정수론 10강 일차 합동식

$ax = c \qquad x = \frac{c}{a}$

$ax \equiv c \pmod m \Rightarrow x \equiv \frac{c}{a} \pmod m$

정수환에서는 곱셈에 대한 역원이 항상 존재하지는 않는다.

$AX = C \qquad X = A^{-1}C$

↳ 가역행렬

$\Rightarrow$ $ax \equiv c \pmod m$를 만족하는 x를 찾자.

$\Leftrightarrow$ $m \mid (ax-c)$를 만족하는 x를 찾자.

$\Leftrightarrow$ $ax - c = k \cdot m$ 가 되게 하는 k와 x를 찾자.

$ax - mk = c$

$ax + m\cdot(-k) = c \qquad \gcd(a,m) = g$

i) $g \nmid c \Rightarrow$ 해가 없다.

$ax + by = c \Rightarrow (x_0 + k\cdot\frac{b}{g},\ y_0 - k\cdot\frac{a}{g})$

ii) $g \mid c \Rightarrow x_0, -k_0$

$(x_0 + n\cdot\frac{m}{g},\ \boxed{-k_0 - n\cdot\frac{a}{g}})$

$x = x_0 + n\cdot\frac{m}{g}$

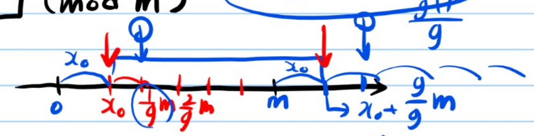
$ax \equiv c\ (\boxed{\bmod m})$ → 합동식 mod m $\underline{0 \sim m-1}$

$103 \equiv \bigcirc \pmod m$

$x = x_0 + n\cdot\frac{m}{g} \qquad n = 0, 1, \cdots, g-1, g$

$0, \frac{1}{g}m, \frac{2}{g}m, \frac{3}{g}m, \cdots, \frac{g}{g}m$

$x \equiv \square \pmod m \qquad \frac{g+1}{g}$



$x \equiv x_0 + n\frac{m}{g} \pmod m \qquad x_0 \equiv x_0 + \frac{g}{g}m \pmod m$

$0 \sim g-1 \qquad g$개

$ax \equiv c \pmod m \qquad \gcd(a,m) \mid c$

$x \equiv x_0 + k\cdot\frac{m}{g} \pmod m \qquad k = \underline{0 \sim g-1}$

확장된 유클리드 알고리즘

ex) $7x \equiv 4 \pmod{14}$

$\gcd(7,14) = 7 \qquad 7 \nmid 4 \Rightarrow$ 해가 없다.

ex) $12x \equiv 8 \pmod 4$

$\gcd(12,4) = 4 \qquad 4 \mid 8$

$4 \mid 12x - 8 \Rightarrow 12x - 8 = 4k$

$12x - 4k = 8$

$12x + 4\cdot(-k) = 8$

x	$-k$	$12x-4k$
1	0	12
0	1	4
1	-3	0

$-3\times$

$x = 0, k = -2$

$(x = 0, k = -1) \times 2$

$12x - 4k = 4$

$12x - 4k = 8$

$x_0 = 0$

$12x \equiv 8 \pmod 4$

$x \equiv 0 + k\cdot\frac{4}{4} \pmod 4 \qquad 4$

$\equiv k \pmod 4 \qquad k = 0 \sim g-1$

$\equiv 0, 1, 2, 3 \pmod 4 = 0 \sim 3$

$12 \cdot 0 \equiv 8 \pmod 4$

$0 \equiv 0$

$\underline{12} \equiv \underline{8} \pmod{4}$ $\quad 12 \cdot 2$