6강. 합동식(三)

$a \equiv b \pmod{m}$ ↳ 법(modulus) 동일

↳ congruent (congruence)

ex) $7 \equiv 4 \pmod{3}$, $6 \equiv 1 \pmod{5}$

$\Leftrightarrow$ ① (a를 m으로 나눈 나머지)와
(b를 m으로 나눈 나머지)가 서로 같다.

$\Leftrightarrow$ ② $m \mid (a-b)$

pf) ① $\Rightarrow$ ② $a = q_1 m + r$, $b = q_2 m + r$ $\quad a-b = m(q_1 - q_2)$, $m \mid (a-b)$

② $\Rightarrow$ ① $a = q_1 m + r_1$, $0 \le r_1 < m$

$b = q_2 m + r_2$, $0 \le r_2 < m$

$m \mid (a-b) = m(q_1 - q_2) + r_1 - r_2 \Rightarrow m \mid r_1 - r_2$ ↳ m의 배수

$|r_1 - r_2| < m$

$\Rightarrow -m < r_1 - r_2 < m$

$-2m \quad -m \quad 0 \quad m \quad 2m$

$r_1 - r_2 = 0 \Rightarrow r_1 = r_2$

* $x \mid a,\ x \mid b \Rightarrow x \mid a \pm b$

pf) $a = xk_1,\ \exists k_1 \in \mathbb{Z}$, $b = xk_2,\ \exists k_2 \in \mathbb{Z}$.

$x \mid a \pm b = x(k_1 \pm k_2)$

*합동식의 성질 (二)

① 이항 법칙

$a = b \quad 0 = b - a$

$a - a = b - a$

*합동식의 이항법칙

$a \equiv b \pmod{m} \Rightarrow a \pm c \equiv b \pm c \pmod{m}$

pf) $a \equiv b \pmod{m} \Longleftrightarrow m \mid a - b + c - c$

$\Longleftrightarrow m \mid (a \pm c) - (b \pm c)$

$\Longleftrightarrow a \pm c \equiv b \pm c \pmod{m}$

* $a \equiv b \pmod{m} \qquad x \equiv y \pmod{m}$

$a \pm x \equiv b \pm y \pmod{m}$

pf) $a \equiv b \pmod{m},\ x \equiv y \pmod{m}$

$\Leftrightarrow m \mid a - b,\ m \mid x - y$

$\Leftrightarrow m \mid (a-b) + (x-y) \Longleftrightarrow a + x \equiv b + y \pmod{m}$

$= (a+x) - (b+y)$

* $a \equiv b \pmod{m}$ $\quad c_1 \equiv c_2 \pmod{m}$

$a \cdot c_1 \equiv b \cdot c_2 \pmod{m}$

pf) $a \equiv b \pmod{m} \iff m \mid a-b \Rightarrow m \mid (a-b)c_1$

$c_1 \equiv c_2 \pmod{m} \iff m \mid c_1 - c_2 \Rightarrow m \mid b \cdot (c_1 - c_2)$

$m \mid ac_1 - bc_2$ $\quad \Rightarrow m \mid ac_1 - \cancel{bc_1}$

$m \mid \cancel{bc_1} - bc_2$

$\Rightarrow m \mid ac_1 - bc_2$

* $a\cancel{c} \equiv b\cancel{c} \pmod{m} \not\Rightarrow a \equiv b \pmod{m}$

$6 \cdot \cancel{2} \equiv 13 \cdot \cancel{2} \pmod{14}$ $\quad 6 \not\equiv 13 \pmod{14}$

$12 \equiv 26 \pmod{14}$

$\begin{array}{r} 26 \\ -14 \\ \hline 12 \end{array}$

$AB = BA = I$ $\quad A \cdot (A^{-1}) = (A^{-1}) \cdot A$