2.1 합동과 합동류

정리 2.1.1 a, b, n은 $n > 0$인 정수라 하자.
$n|(a-b)$이면 a가 n을 법으로 하여 b와 합동이다 (a is congruent to b modulo n)라고 한다. 이 때, 기호 $a \equiv b \pmod{n}$으로 쓴다.

▌보기 2.1.1 ▌ $17 \equiv 5 \pmod 6$. 왜냐면, 6은 17-5=12의 약수이기 때문이다. 비슷하게, $4 \equiv 25 \pmod 7$. 왜냐면, 7은 4-25=-21의 약수이기 때문이다. 역시 $6 \equiv -4 \pmod 5$. 왜냐면, 5는 6-(-4)=10의 약수이기 때문이다. ■

주목 2.1.1 "$a \equiv b \pmod{n}$"에서, 기호 "$\equiv$"과 "$\pmod{n}$"은 실제로 하나의 기호의 부분들이다. "$a \equiv b$"자체로는 의미가 없다. 어떤 교제는 "$a \equiv b \pmod{n}$"대신에 "$a \equiv_n b$"를 쓴다.

우리는 이제 같음이 다음의 동치관계의 모든 조건을 만족함을 안다 :

반사한다 : 그들 정수 a에 대하여 $a = a$,
대칭이다 : $a = b$면, $b = a$,
이동한다 : $a = b$이고 $b = c$면, $a = c$.

정리 2.1.2 n은 양의 정수라하자. 모든 $a, b, c \in \mathbb{Z}$에 대하여,
(1) $a \equiv a \pmod{n}$.
(2) $a \equiv b \pmod{n}$이면, $b \equiv a \pmod{n}$.
(3) $a \equiv b \pmod{n}$이고 $b \equiv c \pmod{n}$이면, $a \equiv c \pmod{n}$.

►증명◄
(1) $a - a = 0$ 이고 $n|0$. 따라서 $a \equiv a \pmod{n}$.
(2) $a \equiv b \pmod{n}$라 가정하자. 그러면 $n|(a-b)$. 그래서
$k \in \mathbb{Z}$가 존재하여 $a - b = nk$이다. 그러므로
$b - a = -(a-b) = -nk = n(-k)$이고 $-k \in \mathbb{Z}$이다.

그래서 $n|(b-a)$. 따라서 $b \equiv a \pmod{n}$.
(3) $a \equiv b \pmod{n}$이고 $b \equiv c \pmod{n}$이라 가정하자. 그러면
$\exists\, k, t \in \mathbb{Z}$ $s.t.$ $a - b = nk$이고 $b - c = nt$.
그래서 $(a-b)+(b-c) = nk + nt$, $a - c = n(k+t)$.
$k + t \in \mathbb{Z}$이므로, $n|(a-c)$. 따라서 $a \equiv c \pmod{n}$. ■

여러 가지 본질적인 셈과 대수적인 교묘한 처리는 다음의 중요한 사실에 달려있다 :

$a = b$이고 $c = d$면, $a + c = b + d$이고 $ac = bd$.

정리 2.1.3 $a \equiv b(\text{mod } n)$이고 $c \equiv d(\text{mod } n)$이라 하자. 그러면

(1) $a+c \equiv b+d(\text{mod } n)$.

(2) $ac \equiv bd(\text{mod } n)$.

►증명◄

(1) 합동의 정의에 의하여,

$\exists\, k, t \in \mathbb{Z}\ \ s.t.\ a-b=nk$이고 $c-d=nt$.

그러면

$$(a-b)+(c-d) = nk+nt,$$
$$a+c-b-d = n(k+t),$$
$$(a+c)-(b+d) = n(k+t).$$

그래서 $n|[(a+c)-(b+d)]$.

따라서 $a+c \equiv b+d(\text{mod } n)$.

(2) $$\begin{aligned} ac-bd &= ac+0-bd \\ &= ac-bc+bc-bd \\ &= (a-b)c+b(c-d) \\ &= (nk)c+b(nt) = n(kc+bt) \end{aligned}$$

그러므로 $n|(ac-bd)$. 따라서 $ac \equiv bd(\text{mod } n)$. ■

정의 2.1.4

a와 n은 $n>0$인 정수라 하자. n을 법으로 a와 합동인 모든 정수들의 집합을 **n을 법으로 하는 a의 합동류**(the congruence class of a mod n)라하고 기호 $[a]$로 쓴다. 따라서

$$[a]=\{b \in \mathbb{Z}: b \equiv a(\text{mod } n)\}.$$

$$b \equiv a\ (\text{mod} n) \Leftrightarrow \exists\, k \in \mathbb{Z}\ \ s.t.\ b-a=kn$$
$$\Leftrightarrow \exists\, k \in \mathbb{Z}\ \ s.t.\ b=a+kn.$$

그러므로

$$[a]=\{b \in \mathbb{Z}: b \equiv a(\text{mod } n)\}$$
$$=\{b \in \mathbb{Z}: \exists\, k \in \mathbb{Z}\ \ s.t.\ b=a+kn\}$$
$$=\{a+kn : k \in \mathbb{Z}\}.$$

▌보기 2.1.2▐ 5를 법으로 하는 합동에서,

$[9]=\{9+5k: k \in \mathbb{Z}\}=\{9,\ 9\pm5,\ 9\pm10,\ 9\pm15,\cdots\}$

$=\{\cdots,\ -11,\ -6,\ -1,\ 4,\ 9,\ 14,\ 19,\ 24,\ \cdots\}$. ■

▌보기 2.1.4▐ 3을 법으로 하는 합동에서, 합동류

[2]={…, -7, -4, -1, 2, 5, 8, …}.

그러나 [-1]=[2]임에 주목하라. 왜냐면,

[-1]={-1+3k: $k\in\mathbb{Z}$}={…, -7, -4, -1, 2, 5, 8,…}

이기 때문이다.

더욱이, $2\equiv -1 \pmod 3$.

■

정리 2.1.5

$a\equiv c \pmod n \Leftrightarrow [a]=[c]$.

A와 C가 두 집합이면, 보통 세 가지 가능성이 있다 : A와 C가 서로소, 또는 A=C 또는 $A\cap C\neq\varnothing$이고 $A\neq C$. 그러나 합동류에서는 두 가지 가능성만 있다.

따름정리 2.1.5−1

n을 법으로 하는 두 합동류는 서로소이거나 또는 같다.

►증명◄

$[a]$와 $[c]$가 서로소면, 증명할 필요가 전혀 없다.

$[a]\cap[c]\neq\varnothing$라 가정하자. 그러면

$\exists b\in\mathbb{Z}\ \ s.t.\ \ b\in[a]$ 이고 $b\in[c]$.

합동류의 정의에 의하여, $b\equiv a \pmod n$이고 $b\equiv c \pmod n$.

합동관계는 동치관계이므로, $a\equiv c \pmod n$. 따라서

정리2.1.5에 의하여, $[a]=[c]$. ■

따름정리 2.1.5−2

n을 법으로 하는 서로 다른 합동류는 꼭 n개 있다. 즉,

$[0],[1],[2],\cdots,[n-1]$.

►증명◄ 우리는 먼저 0,1,2,…,n-1 중의 어느 두 개도 n을 법으로 하여 합동이 아님을 주장한다. 이것을 보이기 위하여 $0\le s<t<n$이라 가정한다. 그러면 $t-s$는 $0<t-s<n$인 정수다. $n\nmid(t-s)$이므로, $t\not\equiv s \pmod n$. 그래서 $[t]\neq[s]$. 그러므로 정리2.1.5에 의하여, 합동류 $[0],[1],[2],\cdots,[n-1]$은 모두 다르다. 이 증명을 완성하기 위하여, 우리는 모든 합동류가 이 n개의 합동류 중의 하

나임을 보여야 한다. $a \in \mathbb{Z}$를 임의로 택하자. 그러면, 나눗셈의 알고리즘에 의하여, $\exists$꼭하나의 $q, r \in \mathbb{Z}$ $s.t.$ $a = nq + r$이고 $0 \le r < n$. 그래서 $a - r = qn$. 즉, $n \mid (a-r)$. 그러므로 $a \equiv r \pmod{n}$. 정리2.1.5에 의하여, $[a] = [r]$. 따라서, $0 \le r < n$이므로, $[a]$는 $[0], [1], [2], \cdots, [n-1]$중의 하나다. ■

정의 2.1.6

n을 법으로 하는 모든 합동류들의 집합을 ("$\mathbb{Z}$법n($\mathbb{Z}$ mod n)" 으로 읽게 되는) $\mathbb{Z}_n$으로 표시한다.

여기서 주의해야할 여러 가지 점이 있다. $\mathbb{Z}_n$의 원들은 류(class)들이지, 하나의 정수가 아니다. 그래서 명제 $[5] \in \mathbb{Z}_n$은 참이지만, 명제 $5 \in \mathbb{Z}_n$은 참이 아니다. 더욱이, $\mathbb{Z}_n$의 모든 원은 여러 가지 다른 방법으로 표시될 수 있다. 예로써,

$2 \equiv 5 \pmod{3}$, $2 \equiv -1 \pmod{3}$, $2 \equiv 14 \pmod{3}$.

그러므로 정리2.1.5에 의하여, $\mathbb{Z}_3$에서, [2]=[5]=[-1]=[14]. 비록 $\mathbb{Z}_n$의 각 원(즉, 각 합동류)이 무한히 많은 다른 표시들을 갖질지라도, 사실상 집합 $\mathbb{Z}_n$은 꼭 n개의 원을 갖는다고 말하는, 따름정리2.1.5-2에 의하여, 유한개의 다른 류 들만이 존재한다.

▌보기 2.1.5 ▌ 집합 $\mathbb{Z}_3$은 세 개의 원 [0],[1]과[2]로 이루어진다. ■

예제 | 2.1.1 $a \equiv b \pmod{n} \Leftrightarrow$ **n으로 나눌때 a와 b는 같은 나머지를 갖는다. 이를 증명하라.**

►풀이◄ 나눗셈 알고리즘에 의하여, $\exists$유일한 $p, q, r, s \in \mathbb{Z}$ $s.t.$ $a = qn + r$, $0 \le r < n$ ... ① 이고 $b = pn + s$, $0 \le s < n$ ... ②

($\Rightarrow$) : $a \equiv b \pmod{n}$라 가정하자. 그러면 $n \mid (a-b)$. 그래서 $\exists k \in \mathbb{Z}$ $s.t.$ $a - b = nk$. ①과 ②에서 $nk = (qn + r) - (pn + s)$ 즉, $r - s = (k - q + p)n$ 또는 $n \mid (r-s)$. 그런데, $r < n$ 이고 $s < n$이므로, $|r - s| < n$.

그러므로 $r-s=0$. 따라서 $r=s$.

($\Leftarrow$) : $r=s$라 가정하자. 그러면, ①과②에서,

$a-b=n(q-p)$ $q-r\in\mathbb{Z}$. 그러므로

$n|(a-b)$. 따라서, $a\equiv b(\text{mod } n)$. ■

예제 | 2.1.2 $k\equiv 1(\text{mod } 4)$**이면** $6k+5\equiv b(\text{mod } 4)$**이다. 이 때,** b**의 가장 작은 양의 정수 값은?**

(가) 1 (나) 2 (다) 3 (라) 4 (마) 5

►풀이◄ $k\equiv 1(\text{mod } 4)$라 가정하자. 그러면 $4|(k-1)$, 즉, $\exists m\in\mathbb{Z}$ $s.t.$ $k-1=4m$ 그래서 $6k+5=24m+11=4(6m+2)+3$ 또는 $(6k+5)-3=4(6m+2)$. 그러므로 $(6k+5)\equiv 3(\text{mod } 4)$. 따라서, $b=3$

예제 | 2.1.3 **합동 방정식** $2x\equiv 3(\text{mod } 5)$**의 모든 해를 구하라.**

►풀이◄ $2x\equiv 3(\text{mod } 5)\Leftrightarrow 5|(2x-3)$.그러면 $x=4$는 $2x\equiv 3(\text{mod } 4)$의 특별한 해이다. 이제

$A=\{a\in\mathbb{Z} : a\equiv 4 \pmod 5\}$

라 하고 임의로 $a\in A$를 택하자. 그러면,

$a\equiv 4(\text{mod } 5)$. 그래서 $\exists u\in\mathbb{Z}$ $s.t.$ $a-4=5\mu$.

그러므로 $2a-3=2(5\mu+4)-3=5(2\mu+1)$, 즉, $5|(2a-3)$.

따라서, a는 $2x\equiv 3(\text{mod } 5)$의 해이다. ■

2.2 합동류의 계산

유한집합 $\mathbb{Z}_n$은 무한집합 $\mathbb{Z}$와 밀접하게 관계된다. 그래서 $\mathbb{Z}_n$에서 덧셈(addition)과 곱셈(multiplication)을 정의해보자.

류$[a]$와$[c]$의 합(sum)은 $a+c$를 포함하는 류 또는,

기호로, $[a]\oplus[c]=[a+c]$

다. 여기서 류들의 덧셈을 보통의 정수들의 덧셈과 구별하기 위하여 $\oplus$로 나타낸다.

우리는 곱셈에 대하여 비슷한 임시의 정의를 시도할 수 있다:

$[a]$와 $[c]$의 곱(product)은 ac를 포함하는 류다:

$$[a]\odot[c]=[ac].$$

여기서 $\odot$은 류들의 곱을 나타낸다.

▌보기 2.2.1▐ $\mathbb{Z}_5$에서,

$[3]\oplus[4]=[3+4]=[7]=[2]$이고

$[3]\odot[2]=[3\cdot 2]=[6]=[1].$

■

정리 2.2.1

$\mathbb{Z}_n$에서 $[a]=[b]$이고 $[c]=[d]$면, $[a+c]=[b+d]$이고 $[ac]=[bd]$.

►증명◄ $[a]=[b]$이고 $[c]=[d]$라 가정하자. 그러면, 정리2.1.5에 의하여, $a\equiv b(\mathrm{mod}n)$이고 $c\equiv d(\mathrm{mod}n)$. 그래서, 정리2.1.4에 의하여, $a+c\equiv b+d(\mathrm{mod}n)$ 이고 $ac\equiv bd(\mathrm{mod}n)$.

따라서 다시 정리2.1.4에 의하여,

$[a+c]=[b+d]$이고 $[ac]=[bd]$. ■

정의 2.2.2 $\mathbb{Z}_n$에서 덧셈과 곱셈은 다음과 같이 정의 된다:

$[a]\oplus[c]=[a+c]$ 이고 $[a]\odot[c]=[ac]$.

▌보기 2.2.2▐ 여기서 $\mathbb{Z}_5$에 대한 완전한 덧셈과 곱셈표가 있다(이 계산이 옳은가를 확인하라):

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3],

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1].

또한 다음은 $\mathbb{Z}_6$에 대한 연산표다:

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4],

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

이 두 셈 계산의 성질을 $\mathbb{Z}$의 잘 알려진 성질과 비교하고 싶다. $\mathbb{Z}$에서 계산에 대한 중요한 사실들은 다음과 같다. 모든 $a, b, c \in \mathbb{Z}$에 대하여:

1. $a, b \in \mathbb{Z}$이면 $a+b \in \mathbb{Z}$. [덧셈에 대하여 닫힘]
2. $a+(b+c)=(a+b)+c$. [결합적인 덧셈]
3. $a+b=b+a$. [교환적인 덧셈]
4. $a+0=a=0+a$. [덧셈의 항등원]
5. 각 $a \in \mathbb{Z}$에 대하여 방정식 $a+x=0$은 $\mathbb{Z}$에서 하나의 해를 갖는다.
6. $a, b \in \mathbb{Z}$이면, $ab \in \mathbb{Z}$. [곱셈에 대하여 닫힘]
7. $a(bc)=(ab)c$. [결합적인 곱셈]

8. $a(b+c)=ab+ac$이고 $(a+b)c=ac+bc$. [분배법칙]
9. $ab=ba$. [교환적인 곱셈]
10. $a \cdot 1=a=1 \cdot a$. [곱셈의 항등원]
11. $ab=0$이면, $a=0$ 또는 $b=0$.

보기 2.2.2에 있는 표를 사용함으로써, 여러분은 위의 성질들 중의 처음 10가지가 $\mathbb{Z}_5$와 $\mathbb{Z}_6$에서 성립하고 성질11은 $\mathbb{Z}_5$에서는 성립하지만 $\mathbb{Z}_6$에서는 실패함을 확인할 수 있다.

그러나 표를 사용하는 것은 그다지 효과적인 증명 방법(특히 결합성질과 분배성질을 증명하는데)이 아니다. 그러므로 성질 1~10이 $\mathbb{Z}_n$에 대하여 성립하는 증명은 $\mathbb{Z}_n$에서의 두 연산과 이러한 성질들이 $\mathbb{Z}$에서 성립한다고 알려진 사실 들에 근거하게 된다.

정리 2.2.2 임의의 류 $[a], [b], [c] \in \mathbb{Z}_n$에 대하여,

1. $[a] \in \mathbb{Z}_n$이고 $[b] \in \mathbb{Z}_n$이면, $[a] \oplus [b] \in \mathbb{Z}_n$.
2. $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$.
3. $[a] \oplus [b] = [b] \oplus [a]$.
4. $[a] \oplus [0] = [a] = [0] \oplus [a]$.
5. 각 $[a] \in \mathbb{Z}_n$에 대하여, 방정식 $[a] \oplus X = [0]$은 $\mathbb{Z}_n$에서 하나의 해를 갖는다.

6. $[a]\in\mathbb{Z}_n$이고 $[b]\in\mathbb{Z}_n$이면, $[a]\odot[b]\in\mathbb{Z}_n$.
7. $[a]\odot([b]\odot[c])=([a]\odot[b])\odot[c]$.
8. $[a]\odot([b]\oplus[c])=[a]\odot[b]\oplus[a]\odot[c]$이고 $([a]\oplus[b])\odot[c]=[a]\odot[c]\oplus[b]\odot[c]$.
9. $[a]\odot[b]=[b]\odot[a]$.
10. $[a]\odot[1]=[a]=[1]\odot[a]$.

▸증명◂ 성질 1과 6은 $\mathbb{Z}_n$에서 $\oplus$과$\odot$의 정의의 직접적일 결과다.

성질 2를 증명하기 위하여, 덧셈의 정의에 의하여,

$$[a]\oplus([b]\oplus[c])=[a]\oplus[b+c]=[a+(b+c)]$$

임에 주목하라. $\mathbb{Z}$에서, 우리는 $a+(b+c)=(a+b)+c$임을 안다. 그래

서 이 정수들의 류들은 $\mathbb{Z}_n$에서 같아야만 한다. 즉,

$$[a+(b+c)]=[(a+b)+c].$$

따라서, $\mathbb{Z}_n$에서 덧셈의 정의에 의하여,

$$[(a+b)+c]=[a+b]\oplus[c]=([a]\oplus[b])\oplus[c].$$

성질 3,7,8과 9의 증명은 비슷하다.

성질 4와 10은 직접적인 계산에 의하여 증명된다. 예컨대,

$$[a]\odot[1]=[a\cdot 1]=[a].$$

성질5에 대하여 $[a]\oplus[-a]=[a+(-a)]=[0]$이므로, $X=[-a]$가 주어진 방정식의 하나의 해임을 알기는 쉽다. ■

새로운 표시법

$\mathbb{Z}_n$을 다루고 있을 때 문맥이 분명할 때는 언제나, 우리는 류표시법 "$[a]$" 대신에 간단히 "a"로 쓸 것이다. $\mathbb{Z}_6$에서, 예컨대, 비록 6과 0이 다른 정수면 6=0은 의미가 없을지라도, 우리는 $\mathbb{Z}_6$의 류들에 대하여 확실히 성립하는 6=0 이라 말 할 수 있다. 우리는 $\mathbb{Z}_n$에서 덧셈과 곱셈에 대하여 각각 보통의 "+"기호 와 "·"기호를 사용할 것이다. 예로써, $\mathbb{Z}_5$에서, 우리는

4+1=0 또는 3·4=2 또는 4+4=3

과 같이 쓸 수 있다. 이 사용법이 혼동을 야기시킬 수 있는 경우에, 우리는 류들의 표시법으로 돌아갈 것이다.

▌보기 2.2.3 ▐ 새로운 표시법에서, $\mathbb{Z}_3$에 대한 덧셈과 곱셈표는 다음과 같다 :

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1.

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1.

■

보통의 계산에서 사용되는 같은 지수표시법이 역시 $\mathbb{Z}_n$에서 편리하다. $a \in \mathbb{Z}_n$이고 k가 양의 정수면, a^k은 $\mathbb{Z}_n$에서 곱 $aaa\cdots a$(k개 인수)를 나타낸다.

보기 2.2.4 $\mathbb{Z}_5$에서 $3^2 = 3 \cdot 3 = 4$이고 $3^4 = 3 \cdot 3 \cdot 3 \cdot 3 = 1$. ■

주목 : 지수들은 보통의 정수다 - $\mathbb{Z}_n$의 원이 아니다. $\mathbb{Z}_3$에서, 예컨대 $2^4 = 2 \cdot 2 \cdot 2 \cdot 2 = 1$이고 $2^1 = 2$. 비록 $\mathbb{Z}_3$에서 $4 = 1$일

지라도, $2^4 \neq 2^1$.

예제 | 2.2.1 $\mathbb{Z}_2$**의 덧셈과 곱셈표를 만들어라.**

►풀이◄

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

▪

예제 | 2.2.2 $\mathbb{Z}_5$**에서 방정식** $x+x+x+x+x=0$**의 해집합은?**

(가) $\mathbb{Z}_5$ (나) {0} (다) {0,1}

(라) {0,1,2} (마) {0,1,2,3}

►풀이◄ (가). ■

예제 | 2.2.3 $\mathbb{Z}_5$**에서** $(a+b)^5$**을 계산하라.**

►풀이◄

$$(a+b)^5 = a^5 + \binom{5}{1}a^4b + \binom{5}{2}a^3b^2 + \binom{5}{3}a^2b^3 + \binom{5}{4}ab^4 + b^5$$

$$= a^5 + \frac{5!}{1!(5-1)!}a^4b + \frac{5!}{2!(5-2)!}a^3b^2 + \frac{5!}{3!(5-3)!}a^2b^3$$

$$+ \frac{5!}{4!(5-4)!}ab^4 + b^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

$$= a^5 + b^5$$ ■

2.3 p가 소수일 때 $\mathbb{Z}_p$의 구조

$\mathbb{Z}_n$중의 어떤 것은 $\mathbb{Z}$의 멋있는 성질들을 공유하지 못한다. 예컨대, $\mathbb{Z}$에서 0이 아닌 정수들의 곱은 언제나 0이 아니다. 그러나 $\mathbb{Z}_6$에서, 비록 $2 \neq 0$이고 $3 \neq 0$일지라도 $2 \cdot 3 = 0$이다.

$a \neq 0$일 때,
방정식 $ax = 1$이 $\mathbb{Z}$에서 해를 갖는다 $\Leftrightarrow a = \pm 1$.

그러나 $\mathbb{Z}_5$에 대한 곱셈표는 임의의 $a \neq 0$에 대하여, 방정식 $ax = 1$은 $\mathbb{Z}_5$에서 해를 가짐을 보여 준다 ; 예로써,

$x = 3$은 $2x = 1$의 해이고,
$x = 4$는 $4x = 1$의 해다.

더 일반적으로, n이 소수일때는 언제나, $\mathbb{Z}_n$은 특별한 성질들을 갖는다 :

정리 2.3.1 $p > 1$은 정수라 하자. 그러면 다음의 조건들은 논리적 으로 같다 :

(1) p는 소수다.
(2) 임의의 $0 \neq a \in \mathbb{Z}_n$에 대하여, 방정식 $ax = 1$은 $\mathbb{Z}_p$ 에서 해를 갖는다.
(3) $\mathbb{Z}_p$에서, $ab = 0$ 이면, $a = 0$ 또는 $b = 0$.

이 정리의 증명은 $\mathbb{Z}_n$을 포함하는 명제들을 증명하기 위하여 두 가지 기초적인 기술을 설명 한다 :

(i) $\mathbb{Z}_n$에서 방정식을 $\mathbb{Z}$에서 논리적으로 같은 합동 명제로 바꾼다. 그러면 $\mathbb{Z}$에서 합동과 셈의 성질들이 사용될 수 있다. $\mathbb{Z}_n$의 원에 대한 원래의 표시법이 혼동을 피하기 위하여 필요할 수 있다.

(ii) $\mathbb{Z}$에서 계산을 포함하지 않고, 직접 $\mathbb{Z}_n$의 계산 성질을 사용한다. 이 경우에, $\mathbb{Z}_n$의 원래의 표시법은 필요 없다.

정리 2.3.1의 증명

(1)⇒(2): 우리는 첫 번째 기술을 사용한다.

p는 소수라 가정하고 $\mathbb{Z}_p$의 임의원 $[a]\neq[0]$를 택하자. 그러면, 정리2.1.5에 의하여, $\mathbb{Z}$에서 $a\not\equiv 0(\mathrm{mod}p)$. 그래서, 합동의 정의에 의하여, $p\nmid a$. 그래서 a와 p의 gcd는 p의 양의 약수고 그러므로 p또는 1이어야만 한다. 역시 $(a,p)|a$이고 $p\nmid a$이므로, $(a,p)=1$이어야만 한다. 정리1.2.3에 의하여,

$$\exists\, u,v\in\mathbb{Z}\quad s.t.\quad au+pv=1.$$

그러면 $au-1=p(-v)$. 그래서 $au\equiv 1(\mathrm{mod}\ p)$. 그러므로, 정리 2.1.5에 의하여, $\mathbb{Z}_p$에서 $[au]=[1]$. 그런데 $[a][u]=[au]=[1]$.

따라서 $x=[u]$는 $[a]x=[1]$의 해다. ■

(2)⇒(3): 우리는 두 번째 기술을 사용한다. 조건(2)가 성립하고 $\mathbb{Z}_p$에서 $ab=0$이라 가정하자. $a=0$이면, 증명할 것이 없다. $a\neq 0$이면, 조건(2)에 의하여, $\exists\, u\in\mathbb{Z}_p\ s.t.\ au=1$. 그러면

$$0=u\bullet 0=u(ab)=(ua)b=(au)b=1\bullet b=b.$$

따라서, 모든 경우에, $a=0$또는 $b=0$.

(3)⇒(1): 첫 번째 기술로 돌아간다. 조건(3)이 성립한다고 가정하고, a는 p의 임의의 약수, 즉, $p=ab$라 하자. p가 소수임을

증명하기 위하여, 우리는 $a=\pm 1$ 또는 $\pm p$임을 보여야만 한다. $p=ab$ 이므로, $ab\equiv 0(\mathrm{mod}\ p)$. 그래서 정리2.1.5에 의하여, $\mathbb{Z}_p$에서 $[a][b]=[ab]=[0]$. 그러므로, 조건(3)에 의하여, $[a]=[0]$또는 $[b]=[0]$. $[a]=[0]$라 가정하자. 그러면 $a\equiv 0(\mathrm{mod}\ p)$. 그래서 $p|a$, 즉, $a=pw$. 그러므로 $p=ab=pwb$. 양변을 p로 나눔으로써 $wb=1$. w와 b는 정수이므로, 가능성은 $w=\pm 1$과 $b=\pm 1$ 뿐이다. 그러므로 $b=\pm 1$이고 $a=pw=\ =p(\pm 1)=\pm p$.한편, 비슷한 논증에 의하여, $[b]=[0]$이면 $a=\pm 1$임을 보일 수 있다. 따라서 p는 소수다. ■

정리2.3.1 에 따라서, $ax=1(a\neq 0)$꼴의 $\mathbb{Z}_n$에서 모든 방정식은 n이 소수일 때 해를 갖는다.

n이 소수가 아니더라도, 이와 같은 어떤 방정식은 해를 가질 수 있다. 예로써, $\mathbb{Z}_{10}$에서, $x=7$은 $3x=1$의 해다.

따름정리 2.3.1

a와 n은 $n>1$인 정수라하자. $\mathbb{Z}$에서 $(a,n)=1$
$\Leftrightarrow \mathbb{Z}_n$에서 방정식 $ax=1$이 해를 갖는다.

►증명◄ ($\Rightarrow$): $(a,n)=1$이라 가정하자. 정리2.3.1의 (1)⇒(2)의 증명에서, $(a,p)=1$인 사실을 입증하기 위하여 p가

소수라는 성질만이 사용된다. $ax=1$이 해를 갖는다는 증명의 나머지는 이 사실에만 관계된다. 따라서 증명의 이 부분은 $(a,n)=1$인 임의의 $\mathbb{Z}_n$에서 성립한다.

($\Leftarrow$): $ax=1$이 $\mathbb{Z}_n$에서 해 u를 갖는다고 가정하자. 그러면 $\mathbb{Z}_n$에서 $au=1$또는 (a와 u를 정수로 생각하여) 논리적으로 같게, $\mathbb{Z}$에서 $au\equiv 1 \pmod{n}$. 그래서 $n|(au-1)$. 그러므로 $\exists v\in\mathbb{Z}\ \ s.t.\ au-1=nv$. 그러면 $au-nv=1$. 그래서 a와 n의 임의의 공약수는 1을 나누어야만 한다. 따라서 $(a,n)=1$. ■

예제 | 2.3.1 **$\mathbb{Z}_7$에서 방정식 $ax=1$이 해를 갖게 되는 a의 값들의 집합은?**

(가) {1,2}　　(나) {1,2,3}　　(다) {1,2,3,4}

(라) {1,2,3,4,5,6}　　(마) {1,2,3,4,5}

►풀이◄ $\mathbb{Z}_7$에서 $ax=1$이 해를 갖는다. $\Leftrightarrow$ $\mathbb{Z}$에서 $(a,7)=1$

따라서 $a=1,2,3,4,5$ 또는 6 ■