Linear Congruences

Lemma : (5.3)

Let $d = (a, m)$. If $d \mid b$, then $ax \equiv b \mod m$ has d solutions.

Proof. Suppose $(a, m) = d$ and $d \mid b$. Thus, $\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$. Note that $\left(\frac{a}{b}, \frac{m}{d}\right) = 1$ so this second congruence has a unique solution r.

Let r be a solution of the first / second congruence. Let s be a solution of $ax \equiv b \mod m$.

$$\begin{aligned} as &\equiv ar \mod m \\ s &\equiv r \mod \frac{m}{d} \qquad \text{from Theorem 4.5} \end{aligned}$$

By the definition of congruence, $\frac{m}{d} \mid (s - r)$. $s - r = k\left(\frac{m}{d}\right)$, so $s = r + k\left(\frac{m}{d}\right), 0 \leq k \leq d-1$. We also have that $r < \frac{m}{d}$ from the second congruence equation.

$$\begin{aligned} s &= r + k\left(\frac{m}{d}\right) \\ &< \frac{m}{d} + (d-1)\left(\frac{m}{d}\right) \\ &= \frac{m}{d} + m - \frac{m}{d} \\ s &< m \end{aligned}$$

So, $s = r + k\left(\frac{m}{d}\right), 0 \leq k \leq d - 1$ are all of the solutions of the original equation. □

Example

Find all the solutions of $5x \equiv 10 \mod 15$.

$(5, 15) = 5$ and $5 \mid 10$, so there should be 5 equations.

$$x \equiv 5 \mod 3$$

So, the 5 solutions are: $x = 2, x = 5, x = 8, x = 11, x = 14$.

Example

Find all the solutions of $9x \equiv 15 \mod 24$.

$(9, 24) = 3$ and $3 \mid 15$, so there should be 3 solutions.

$$\begin{aligned} 3x &\equiv 5 \mod 8 \\ 3x &\equiv 13 \mod 8 \\ 3x &\equiv 21 \mod 8 \\ x &\equiv 7 \mod 8 \end{aligned}$$

So, the 3 solutions are: $x = 7, x = 15, x = 23$.

Example

Find x such that $x \equiv 1 \mod 3$, $x \equiv 2 \mod 5$, and $x \equiv 3 \mod 7$.

The first congruence gives $x = 1 + 3k_1$, now plug this into the second congruence.

$$\begin{aligned} x &\equiv 2 \mod 5 \\ 1 + 3k_1 &\equiv 2 \mod 5 \\ 3k_1 &\equiv 1 \mod 5 \\ 3k_1 &\equiv 6 \mod 5 \\ k_1 &\equiv 2 \mod 5 \end{aligned}$$

This congruence gives $k_1 = 2 + 5k_2$.

$$\begin{aligned} x &= 1 + 3k_1 \\ &= 1 + 3(2 + 5k_2) \\ &= 1 + 6 + 15k_2 \\ &= 7 + 15k_2 \end{aligned}$$

Plugging this into the third congruence gives:

$$\begin{aligned} x &\equiv 3 \mod 7 \\ 7 + 15k_2 &\equiv 3 \mod 7 \\ 15k_2 &\equiv 3 \mod 7 \\ 5k_2 &\equiv 1 \mod 7 \\ 5k_2 &\equiv 8 \mod 7 \\ 5k_2 &\equiv 15 \mod 7 \\ k_2 &\equiv 3 \mod 7 \end{aligned}$$

This congruence gives us $k_2 = 3 + 7k_3$.

$$\begin{aligned} x &= 7 + 15k_2 \\ &= 7 + 15(3 + 7k_3) \\ &= 7 + 45 + 105k_3 \\ &= 52 + 105k_3 \end{aligned}$$

This means, $x \equiv 52 \mod 105$, and that $x = 52$ is the unique solution.

Theorem : The Chinese Remainder Theorem

The linear congruence system

$$x \equiv a_1 \mod m_1, \qquad x \equiv a_2 \mod m_2, \quad \dots \quad , x = a_n \mod m_n$$

has a unique solution modulo $m_1 \times m_2 \times \cdots \times m_n$ if for each (m_i, m_j), where $i \neq j$, $(m_i, m_j) = 1$.

Proof. The result is trivial when $n = 1$. If $n = 2$, then

$$x \equiv a_1 \mod m_1 \quad \text{and} \quad x \equiv a_2 \mod m_2$$

where m_1 and m_2 are relatively prime. From the first congruence, we have that $x = a_1 + k_1 m_1$

$$\begin{aligned} x &\equiv a_2 \mod m_2 \\ a_1 + k_1 m_1 &\equiv a_2 \mod m_2 \\ k_1 m_1 &\equiv a_2 - a_1 \mod m_2 \end{aligned}$$

k_1 is the variable, and since (m_1, m_2), there is a unique solution we will call t. Note, $k_1 = t + k_2 m_2$

$$\begin{aligned} x &= a_1 + k_1 m_1 \\ &= a_1 + (t + k_2 m_2)(m_1) \\ &= a_1 + t m_1 + k_2 m_2 m_1 \\ &\equiv a_1 + t m_1 \mod m_1 m_2 \end{aligned}$$

satisfies both equations.

Suppose the result holds for $n - 1$ equations:

$$x \equiv a_1 \mod m_1 \quad \dots \quad x \equiv a_{n-1} \mod m_{n-1}$$

Has a solution $x \equiv s \mod m_1 \times \cdots \times m_{n-1}$. Now suppose you have another congruence, $x \equiv a_n \mod m_n$. This creates a system of two congruences which we already proved has a unique solution modulo $(m_1 \times \cdots \times m_{n-1}) \cdot (m_n)$.

Now, for uniqueness. Suppose r and s are solutions.

$$r \equiv s \mod m_1, \quad \dots, \quad r \equiv s m_k$$

$$r - s \equiv 0 \mod m_1 \quad \dots, \quad r - s \equiv 0 \mod m_k$$

$$m_1 \mid (r - s), \quad m_2 \mid (r - s), \quad \dots, \quad m_k \mid (r - s)$$

Thus, $m_1 \times m_2 \times \cdots \times m_k \mid (r - s)$ since $(m_i, m_j), i \neq k$

$$0 \leq r < m_1 \times m_2 \times \cdots \times m_k, \quad 0 \leq s < m_1 \times m_2 \times \cdots \times m_k$$

$$-m_1 \times m_2 \times \cdots \times m_k < r - s < m_1 \times m_2 \times \cdots \times m_k$$

$$r - s = 0 \Rightarrow r = s$$

□

The Chinese Remainder Theorem is very efficient for computers. It is helpful in error correcting codes, signal processing, RSA algorithms, etc.