로소는 gcd = 1)

• Z_n^*에서 n이 **소수**이면, $Z_n^* = Z_n - \{0\} = \{1, 2, 3, \cdots, n-1\}$이다.

예제 1

Z_6과 Z_6^*은? (여기서, 6은 소수가 아니다)

$Z_6 = \{0, 1, 2, 3, 4, 5\}$ → Z_6은 6으로 나눈 나머지의 집합이다.

$Z_6^* = \{1, 5\}$ → Z_6^*은 6으로 나눈 나머지에서 6과 서로소인 나머지 집합이다.

예제 2

Z_{13}과 Z_{13}^*은? (여기서, 13은 소수이다)

$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. 11, 12\}$

→ Z_{13}은 13으로 나눈 나머지의 집합이다.

$Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10. 11, 12\}$

→ Z_{13}^*은 13으로 나눈 나머지에서 13과 서로소인 나머지 집합이다.

// 암호에서 Z_n과 Z_n^*

• Z_n : 암호에서 **덧셈에 대한 역원**이 필요할 때 사용

• Z_n^* : 암호에서 **곱셈에 대한 역원**이 필요할 때 사용

◈ 합동식에서 역원

Z_n = {0, 1, 2, 3, ⋯, n−1}에서 두 수 a, b가 다음을 만족할 때

① a+b≡0 (mod n)	• 두 수 a, b는 서로서로가 **덧셈**에 대한 **역원**이다. • 덧셈에 대한 항등원은 0이다.
② a×b≡1 (mod n)	• 두 수 a, b는 서로서로가 **곱셈**에 대한 **역원**이다. • 곱셈에 대한 항등원은 1이다.

① 모듈러 연산에서 각각의 모든 정수는 덧셈에 대한 역원을 갖는다.
→ 그 정수와 덧셈에 대한 역원의 합은 모듈러 n에 대하여 0과 합동이다.

② 모듈러 연산에서 각 정수는 곱셈에 대한 역원이 있을 수도, 없을 수도 있다.
→ 곱셈에 대한 역원이 있으면, 그 정수와 역원의 곱은 모듈러 n에서 1과 합동이다.

예제

Z_{10} = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}에서 덧셈과 곱셈에 대한 모든 역원 쌍은?

덧셈에 대한 역원 쌍 : (0, 0), (1, 9), (2, 8), (3, 7), (4, 6), (5, 5)
곱셈에 대한 역원 쌍 : (1, 1), (3, 7), (9, 9) → 0, 2, 4, 5, 6, 8은 곱셈에 대한 역원이 없다.

// Z_{10}에 대한 덧셈과 곱셈표

	0	1	2	3	4	5	6	7	8	9
0	**0**	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	**0**
2	2	3	4	5	6	7	8	9	**0**	1
3	3	4	5	6	7	8	9	**0**	1	2
4	4	5	6	7	8	9	**0**	1	2	3
5	5	6	7	8	9	**0**	1	2	3	4
6	6	7	8	9	**0**	1	2	3	4	5
7	7	8	9	**0**	1	2	3	4	5	6
8	8	9	**0**	1	2	3	4	5	6	7
9	9	**0**	1	2	3	4	5	6	7	8

	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	**1**	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	**1**	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	**1**	8	0	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	**1**

다음은 합동식에서 곱셈에 대한 역원을 이해할 수 있는 프로그램이다.

비주얼베이직	C 언어

Private Sub Command1_Click()
  e = 13
  For d = 1 To 60
  Debug.Print d, e * d Mod 60
  Next
End Sub
	void main()
	{
	  int e = 13, d;
	  for(d=1; d<=60; d++)
	  printf("%5d, %5d\n", d, e * d % 60);
	}

e = 13일 때, d = 37				e = 17일 때, d = 53			
1	13	31	43	1	17	31	47
2	26	32	56	2	34	32	4
3	39	33	9	3	51	33	21
4	52	34	22	4	8	34	38
5	5	35	35	5	25	35	55
6	18	36	48	6	42	36	12
7	31	**37**	**1**	7	59	37	29
8	44	38	14	8	16	38	46
9	57	39	27	9	33	39	3
10	10	40	40	10	50	40	20
11	23	41	53	11	7	41	37
12	36	42	6	12	24	42	54
13	49	43	19	13	41	43	11
14	2	44	32	14	58	44	28
15	15	45	45	15	15	45	45
16	28	46	58	16	32	46	2
17	41	47	11	17	49	47	19
18	54	48	24	18	6	48	36
19	7	49	37	19	23	49	53
20	20	50	50	20	40	50	10
21	33	51	3	21	57	51	27
22	46	52	16	22	14	52	44
23	59	53	29	23	31	**53**	**1**
24	12	54	42	24	48	54	18
25	25	55	55	25	5	55	35
26	38	56	8	26	22	56	52
27	51	57	21	27	39	57	9
28	4	58	34	28	56	58	26
29	17	59	47	29	13	59	43
30	30	60	0	30	30	60	0

• 합동식에서 곱셈에 대한 역원은 1이다.

e * d mod 60 = 1