제 1 장　해　설

§1.2.1　약수와 배수

§1.2.2　최대공약수와 최소공배수

§1.2.3　素數와 소인수분해

§1.2.4　합 동

§1.2.1 약수와 배수

이 절에서는, 정수 전체의 집합 $\mathbb{Z}$ 안에서 생각하기로 한다.

정의 1 두 정수 a, b에 대하여

$$b = ac$$

인 정수 c가 존재할 때, a를 b의 **약수**(約數 divisor) 또는 **인수**(因數 factor)라 하고 b를 a의 **배수**(倍數 multiple)라고 하며, 이 사실을

$$a \mid b$$

로 나타낸다. 그리고 $a \mid b$일 때 'a는 b를 나누어 떨어뜨린다'고 말하고, $a \mid b$가 아닌 경우에 이 사실을 $a \nmid b$로 나타낸다.

정리 2 정수 a, b, c, d에 대하여 다음이 성립한다.

(1) $1 \mid a$이고, 또 $a \mid 1$이면 $a = \pm 1$이다.
(2) $a \mid 0$이고, 또 $0 \mid a$이면 $a = 0$이다.
(3) $a \mid a$
(4) $a \mid b,\ b \mid a$이면, $a = \pm b$이다.
(5) $a \mid b,\ b \mid c$이면, $a \mid c$이다.

정리 3 정수 a, b, d에 대하여 $d \mid a,\ d \mid b$이면, 임의의 정수 x, y에 대하여 $d \mid (ax + by)$이다.

특히, $d \mid a,\ d \mid b$이면, $d \mid (a+b),\ d \mid (a-b)$이다.

증 명 $d \mid a,\ d \mid b$이면, 적당한 정수 s, t에 대하여 $a = ds,\ b = dt$이고 이때

$$ax + by = d(sx + ty)$$

이므로 $d \mid (ax + by)$이다.

정리 4 정수 a, b, c, d 에 대하여 다음이 성립한다.

(1) $a|b$ 이면, $a|(-b)$, $(-a)|b$, $(-a)|(-b)$, $a^n|b^n$ 이다.

(2) $a|b$, $b\neq 0$ 이면, $1\leq|a|\leq|b|$ 이다.

(3) $a|b$, $c|d$ 이면, $ac|bd$ 이다.

(4) $a|b$ 이면, $a|bc$, $ac|bc$ 이다.

(5) $a|b$ 이면, 모든 양의 정수 n 에 대하여 $a^n|b^n$ 이다.

(6) $ac|bc$, $c\neq 0$ 이면, $a|b$ 이다.

정의 5 실수 x 에 대하여, x 보다 작거나 같은 정수 중에서 가장 큰 정수를 x 의 **정수부분**(整數部分 integral part) 또는 **최저한도**(最低限度 floor)라 하고 이것을 $[x]$ 또는 $\lfloor x\rfloor$ 로 나타낸다. 또,

$$\{\{x\}\}=x-[x]$$

를 x 의 **소수부분**(decimal part)이라고 한다.

즉, $x=[x]+\{\{x\}\}$, $[x]\in\mathbb{Z}$, $0\leq\{\{x\}\}<1$

그리고, x 보다 크거나 같은 정수 중에서 가장 작은 정수를 x 의 **최고한도**(最高限度 ceiling)라 하고 $\lceil x\rceil$ 로 나타낸다.

정리 6 실수 x 에 대하여 $[x]$ 와 $\lceil x\rceil$ 는 정수이고 다음이 성립한다.

(1) $x=[x]+\{\{x\}\}$, $[x]\leq x<[x]+1$, $0\leq\{\{x\}\}<1$

(2) $\lceil x\rceil-1<x\leq\lceil x\rceil$

정리 7 두 양의 정수 n, m $(n\geq m)$ 에 대하여 q, r 를

$$n=qm+r,\quad 0\leq r<m$$

인 정수라고 하면 다음이 성립한다.

(1) $\left[\frac{n}{m}\right]=q$, $\frac{n}{m}<\left[\frac{n}{m}\right]+1$, $\left\lceil\frac{n}{m}\right\rceil-1<\frac{n}{m}$

(2) $r=0$ 이면 $\left\lceil\frac{n}{m}\right\rceil=q$ 이고, 또 $r\neq 0$ 이면 $\left\lceil\frac{n}{m}\right\rceil=q+1$ 이다.

(3) 정수 $1, 2, 3, \cdots, n$ 중에서 m 의 배수인 정수의 개수는 q 이다.

정리 8 실수 x와 두 양의 정수 a, b에 대하여 다음이 성립한다.

(1) $\left[\frac{x}{a}\right] = \left[\frac{[x]}{a}\right]$

(2) $\left[\frac{x}{ab}\right] = \left[\frac{\left[\frac{x}{b}\right]}{a}\right], \quad \left[\frac{x}{a^2}\right] = \left[\frac{\left[\frac{x}{a}\right]}{a}\right]$

증 명 (1) 두 정수 q, r를 $[x] = qa + r,\ 0 \le r < a$ 인 정수라고 하면,

$\frac{[x]}{a} = q + \frac{r}{a},\ 0 \le \frac{r}{a} < 1$ 이므로 다음이 성립한다.

$$\left[\frac{[x]}{a}\right] = q, \quad x = [x] + \{\{x\}\} = qa + r + \{\{x\}\},$$

$$0 \le r + \{\{x\}\} < (a-1) + 1 = a$$

$$\frac{x}{a} = q + \frac{r + \{\{x\}\}}{a}, \quad 0 \le \frac{r + \{\{x\}\}}{a} < 1$$

그러므로, $\left[\frac{x}{a}\right] = q = \left[\frac{[x]}{a}\right]$ 이다.

(2) 등식 (1)의 x 대신에 각각 $\frac{x}{b}$, $\frac{x}{a}$ 를 대입하면, 등식 (2)를 얻는다.

정의 9 정수 a의 배수 전체의 집합을 $a\mathbb{Z}$ 로 나타낸다. 즉,

$$a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\} = \{0, \pm a, \pm 2a, \pm 3a, \cdots\}$$

$$a\mathbb{Z} = (-a)\mathbb{Z}, \quad 1\mathbb{Z} = \mathbb{Z} = (-1)\mathbb{Z}, \quad 0\mathbb{Z} = \{0\}$$

정리 10 정수 a에 대하여 $a\mathbb{Z}$ 는 덧셈과 뺄셈에 관하여 닫혀 있다.

역으로, $\mathbb{Z}$ 의 부분집합 $S\ (\neq \emptyset)$ 가 덧셈과 뺄셈에 관하여 닫혀 있으면, 다음과 같은 정수 m이 단 하나 존재한다.

$$S = m\mathbb{Z}, \qquad m \ge 0$$

증 명 임의의 두 정수 x, y 에 대하여

$$ax \pm ay = a(x \pm y) \in a\mathbb{Z}$$

이므로 $a\mathbb{Z}$ 는 덧셈과 뺄셈에 관하여 닫혀 있다.

다음에 $\mathbb{Z}$ 의 부분집합 $S\,(\neq\emptyset)$ 가 덧셈과 뺄셈에 관하여 닫혀 있다고 가정하자. 이 때, 한 원소 $a\in S$ 가 존재하고 이때 $0=a-a\in S$ 이다.

먼저 $S=\{0\}$ 이면, $S=0\mathbb{Z}$ 이다.

이제 $\{0\}\subsetneq S$ 이라고 하자. 이 때, S 에는 0 이 아닌 정수 a 가 존재하고 $-a=0-a\in S$ 이므로 S 에는 양의 정수가 존재한다. 따라서 정수의 정렬성(정리 1.3.4) 에 의하여 S 에 속하는 정수 중에서 가장 작은 양의 정수 m 이 단 하나 존재한다. 또, 임의의 양의 정수 k 에 대하여

$$km=m+m+\cdots+m\in S,\quad (-k)m=0-km\in S$$

이고 또 $0m=0\in S$ 이므로 $m\mathbb{Z}\subseteq S$ 이다.

한편, 임의의 $a\in S$ 에 대하여 q, r 를 $a=qm+r,\ 0\le r<m$ 인 정수라고 하면, $qm\in S$ 이므로 $r=a-qm\in S$ 이고 m 의 最小性에 의하여, 이는 $r=0$ 임을 뜻하므로 $a=qm\in m\mathbb{Z}$ 이다. 따라서 $S\subseteq m\mathbb{Z}$ 이다.

그러므로 $S=m\mathbb{Z}$ 이다.

정리 11 두 정수 a, b 에 대하여 다음이 성립한다.

(1) $b\mathbb{Z}\subseteq a\mathbb{Z}\iff a\mid b$ (2) $a\mathbb{Z}=b\mathbb{Z}\iff b=\pm a$

증 명 (1) 먼저 $b\mathbb{Z}\subseteq a\mathbb{Z}$ 이면, $b\in b\mathbb{Z}\subseteq a\mathbb{Z}$ 이므로 $a\mid b$ 이다.

역으로, $a\mid b$ 이라고 하자. 이 때, 적당한 정수 c 에 대하여 $b=ac$ 이고 임의의 정수 x 에 대하여 $bx=a(cx)\in a\mathbb{Z}$ 이므로 $b\mathbb{Z}\subseteq a\mathbb{Z}$ 이다.

(2) 위의 (1) 과 정리 1.4.2 에 의하여 다음이 성립한다.

$$\begin{aligned} & a\mathbb{Z}=b\mathbb{Z} \\ \iff & a\mathbb{Z}\subseteq b\mathbb{Z}\text{ 이고 }b\mathbb{Z}\subseteq a\mathbb{Z} \\ \iff & a\mid b\text{ 이고 }b\mid a \\ \iff & b=\pm a \end{aligned}$$

§1.2.2 최대공약수와 최소공배수

이 절에서는, 정수 전체의 집합 $\mathbb{Z}$ 안에서 생각한다.

정의 1 두 정수 a, b에 대하여

$$d \mid a, \quad d \mid b$$

인 정수 e를 a, b의 **공약수**(公約數 common divisor)라 하고

$$a \mid c, \quad b \mid c$$

인 정수 c를 a, b의 **공배수**(公倍數 common multiple)라고 한다.

정의 2 두 정수 a, b에 대하여 다음 세 조건을 만족시키는 정수 d를 a, b의 **최대공약수**(greatest common divisor)라 하고, 이것을 (a, b) 또는 $\gcd\{a, b\}$로 나타낸다.

(i) $d \geq 0$

(ii) $d \mid a,\ d \mid b$

(iii) 정수 e에 대하여 $e \mid a,\ e \mid b$이면, $e \mid d$이다.

그리고, 다음 세 조건을 만족시키는 정수 l을 a, b의 **최소공배수**(least common multiple)라 하고, 이것을 $[a, b]$ 또는 $\mathrm{lcm}\{a, b\}$로 나타낸다.

(i)' $l \geq 0$

(ii)' $a \mid l,\ b \mid l$

(iii)' 정수 c에 대하여 $a \mid c,\ b \mid c$이면, $l \mid c$이다.

임의의 정수 s, t에 대하여 $s \mid t,\ s \mid -t,\ (-s) \mid t,\ (-s) \mid (-t)$는 서로 동치이다(정리 1.4.4). 따라서 두 정수 a, b에 대하여 다음이 성립한다.

$$(a, -b) = (-a, b) = (-a, -b) = (a, b),$$
$$[a, -b] = [-a, b] = [-a, -b] = [a, b]$$

두 정수 a, b의 최대공약수 d에 대한 세 조건과 최소공배수 l에 대한 세 조건은 각각 다음과 같이 고쳐 쓸 수 있다.

(i) $d \geq 0$

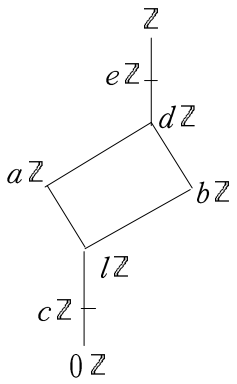
(ii) $a\mathbb{Z} \subseteq d\mathbb{Z},\ b\mathbb{Z} \subseteq d\mathbb{Z}$

(iii) 정수 e에 대하여 $a\mathbb{Z} \subseteq e\mathbb{Z},\ b\mathbb{Z} \subseteq e\mathbb{Z}$ 이면, $d\mathbb{Z} \subseteq e\mathbb{Z}$이다.

(i)' $l \geq 0$

(ii)' $l\mathbb{Z} \subseteq a\mathbb{Z},\ l\mathbb{Z} \subseteq b\mathbb{Z}$

(iii)' 정수 c에 대하여 $c\mathbb{Z} \subseteq a\mathbb{Z},\ c\mathbb{Z} \subseteq b\mathbb{Z}$ 이면, $c\mathbb{Z} \subseteq l\mathbb{Z}$ 이다.



정리 3 두 정수 a, b에 대하여 a, b의 최대공약수 $d = (a, b)$와 최소공배수 $l = [a, b]$은 단 하나씩 존재하고 또 다음이 성립한다.

(1) $S = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$이라고 하면, $S = d\mathbb{Z}$이고 또 $d = as + bt$ 인 정수 s, t가 존재한다.

(2) $a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z}$

증 명 (1) 임의의 두 정수 x, y에 대하여

$$ax = ax + b0 \in S, \quad by = a0 + by \in S$$

이므로 $a\mathbb{Z} \subseteq S,\ b\mathbb{Z} \subseteq S$이다. 그리고, 임의의 정수 x, y, u, v에 대하여

$$(ax + by) \pm (au + bv) = a(x \pm u) + b(y \pm v) \in S$$

이므로 S는 덧셈과 뺄셈에 관하여 닫혀 있고, 따라서 $S = d\mathbb{Z},\ d \geq 0$ 인 정수 d가 단 하나 존재한다.

그런데, $a \in a\mathbb{Z} \subseteq S = d\mathbb{Z}, b \in b\mathbb{Z} \subseteq S = d\mathbb{Z}$이므로 $d \mid a,\ d \mid b$이다.

그리고, $d \in d\mathbb{Z} = S$이므로 적당한 정수 s, t에 대하여 $d = as + bt$ 이고, 따라서 정수 e에 대하여 $e \mid a,\ e \mid b$이면 $e \mid d$이다.

그러므로 d는 a, b의 최대공약수이다.

(2) 이제 $T = a\mathbb{Z} \cap b\mathbb{Z}$이라고 하자. 이 때, $0 \in T$이므로 $T \neq \emptyset$ 이다.

그리고, $c, d \in T$이라고 하면, 적당한 정수 x, u, y, v에 대하여 $c = ax = bu,\ d = ay = bv$이고 이때

$$c \pm d = a(x \pm y) = b(u \pm v) \in T$$

이므로 T는 덧셈과 뺄셈에 관하여 닫혀 있다. 따라서 $T = l\mathbb{Z}$, $l \geq 0$ 인 정수 l이 단 하나 존재한다. 그런데, $l \in l\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$ 이므로 $a|l$, $b|l$ 이다. 또, 정수 c에 대하여 $a|c$, $b|c$ 이면, $c \in a\mathbb{Z} \cap b\mathbb{Z} = l\mathbb{Z}$ 이므로 $l|c$ 이다. 따라서 l은 a, b의 최소공배수이다.

정리 4 네 정수 a, b, c, k 에 대하여 $(bk + c, b) = (c, b)$ 이다.

특히, 정수 a를 양의 정수 m으로 나누었을 때의 나머지를 r라고 하면, $(a, m) = (r, m)$, $0 \leq r < m$ 이다.

증 명 이제 $a = kb + c$이라 하고 $d = (a, b)$, $e = (c, b)$이라고 하자.

이 때, $d|a$, $d|b$이므로 $d|c$, $d|b$이고 따라서 $d|e$이다.

그리고, $e|c$, $e|b$이므로 $e|a$, $e|b$이고 따라서 $e|d$이다.

그런데 $d \geq 0$, $e \geq 0$이므로 이 결과는 $d = e$임을 뜻한다.

정리 5 (유클리드의 알고리즘, Euclidean algorithm) 두 양의 정수 a, b에 대하여 $r_0 = a$, $r_1 = b$이라 놓고 $a_0, \cdots, a_m, r_2, \cdots, r_m, r_{m+1}$을 다음과 같은 정수라고 하자.

$$
\begin{aligned}
r_0 &= a_0 r_1 + r_2, && 0 < r_2 < r_1 \\
r_1 &= a_1 r_2 + r_3, && 0 < r_3 < r_2 \\
r_2 &= a_2 r_3 + r_4, && 0 < r_4 < r_3 \\
&\vdots && \vdots \\
r_{m-1} &= a_{m-1} r_m + r_{m+1}, && 0 < r_{m+1} < r_m \\
r_m &= a_m r_{m+1}
\end{aligned}
$$

a_0	r_0	r_1	a_1
	$a_0 r_1$	$a_1 r_2$	
	$\vdots$	$\vdots$	
a_{m-1}	r_{m-1}	r_m	a_m
	$a_{m-1} r_m$	$a_m r_{m+1}$	
	r_{m+1}	0	

이 때, $(a, b) = r_{m+1}$ 이고, 또

$$
\begin{aligned}
s_0 &= 1,\ s_1 = 0, && s_i = s_{i-2} - a_{i-2} s_{i-1} \\
t_0 &= 0,\ t_1 = 1, && t_i = t_{i-2} - a_{i-2} t_{i-1}
\end{aligned}
\qquad (2 \leq i \leq m+1)
$$

이라고 하면 다음이 성립한다.

$$
r_i = a s_i + b t_i \quad (0 \leq i \leq m+1)
$$

$$
(a, b) = r_{m+1} = a s_{m+1} + b t_{m+1}
$$

a_i	a_0	a_1	a_2	$\cdots$	a_{m-1}		
s_i	1	0	s_2	$\cdots$	s_{m-1}	s_m	s_{m+1}
t_i	0	1	t_2	$\cdots$	t_{m-1}	t_m	t_{m+1}

증 명 나눗셈 알고리즘에 의하여 정수 $a_0, a_1, \cdots, a_m, r_2, \cdots, r_{m+1}$ 은 존재하고, 또 다음이 성립한다.

$$d = (a, b) = (r_0, r_1) = (r_1, r_2) = \cdots = (r_m, r_{m+1}) = r_{m+1}$$

분명히 $r_0 = a = as_0 + bt_0$, $r_1 = b = as_1 + bt_1$ 이다.

그리고, $0 \le k \le m$ 일 때, 정수 $i\ (0 \le i \le k)$ 에 대하여 $r_i = as_i + bt_i$ 이라고 가정하면, 다음이 성립한다.

$$\begin{aligned} r_{k+1} &= r_{k-1} - a_{k-1} r_k \\ &= as_{k-1} + bt_{k-1} - a_{k-1}(as_k + bt_k) \\ &= a(s_{k-1} - a_{k-1}s_k) + b(t_{k-1} - a_{k-1}t_k) \\ &= as_{k+1} + bt_{k+1} \end{aligned}$$

따라서 수학적 귀납법에 의하여

$$r_i = as_i + bt_i \qquad (1 \le i \le m+1)$$

이고, 특히 $(a, b) = r_{m+1} = as_{m+1} + bt_{m+1}$이다.

정의 6 두 정수 a와 b의 최대공약수가 1일 때, 즉 $(a, b) = 1$ 일 때, 두 정수 a, b는 **서로 소**(relatively prime)라고 한다.

정리 7 두 정수 a, b에 대하여 다음 두 조건은 서로 동치이다.

(1) $(a, b) = 1$

(2) $as + bt = 1$ 인 정수 s, t가 존재한다.

증 명 먼저 $(a, b) = 1$ 이면, (2)가 성립한다.

역으로, 조건 (2)가 성립할 때, $d = (a, b)$ 라고 하면, $d \mid a, d \mid b$ 이므로 $d \mid (as + bt)$ 즉 $d \mid 1$ 이고 따라서 $d = 1$ 이다.

따름정리 8 두 정수 a, b에 대하여 $d = (a, b) \ge 1$ 이라고 할 때, $(\frac{a}{d}, \frac{b}{d}) = 1$ 이다.

정리 9 정수 a, b, m에 대하여 다음이 성립한다.

$$(a, m) = (b, m) = 1 \Leftrightarrow (ab, m) = 1$$

증 명 먼저 $(a, m) = (b, m) = 1$이면, $as + mt = 1$, $bu + mv = 1$인 정수 s, t, u, v가 존재하고 이때 $(as + mt)(bu + mv) = 1$ 즉

$$ab(su) + m(asv + but + mtv) = 1$$

이므로 $(ab, m) = 1$이다.

역으로, $(ab, m) = 1$이면, $(ab)s + mt = 1$인 정수 s, t가 존재하고 이때

$$a(bs) + mt = 1, \qquad b(as) + mt = 1$$

이므로 $(a, m) = 1$, $(b, m) = 1$이다.

따름정리 10 정수 $a, b, a_1, \cdots, a_n$과 양의 정수 m, n에 대하여 다음이 성립한다.

(1) $(a, b) = 1 \Leftrightarrow (a^n, b) = 1 \Leftrightarrow (a, b^n) = 1$

(2) $(a, b) = 1 \Leftrightarrow (a^m, b^n) = 1$

(3) $(a_1, b) = \cdots = (a_n, b) = 1 \Leftrightarrow (a_1 \cdots a_n, b) = 1$

정리 11 세 정수 a, b, c에 대하여 다음이 성립한다.

(1) $(a, b) = 1$일 때, $a|c$, $b|c$이면 $ab|c$이다.

(2) $(a, b) = 1$일 때, $a|bc$이면 $a|c$이다.

(3) $(a, b) = 1$일 때, $[a, b] = |ab|$이다.

증 명 (1), (2) 가정에 의하여 $as + bt = 1$인 정수 s, t가 존재한다

그런데 $a|c$, $b|c$이면, $(ac)s + (bc)t = c$, $\quad ab|ac$, $ab|bc$

이므로 $ab|c$이다. 또, $a|bc$이면, $a(cs) + (bc)t = c$, $\quad a|a$, $a|bc$

이므로 $a|c$이다.

(3) 먼저 a, b가 양의 정수일 때, ab는 양의 정수이고 $a|ab$, $b|ab$이며 (1) 이 성립하므로 정의에 의하여 $[a, b] = ab$이다(정리 1.5.2).

위의 결과로부터 그 밖의 경우에 $[a, b] = |ab|$ 임을 알 수 있다.

정리 12 두 양의 정수 a, b 에 대하여 $(a, b)[a, b] = ab$ 이다.
특히, $(a, b) = 1$ 일 때 그리고 이때에만 $[a, b] = ab$ 이다.

증 명 이제 $d = (a, b)$ 이라 하고 $a = ud,\ b = vd$ 라고 하자. 이 때, $l = va$ 이라 놓고 정의 1.5.2 에 따라 $l = [a, b]$ 임을 증명한다.
먼저 $l \geq 1$ 이고, $l = va = vud = ub$ 이므로 $a|l,\ b|l$ 이다.
다음에 $a|c,\ b|c$ 이라 가정하고 $c = ak = br$ 이라고 하자. 이 때,

$$ld = vad = ab$$

이고 적당한 정수 s, t 에 대하여 $d = as + bt$ 이므로 다음이 성립한다.

$$\frac{c}{l} = \frac{cd}{ld} = \frac{cd}{ab} = \frac{acs + bct}{ab} = \left(\frac{c}{b}\right)s + \left(\frac{c}{a}\right)t = rs + kt$$

이 등식은 $\frac{c}{l}$ 가 정수임을 뜻하므로 $l|c$ 이다.
그러므로, $l = [a, b]$ 이고, 따라서 $(a, b)[a, b] = dl = ab$ 이다.

정의 13 정수 $a_1, a_2, \cdots, a_n\ (n \geq 2)$ 에 대하여

$$d|a_1,\ d|a_2,\ \cdots,\ d|a_n$$

인 정수 d 를 이들 정수의 **공약수**라 하고, 또

$$a_1|c,\ a_2|c,\ \cdots,\ a_n|c$$

인 정수 c 를 이들 정수의 **공배수**라고 한다,

정의 14 정수 $a_1, a_2, \cdots, a_n$ 에 대하여 다음 세 조건을 만족시키는 정수 d 를 $a_1, a_2, \cdots, a_n$ 의 **최대공약수**라 하고, d 를 $(a_1, a_2, \cdots, a_n)$ 또는 $\gcd\{a_1, a_2, \cdots, a_n\}$ 으로 나타낸다.

(i) $d \geq 0$
(ii) $d|a_1,\ d|a_2,\ \cdots,\ d|a_n$
(iii) 정수 e 에 대하여 $e|a_1,\ e|a_2,\ \cdots,\ e|a_n$ 이면, $e|d$ 이다.

정의 15 정수 $a_1, a_2, \cdots, a_n$ 에 대하여 다음 세 조건을 만족시키는 정수 l 을 $a_1, a_2, \cdots, a_n$ 의 **최소공배수**라 하고, l 을

$$[a_1, a_2, \cdots, a_n] \quad \text{또는} \quad \text{lcm}\{a_1, a_2, \cdots, a_n\}$$

으로 나타낸다.

(i) $l \geq 0$

(ii) $a_1 | l,\ a_2 | l,\ \cdots,\ a_n | l$

(iii) 정수 c 에 대하여 $a_1 | c,\ a_2 | c,\ \cdots,\ a_n | c$ 이면, $l | c$ 이다.

정리 16 정수 $a_1, a_2, a_3, \cdots, a_n$ 에 대하여 이들 정수의 최대공약수와 최고공배수는 각각 단 하나씩 존재하며 다음이 성립한다.

$$(a_1, a_2, \cdots, a_{n-1}, a_n) = ((a_1, a_2, \cdots, a_{n-1}), a_n)$$
$$[a_1, a_2, \cdots, a_{n-1}, a_n] = [[a_1, a_2, \cdots, a_{n-1}], a_n]$$

정리 17 정수 $a_1, a_2, \cdots, a_n$ 의 최대공약수를 d 라고 하면, 적당한 정수 $s_1, s_2, \cdots, s_n$ 에 대하여 $d = a_1 s_1 + a_2 s_2 + \cdots + a_n s_n$ 이다.

정의 18 정수 $a_1, a_2, \cdots, a_n$ 에 대하여 $(a_1, a_2, \cdots, a_n) = 1$ 일 때, 이들 정수는 **서로 소**(mutually prime)라고 한다. 그리고,

$$(a_i, a_j) = 1 \qquad (1 \leq i \neq j \leq n)$$

일 때, 이들 정수는 **쌍마다 서로 소**(pairwise relatively prime)라고 한다.

정리 19 정수 $a_1, a_2 \cdots, a_n$ 에 대하여 다음 두 조건은 동치이다.

(1) $a_1, a_2, \cdots, a_n$ 은 서로 소이다.

(2) 적당한 $s_1, s_2, \cdots, s_n$ 에 대하여 $a_1 s_1 + a_2 s_2 + \cdots + a_n s_n = 1$ 이다.

정리 20 양의 정수 $a_1, a_2, \cdots, a_n$ 이 쌍마다 서로 소이면 다음이 성립한다.

(1) $a_1 | c,\ a_2 | c,\ \cdots,\ a_n | c$ 이면, $a_1 a_2 \cdots a_n | c$ 이다.

(2) $[a_1, a_2, \cdots, a_n] = a_1 a_2 \cdots a_n$

§1.2.3 素數와 소인수분해

이 절에서는, 특수한 성질을 가진 정수에 대하여 간단히 논한다.

정의 1 정수 $p\ (\geq 2)$의 양의 약수가 $1, p$뿐일 때, p를 **소수**(素數 prime, prime number)라고 한다.

그리고, 정수 $a\ (\geq 2)$가 素數가 아닐 때, 즉

$$a = de, \qquad 2 \leq d \leq e < a$$

인 정수 d, e가 존재할 때, a를 **합성수**(合成數 composite number)라고 한다.

정리 2 정수 p가 素數일 때, 정수 a와 양의 정수 n, m에 대하여 다음이 성립한다

(1) $p \mid a \iff (a, p) = p, \qquad p \nmid a \iff (a, p) = 1$

(2) $(a, p^n) = 1 \iff (a, p) = 1$

(3) $(a, p) = 1 \iff (a^n, p) = 1$

(4) p, q가 서로 다른 素數이면, $(p, q) = 1, (p^n, q^m) = 1$이다.

정리 3 정수 p가 素數일 때, 두 정수 a, b에 대하여 $p \mid ab$이면, $p \mid a$ 또는 $p \mid b$이다.

증 명 素數 p에 대하여 $p \mid ab$일 때, $p \nmid a$이라고 가정하자,
이 때, $(a, p) = 1$이고 $p \mid ab$이므로 $p \mid b$이다.
따라서 $p \mid ab$이면, $p \mid a$ 또는 $p \mid b$이다.

따름정리 4 정수 p가 素數일 때, 정수 a와 양의 정수 n 그리고 n개의 정수 $a_1, a_2, , \cdots, a_n$에 대하여 다음이 성립한다.

(1) $p \mid a^n$이면, $p \mid a$이다.

(2) $p \mid a_1 a_2 a_3 \cdots a_n$이면 적당한 $i\ (1 \leq i \leq n)$에 대하여 $p \mid a_i$이다.

정의 5 정수 a의 인수(약수) 중에서 특히 素數인 인수를 a의 **소인수**(素因數 prime factor)라고 한다.

정리 6 정수 $a\ (\geq 2)$에 대하여 a의 소인수가 적어도 하나 존재한다.

정리 7 양의 정수 n이 합성수이면, n의 소인수 중에는 $p \leq [\sqrt{n}]$인 소인수 p가 존재한다.

정리 8 (유클리드) 素數는 무한히 많다.

정의 9 정수 n의 素數인 인수(약수)를 n의 **소인수**라고 한다.
그리고, 정수 $n\ (\geq 2)$이 유한 개의 소인수 $p_1, p_2, \cdots, p_k$의 곱

$$n = p_1 p_2 \cdots p_k$$

으로 나타내어질 때, 정수 n은 **소인수분해된다**고 말하고 또 이 등식을 n의 **소인수분해**(素因數分解 prime factorization)라고 한다.

정리 10 (유일 인수분해 정리, Unique Factorization Theorem)
정수 $n\ (\geq 2)$은 유한 개의 素數 $p_1, p_2, \cdots, p_s$의 곱 $n = p_1 p_2 \cdots p_s$으로 소인수분해된다(여기서, $p_1, p_2, \cdots, p_s$에 같은 것이 있을 수 있다).
더욱이, $n\ (\geq 2)$의 소인수분해는 본질적으로 단 한 가지 뿐이다. 즉,

$$n = p_1 p_2 \cdots p_s, \qquad n = q_1 q_2 \cdots q_t$$

을 n의 소인수분해라고 하면, $s = t$이고 $p_1, p_2, \cdots, p_s$와 $q_1, q_2, \cdots, q_t$는 그 순서만이 다르다.

정의 11 정수 $n\ (\geq 2)$의 서로 다른 소인수 전체가 $p_1, p_2, \cdots, p_r$일 때, n은 단 한 가지 방법으로 다음과 같이 소인수분해된다.

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \qquad (e_1 \geq 1, e_2 \geq 1, \cdots, e_r \geq 1)$$

위의 등식을 n의 **표준분해**(standard decomposition)라고 한다.

정의 12 한 정수의 제곱인 정수를 **제곱수**(square)라 하고, 특히 1 보다 정수의 제곱인 정수를 **완전제곱수**(perfect square) 라고 한다.

정리 13 양의 정수 a, b 가 서로 다른 素數 $p_1, p_2, \cdots, p_t$ 에 대하여

$$a = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}, \quad b = p_1^{s_1} p_2^{s_2} \cdots p_t^{s_t} \quad (k_i \geq 0,\ s_i \geq 0)$$

으로 나타내어질 때, $m_i = \min\{k_i, s_i\}$, $n_i = \max\{k_i, s_i\}$ 라고 하면 다음이 성립한다.

(1) $(a, b) = p_1^{m_1} p_2^{m_2} \cdots p_t^{m_t}, \quad [a, b] = p_1^{n_1} p_2^{n_1} \cdots p_t^{n_t}$

(2) $(a, b)[a, b] = ab$

정의 14 두 양의 정수 a, b 에 대하여 $b^e \mid a$, $b^{e+1} \nmid a$ $(e \geq 0)$ 일 때, 이 사실을 $b^e \| a$ 로 나타낸다.

양의 정수 a 의 서로 다른 소수인 전체가 $p_1, p_2, \cdots, p_r$ 일 때, 각 p_i 에 대하여 $p_i^{e_i} \| a$ 이면, a 의 표준분해는 $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ 이다.

정리 15 정수 n (≥ 2) 의 계승 $n! = 1 \cdot 2 \cdot \cdots \cdot n$ 과 素數 p 에 대하여 $p^e \| n!$ 인 지수 e 를 $e_p(n)$ 으로 나타내면 다음이 성립한다.

$$e_p(n) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

§1.2.4 합 동

이 장에서 논할 합동 개념은 독일 수학자 가우스(Karl Friedrich Gauss)가 19 세기 초에 처음으로 도입한 개념이다.

정의 1 양의 정수 m에 대하여, 두 정수 a, b의 차가 m의 배수일 때, 즉 $m|(a-b)$ 일 때, a와 b는 **법**(法 modulus) m에 관하여 **합동**(合同 congruent)이라 하고, 이 사실을 $a \equiv b \pmod{m}$으로 나타낸다. 즉,

$$a \equiv b \pmod{m} \iff m|(a-b)$$

합동 기호 $\equiv$가 들어 있는 식을 **합동식**(合同式)이라고 한다. 그리고, $a \equiv b \pmod{m}$가 아닌 경우에 이 사실을 $a \not\equiv b \pmod{m}$로 나타낸다.

정리 2 양의 정수 m과 정수 a, b, c에 대하여 다음이 성립한다.

(1) $a \equiv a \pmod{m}$

(2) $a \equiv b \pmod{m}$이면, $b \equiv a \pmod{m}$이다.

(3) $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$이면, $a \equiv c \pmod{m}$이다.

정리 3 정수 m, n이 양의 정수라고 하자.

(1) $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$이면, 다음이 성립한다.

$$a+c \equiv b+d \pmod{m}, \quad ac \equiv bd \pmod{m}$$

(2) $a \equiv b \pmod{m}$이면, 다음이 성립한다.

$$a+c \equiv b+c \pmod{m}, \quad ac \equiv bc \pmod{m}$$

(3) $a_1 \equiv b_1 \pmod{m}, \cdots, a_n \equiv b_n \pmod{m}$이면, 다음이 성립한다.

$$a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{m},$$

$$a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{m}$$

(4) $a \equiv b \pmod{m}$이면, $a^n \equiv b^n \pmod{m}$이다.

따름정리 4 정수를 계수로 가지는 두 다항식

$$f(x) = a_0 + a_1x + \cdots + a_nx^n,$$
$$g(x) = b_0 + b_1x + \cdots + b_nx^n$$

에 대하여 다음이 성립한다.

(1) $a \equiv b \pmod{m}$ 이면, $f(a) \equiv f(b) \pmod{m}$ 이다.

(2) $a_0 \equiv b_0 \pmod{m}$, $a_1 \equiv b_1 \pmod{m}$, $\cdots$, $a_n \equiv b_n \pmod{m}$ 이면, $f(a) \equiv g(a) \pmod{m}$ 이다.

정리 5 양의 정수 m에 관하여 집합 $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$은 다음 두 조건을 만족시킨다.

(1) 법 m에 관하여 $0, 1, \cdots, m-1$은 어느 둘도 합동이 아니다.

(2) 임의의 정수 a는 법 m에 관하여 $\mathbb{Z}_m$의 단 하나의 원소와 합동이다.

실제로, 임의의 정수 a를 m으로 나누었을 때의 나머지가 r라고 하면, $a \equiv r \pmod{m}$, $0 \le r < m$이고 이와 같은 r는 단 하나 뿐이다.

정리 6 양의 정수 m과 정수 a, b, c에 대하여 다음이 성립한다.

(1) $(a, m) = 1$일 때, $ab \equiv 0 \pmod{m}$이면 $b \equiv 0 \pmod{m}$이다.

(2) $(a, m) = 1$일 때, $ab \equiv ac \pmod{m}$이면 $b \equiv c \pmod{m}$이다.

증 명 (1) $(a, m) = 1$일 때, $ab \equiv 0 \pmod{m}$이면 $m \mid ab$이므로 $m \mid b$이고 따라서 $b \equiv 0 \pmod{m}$이다.

(2) $ab \equiv ac \pmod{m}$이면, $a(b-c) \equiv 0 \pmod{m}$이므로 위의 (1)에 의하여 $b - c \equiv 0 \pmod{m}$ 즉 $b \equiv c \pmod{m}$이다.

정리 7 일차합동식

$$ax \equiv b \pmod{m}, \qquad (a, m) = 1$$

는 법 m에 관하여 단 하나의 해 $x \equiv c \pmod{m}$를 가진다.

여기서, 정수 c를 $0 \le c < m$이 되도록 택할 수 있다.

증 명 먼저 $(a, m) = 1$ 이므로 $as + mt = 1$ 인 정수 s, t 가 존재하고 이 때,

$$asb + mtb = b \quad \text{즉} \quad a(sb) \equiv b \pmod{m}$$

이므로 $k = sb$ 를 m 으로 나누었을 때의 나머지를 c 라고 하면,

$$ac \equiv ak \equiv a(sb) \equiv b \pmod{m}$$

이므로 $x \equiv c \pmod{m}$ 는 합동식 $ax \equiv b \pmod{m}$ 의 해이다.

이제

$$x \equiv x_1 \pmod{m}, \quad x \equiv x_2 \pmod{m}$$

를 합동식 $ax \equiv b \pmod{m}$ 의 해라고 하면,

$$ax_1 \equiv b \equiv ax_2 \pmod{m}$$

이고 또 $(a, m) = 1$ 이므로 $x_1 \equiv x_2 \pmod{m}$ 이다.

정리 8 양의 정수 m, n 과 정수 a, b 에 대하여 다음 두 조건은 서로 동치이다.

(1) $a \equiv b \pmod{m}, \quad a \equiv b \pmod{n}$

(2) $a \equiv b \pmod{[m, n]}$

특히, $(m, n) = 1$ 이면, 다음 두 조건은 서로 동치이다.

(1)' $a \equiv b \pmod{m}, \quad a \equiv b \pmod{n}$

(2)' $a \equiv b \pmod{mn}$

정리 9 양의 정수 $m_1, \cdots, m_n$ $(n \geq 2)$ 과 정수 a, b 에 대하여 다음 두 조건은 서로 동치이다.

(1) $a \equiv b \pmod{m_1}, \cdots, a \equiv b \pmod{m_n}$

(2) $a \equiv b \pmod{[m_1, \cdots, m_n]}$

특히, $m_1, \cdots, m_n$ 이 쌍마다 서로 소이면, 다음 두 조건은 서로 동치이다.

(1)' $a \equiv b \pmod{m_1}, \cdots, a \equiv b \pmod{m_n}$

(2)' $a \equiv b \pmod{m_1 \cdots m_n}$

정리 10 (중국인의 나머지 정리) 양의 정수 $m_1, m_2, \cdots, m_n$ $(n \geq 2)$ 이 쌍마다 서로 소일 때, $M = m_1 m_2 \cdots m_n$ 이라고 하면 연립일차합동식

$$(*) \qquad \begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv b_n \pmod{m_n} \end{cases}$$

은 법 M에 관하여 단 한 개의 해 $x \equiv c \pmod{M}$ 를 가진다.

증 명 양의 정수 $m_1, m_2, \cdots, m_n$ 이 쌍마다 서로 소이므로

$$M = m_1 M_1 = m_2 M_2 = \cdots = m_n M_n$$

이라고 하면,

$$(M_i, m_i) = 1 \qquad (1 \leq i \leq n)$$

이므로 $M_i N_i \equiv 1 \pmod{m_i}$ 인 정수 N_i 가 존재한다. 그리고

$$M_j \equiv 0 \pmod{m_i} \qquad (1 \leq i \neq j \leq n)$$

이므로

$$c = M_1 N_1 b_1 + M_2 N_2 b_2 + \cdots + M_n N_n b_n$$

이라고 놓으면, 다음이 성립한다.

$$c \equiv M_i N_i b_i \equiv b_i \pmod{m_i} \qquad (1 \leq i \leq n)$$

따라서 주어진 연립일차합동식의 각 합동식은

$$x \equiv c \pmod{m_1},\ x \equiv c \pmod{m_2},\ \cdots,\ x \equiv c \pmod{m_n}$$

으로 고쳐 쓸 수 있으며, 이는 $x \equiv c \pmod{M}$ 임을 뜻한다.

한편, $x \equiv u \pmod{M}$ 가 주어진 연립합동식의 해이면,

$$u \equiv b_i \equiv c \pmod{m_i} \qquad (1 \leq i \leq n)$$

이고 따라서 $u \equiv c \pmod{M}$ 이다.

그러므로, $(*)$ 는 법 M에 관하여 단 하나의 해 $x \equiv c \pmod{M}$ 를 가진다.

정리 11 (Fermat 의 정리) 정수 p가 素數일 때 다음이 성립한다.

(1) 임의의 두 정수 a, b에 대하여 $(a+b)^p \equiv a^p + b^p \pmod{p}$ 이다.

(2) 모든 정수 a에 대하여 $a^p \equiv a \pmod{p}$ 이다.

특히, $(a, p) = 1$ 인 정수 a에 대하여 $a^{p-1} \equiv 1 \pmod{p}$ 이다.

증 명 (1) 임의의 두 정수 a, b에 대하여 다음이 성립한다.

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{r} a^{p-r}b^r + \cdots + b^p$$

여기서, $\binom{p}{r} = \dfrac{p!}{r!(p-r)!}$ 는 정수이고 $p! = \binom{p}{r} r!(p-r)!$ 이다.

그런데, $1 \le r \le p-1$ 일 때,

$$p \nmid 1 \cdot 2 \cdot \cdots \cdot r, \qquad p \nmid 1 \cdot 2 \cdot \cdots \cdot (p-r), \quad p \mid p!$$

이므로 $p \mid \binom{p}{r}$ 즉 $\binom{p}{r} \equiv 0 \pmod{p}$ 이다.

따라서 $(a+b)^p \equiv a^p + b^p \pmod{p}$ 이다.

(2) 먼저 $n = 1$ 일 때, $n \equiv 1^p \equiv 1 = n \pmod{p}$ 이다.

다음에 양의 정수 k에 대하여 $k^p \equiv k \pmod{p}$ 이라고 가정하면. (1) 에 의하여 $(k+1)^p \equiv k^p + 1^p \equiv k+1 \pmod{p}$ 이다.

따라서 모든 양의 정수 n에 대하여 $n^p \equiv n \pmod{p}$ 이다. 그리고,

$p = 2$ 일 때 $(-n)^p \equiv n^p \equiv n \equiv -n \pmod{p}$ 이다.

p가 홀수일 때 $(-n)^p \equiv (-1)^p n^p \equiv -n^p = -n \pmod{p}$ 이다.

또, $0^p \equiv 0 \pmod{p}$ 이므로 모든 정수 a에 대하여 $a^p \equiv a \pmod{p}$ 이다. 특히, $(a, p) = 1$ 이면, $a^{p-1} \equiv 1 \pmod{p}$ 이다.

정의 12 양의 정수 m에 대하여 집합 $\mathbb{Z}_m = \{0, 1, \cdots, m-1\}$ 의 원소 중에서 m과 서로 소인 원소 전체로 이루어진 집합을 $\mathbb{Z}_m^*$ 로 나타내고 또이와 같은 원소 전체의 개수를 $\varphi(m)$ 으로 나타낸다. 즉

그리고, 함수 $\varphi : \mathbb{N} \longrightarrow \mathbb{R}$ 를 **Euler 의 φ 함수**라고 한다

정리 13 素數 p와 양의 정수 k에 대하여 다음이 성립한다.

$$\mathbb{Z}_p{}^* = \{1, 2, \cdots, p-1\}, \quad \varphi(p) = p-1$$
$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1), \quad \varphi(2^k) = 2^{k-1}$$

증 명 정리 2.1.2 에 의하면, 정수 a에 대하여

$$(a, p^k) = 1 \Leftrightarrow (a, p) = 1 \Leftrightarrow p \nmid a$$

이고, $\mathbb{Z}_{p^k} = \{0, 1, \cdots, p^k - 1\}$의 원소 중에서 p의 배수인 것은 p^{k-1} 개의 정수 $0, p, 2p, \cdots, (p^{k-1}-1)p$ 뿐이다.

따라서 $\varphi(p^k) = p^k - p^{k-1}$ 이다.

정리 14 Euler의 φ 함수는 곱셈함수이다. 즉,

(1) $\varphi(1) = 1$

(2) 서로 소인 양의 정수 m, n에 대하여 $\varphi(mn) = \varphi(m)\varphi(n)$ 이다.

양의 정수 m의 표준분해가 $m = p_1^{e_1} \cdots p_r^{e_r}$ 일 때, $\varphi(m)$의 값은 다음과 같다.

$$\varphi(m) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r}) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p_r^{e_r-1})$$

즉,
$$\varphi(m) = p_1^{e_1}(1 - \frac{1}{p_1}) \cdots p_r^{e_r}(1 - \frac{1}{p_r})$$
$$= m(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r})$$

정리 15 양의 정수 m에 대하여 다음이 성립한다.

$$\sum_{d \mid m} \varphi(d) = \sum_{d \mid m} \varphi(\frac{m}{d}) = m$$

여기서, $\sum_{d \mid m}$ 은 m의 양의 약수 d 전체에 대한 합을 나타낸다.