현빈 : 15 수의 합동 (3)

April 7, 2015

6 중국인의 나머지 정리 (The Chinese Remainder Theorem)

예시 31)

다음과 같은 문제를 풀어보자.

> 5으로 나누었을 때의 나머지가 1이고, 6으로 나누었을 때의 나머지가 2이고, 7로 나누었을 때의 나머지가 3인 숫자를 구하여라.

이 문제는 다음 연립 일차 합동식을 푸는 것과 같다.

$$x \equiv 1 \pmod{5} \tag{1}$$

$$x \equiv 2 \pmod{6} \tag{2}$$

$$x \equiv 3 \pmod{7} \tag{3}$$

(1)에 의해 $x = 5t + 1$이다. 이를 (2)에 넣으면

$$5t + 1 \equiv 2 \pmod{6}$$

이고 1을 이항하면

$$5t \equiv 1 \pmod{6}$$

이다. 따라서 t는 5의 역원인 5이다$\pmod 6$. 즉

$$t \equiv 5 \pmod{6}$$

혹은

$$t = 6u + 5$$

이다. 따라서

$$x = 5(6u + 5) + 1 = 30u + 26$$

이다. 이것을 다시 (3)에 넣으면

$$30u + 26 \equiv 3 \pmod{7}$$

이고 $30 \equiv 2 \pmod{7}$ 이므로

$$2u \equiv 30u \equiv 3 - 26 \equiv -23 \equiv 5 \pmod{7}$$

이다. 양변에 $2^{-1}(\equiv 4)$를 곱하면

$$u \equiv 20 \equiv 6 \pmod{7}$$

따라서

$$u = 7v + 6$$

이고

$$x = 30(7v + 6) + 26 = 210v + 206$$

이다. 즉

$$x \equiv 206 \pmod{210}$$

인 모든 정수이다.

이와 같은 문제를 푸는 일반적인 해법은 5세기 남북조 시대의 중국 수학서 ≪손자산경(孫子算經)≫에 최초로 등장하였다. 따라서 "중국인의 나머지 정리"라는 이름으로 불린다.

정리 32) 중국인의 나머지 정리(The Chinese Remainder Theorem)

$m_1, m_2, m_3, \cdots, m_r$이 자연수이고 임의의 두 쌍의 m_i, m_j가 서로소이다. (즉 $i \neq j$이면 $(m_i, m_j) = 1$이다.) $M = m_1 \cdots m_r$이라고 하자. 그러면 다음 연립 합동 방정식의 해는 mod M에 대해 유일하게 존재한다.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

증명). 먼저 이 연립 합동 방정식의 해가 존재함을 밝히고, 그 다음에 그 해가 mod M에 대해 유일하다는 것을 밝히면 된다.

(존재성) :
임의의 k에 대해 $(1 \leq k \leq r)$

$$M_k = M/m_k$$

라고 하자. 가정에 의해

$$(M_k, m_k) = 1$$

이다. 따라서 mod m_k에서 M_k의 역원 y_k가 존재한다. 즉

$$M_k y_k \equiv 1 \pmod{m_k}$$

이다. 그러면

$$x = a_1 M_1 y_1 + \cdots + a_r M_r y_r$$

이 연립 합동 방정식을 만족한다.

(유일성) :
만약 x, x'이 모두 연립 합동 방정식의 근이라면,

$$\begin{aligned} m_1 &\mid x - x' \\ m_2 &\mid x - x' \\ &\vdots \\ m_r &\mid x - x' \end{aligned}$$

이다. 따라서

$$M \mid x - x'$$

이고,

$$x \equiv x' \pmod{M}$$

□

예시 33)

연립 합동 방정식

$$x \equiv 1 \pmod{3}$$
$$x \equiv 2 \pmod{5}$$
$$x \equiv 3 \pmod{7}$$

을 생각하자. $M = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, $M_3 = 105/7 = 15$ 이다. 또 $35y_1 \equiv 1 \pmod{3}$ 를 풀면 $y_1 \equiv 2 \pmod{3}$ 이고, 마찬가지로 $y_2 \equiv 1 \pmod{5}$, $y_3 \equiv 1 \pmod{7}$ 이다. 따라서

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 151 \equiv 52 \pmod{105}$$

이다.

연습문제 34)

다음 연립 합동 방정식을 풀어라.

(1)

$$x \equiv 4 \pmod{11}$$
$$x \equiv 3 \pmod{17}$$

(2)

$$x \equiv 1 \pmod{2}$$
$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$

(3)

$$x \equiv 0 \pmod{2}$$
$$x \equiv 0 \pmod{3}$$
$$x \equiv 1 \pmod{5}$$
$$x \equiv 6 \pmod{7}$$