

연 습 문 제 (2.2)

1. 가환환 \mathbb{Z}_m 에서 $a, c \in \mathbb{Z}_m^*$, $b, d \in \mathbb{Z}_m$ 일 때 \mathbb{Z}_m 위의 두 아핀변환

$$T_{a,b} : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m, T_{a,b}(x) = ax + b$$

$$T_{c,d} : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m, T_{c,d}(x) = cx + d$$

에 대하여 $T_{c,d} \circ T_{a,b}$ 는 \mathbb{Z}_m 위의 아핀변환임을 밝혀라.

그리고, 두 아핀변환

$$T_{a,0} : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m, T_{a,0}(x) = ax$$

$$T_{1,b} : \mathbb{Z}_m \longrightarrow \mathbb{Z}_m, T_{1,b}(x) = x + b$$

에 대하여 $T_{a,b} = T_{1,b} \circ T_{a,0}$ 임을 밝혀라.

[풀이] 임의의 $x \in \mathbb{Z}_m$ 에 대하여

$$\begin{aligned} (T_{c,d} \circ T_{a,b})(x) &= T_{c,d}(T_{a,b}(x)) = T_{c,d}(ax + b) \\ &= c(ax + b) + d = cax + cb + d \end{aligned}$$

이고, $(a, m) = (c, m) = 1$ 이므로 $(ca, m) = 1$ 이다(정리 1.2.8). 따라서

$ca \in \mathbb{Z}_m^*$, $cb + d \in \mathbb{Z}_m$ 이므로 $T_{c,d} \circ T_{a,b}$ 는 \mathbb{Z}_m 위의 아핀변환이다.

그리고, 임의의 $x \in \mathbb{Z}_m$ 에 대하여

$$(T_{1,b} \circ T_{a,0})(x) = T_{1,b}(T_{a,0}(x)) = T_{1,b}(ax) = ax + b = T_{a,b}(x)$$

이므로 $T_{a,b} = T_{1,b} \circ T_{a,0}$ 이다.

[참고] 아핀변환을 행렬로 나타낼 수 있다. 실제로, 두 아핀변환의 합성변환과 아핀변환의 역변환은 다음과 같이 두 행렬의 곱과 역행렬에 대응한다.

$$\begin{aligned} \begin{bmatrix} c & d \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} &= \begin{bmatrix} ca & cb + d \\ 0 & 1 \end{bmatrix} \\ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}^{-1} &= \begin{bmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{bmatrix} \end{aligned}$$

3. 가환환 \mathbb{Z}_{26} 위의 아핀변환

$$T_{a,b} : \mathbb{Z}_{26} \rightarrow \mathbb{Z}_{26}, T_{a,b}(x) = ax + b$$

에 대하여 $T_{a,b}(4) = 5$, $T_{a,b}(3) = 6$ 일 때 a 와 b 를 구하여라.

[풀이] 가정에 의하여 다음이 성립한다.

$$4a + b \equiv 5 \pmod{26}$$

$$3a + b \equiv 6 \pmod{26}$$

위의 첫째 합동식에서 둘째 합동식을 빼면

$$a \equiv -1 \equiv 25 \pmod{26}$$

이고 이것을 첫째 합동식에 대입하면 다음 결과를 얻는다.

$$-4 + b \equiv 5 \pmod{26}$$

$$b \equiv 9 \pmod{26}$$

그러므로 $a = 25$, $b = 9$ 이다.

4. 다음 일차합동식의 해를 구하여라.

$$(1) 19x \equiv 3 \pmod{26}$$

[풀이] 오른쪽 표에 의하여

$$(26, 19) = 1$$

이고

$$26 \cdot (-8) + 19 \cdot 11 = 1$$

이므로 다음이 성립한다.

$$26 \cdot (-24) + 19 \cdot 33 = 3$$

$$19 \cdot 33 \equiv 3 \pmod{26}$$

$$19 \cdot 7 \equiv 3 \pmod{26}$$

따라서 일차합동식 $19x \equiv 3 \pmod{26}$

의 해는 $x \equiv 7 \pmod{26}$ 이다.

1	26	19	2
	<u>19</u>	<u>14</u>	
1	7	<u>5</u>	2
	<u>5</u>	<u>4</u>	
2	2	<u>1</u>	
	<u>2</u>		
	0		

1	2	1	2		
1	0	1	-2	3	-8
0	1	-1	3	-4	11

5. 다음 두 일차합동식을 동시에 만족키는 해를 구하여라.

$$(1) 4a + b \equiv 11 \pmod{26}, \quad a + b \equiv 5 \pmod{26}$$

[풀이] $4a + b \equiv 11 \pmod{26}, \quad a + b \equiv 5 \pmod{26}$ 이므로

$$3a \equiv 6 \pmod{26}$$

이고 따라서 $a \equiv 2 \pmod{26}$ 이다.

이 결과를 둘째 합동식에 대입하면, $b \equiv 5 - 2 \equiv 3 \pmod{26}$ 이므로
구하는 해는 다음과 같다.

$$a \equiv 2 \pmod{26}, \quad b \equiv 3 \pmod{26}$$

6. $y \equiv 23x + 10 \pmod{26}$ 일 때,

$$x \equiv cy + d \pmod{26}, \quad 0 \leq c \leq 25, \quad 0 \leq d \leq 25$$

인 정수 c, d 를 구하여라.

[풀이] 오른쪽 표에 의하여

$$(26, 23) = 1,$$

$$26 \cdot 8 + 23 \cdot (-9) = 1$$

이므로 다음이 성립한다.

$$23 \cdot (-9) \equiv 1 \pmod{26}$$

$$\text{즉 } 23 \cdot 17 \equiv 1 \pmod{26}$$

한편, $y \equiv 23x + 10 \pmod{26}$ 이므로

$$23x \equiv y - 10 \pmod{26}$$

이고 따라서

$$23 \cdot 17x \equiv 17y - 10 \cdot 17 \pmod{26}$$

$$x \equiv 17y - 10 \cdot 17 \pmod{26}$$

이므로 다음이 성립한다.

$$x \equiv 17y - 14 \equiv 17y + 12 \pmod{26}$$

그러므로 $c = 17, \quad d = 12$ 이다.

$$\begin{array}{r|rr|r} 1 & 26 & 23 & 7 \\ & 23 & 21 & \\ 1 & 3 & 2 & 2 \\ & 2 & 2 & \\ & 1 & 0 & \end{array}$$

1	7	1		
1	0	1	-7	8
0	1	-1	8	-9

연 습 문 제 (2.3)

1. 다음 치환의 역치환을 구하여라.

$$(1) \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 4 & 2 \end{pmatrix} \quad (2) \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 7 & 1 & 5 & 4 & 2 \end{pmatrix}$$

[풀이]

$$(1) \sigma^{-1} = \begin{pmatrix} 3 & 1 & 5 & 4 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$$

$$(2) \sigma^{-1} = \begin{pmatrix} 6 & 3 & 7 & 1 & 5 & 4 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 2 & 6 & 5 & 1 & 3 \end{pmatrix}$$

2. 보기 2.3.3 에서 유한수열을 치환

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}$$

를 이용하여 변환시켜라.

[풀이] 유한수열 (*)를 다음과 같이 처음부터 차례로 5 개씩 묶는다.

$$(*) \quad 18 \ 4 \ 13 \ 3 \ 12 : 4 \ 0 \ 3 \ 14 \ 2 : 20 \ 12 \ 4 \ 13 \ 19$$

이제 열쇠 K 를 치환

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 2 & 3 \end{pmatrix}$$

으로 택하여 함수

$$E_K : \mathbb{Z}_{26}^5 \longrightarrow \mathbb{Z}_{26}^5, \quad E_K(x_1, x_2, x_3, x_4, x_5) = (x_1, x_5, x_4, x_2, x_3)$$

를 이용하면 (*)는 다음과 같은 유한수열로 변환된다.

$$18 \ 12 \ 3 \ 4 \ 13 : 4 \ 2 \ 14 \ 0 \ 3 : 20 \ 19 \ 13 \ 12 \ 4$$

연 습 문 제 (2.5)

1. 素數
- $p = 13$
- 과 정수
- $e = 5$
- 에 대하여

$$ed \equiv 1 \pmod{p-1}, \quad 1 \leq d < p-1$$

인 정수 d 를 구하여라. 그리고, $a = 3$ 에 대하여

$$b \equiv a^e \pmod{p}, \quad 1 \leq b < p$$

인 정수 b 를 구하여라.

[풀이] 오른쪽 표에 의하여

$$12(-2) + 5 \cdot 5 = 1$$

$$5 \cdot 5 \equiv 1 \pmod{12}$$

$$\begin{array}{r|rr} 2 & 12 & 5 & 2 \\ & 10 & 4 & \\ \hline 2 & 2 & 1 & \\ & 2 & & \\ \hline & 0 & & \end{array}$$

2	2		
1	0	1	-2
0	1	-2	5

이므로 $d = 5$ 이다. 또, $a = 3$ 일 때,

$$b \equiv a^e \equiv 3^5 \equiv 3^2 \cdot 3^3 \equiv 9 \cdot 1 \equiv 9 \pmod{13}$$

이므로 $b = 9$ 이다.

2. 素數
- $p = 19$
- 과 정수
- $e = 5$
- 에 대하여

$$ed \equiv 1 \pmod{p-1}, \quad 1 \leq d < p-1$$

인 정수 d 를 구하여라. 그리고, $a = 3$ 일 때,

$$b \equiv a^e \pmod{p}, \quad 1 \leq b < p$$

인 정수 b 를 구하여라.

[풀이] 오른쪽 표에 의하여

$$18 \cdot 2 + 5 \cdot (-7) = 1$$

$$5 \cdot (-7) \equiv 1 \pmod{18}$$

$$\begin{array}{r|rr} 3 & 18 & 5 & 1 \\ & 15 & 3 & \\ \hline 1 & 3 & 2 & 2 \\ & 2 & 2 & \\ \hline & 1 & 0 & \end{array}$$

3	1	1		
1	0	1	-1	2
0	1	-3	4	-7

이므로 $5 \cdot 11 \equiv 1 \pmod{18}$ 이고

따라서 $d = 11$ 이다. 또, $a = 3$ 일 때,

$$b \equiv a^e \equiv 3^5 \equiv 3^2 \cdot 3^3 \equiv 9 \cdot 8 \equiv 72 \equiv 15 \pmod{19}$$

이므로 $b = 15$ 이다.