

1. Find the solutions of the system of congruences $x \equiv 4 \pmod{6}$ and $x \equiv 13 \pmod{15}$.

Solution: Can you use the Chinese Remainder Theorem directly ? **NO!** This is because 6 and 15 are not relatively prime. We have to factorize these two numbers: $6 = 2 \times 3$ and $15 = 3 \times 5$. So we get the following system of congruences:

$$x \equiv 0 \pmod{2}$$

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

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

$$M_1 = 15, a_1 = 0; m_1 = 2, y_1 = 1$$

$$M_2 = 10, a_2 = 1; m_2 = 3, y_2 = 1$$

$$M_3 = 6, a_3 = 3; m_3 = 5, y_3 = 1$$

So the solution is:

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 = 0 + 10 + 3 \times 6 \pmod{30} \equiv 28 \pmod{30}.$$

2. Show that the system of congruences $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$ has a solution if and only if $\gcd(m_1, m_2) \mid (a_1 - a_2)$.

Solution: \rightarrow : From $x \equiv a_1 \pmod{m_1}$

and $x \equiv a_2 \pmod{m_2}$ we have $x = a_1 + sm_1 = a_2 + tm_2$ for some integers s and t . So $a_1 - a_2 = tm_2 - sm_1$. Therefore, $\gcd(m_1, m_2) | (a_1 - a_2)$.

\leftarrow : From $\gcd(m_1, m_2) | (a_1 - a_2)$ we have $a_1 - a_2 = k\gcd(m_1, m_2) = ksm_1 + ktm_2$. So $a_1 - ksm_1 = a_2 + ktm_2 = x$. Therefore, $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$.

3. Show that an inverse of $a \pmod{m}$ does not exist if $\gcd(a, m) > 1$.

Solution: Prove by contradiction. Suppose the inverse exists and it is y such that $ay \equiv 1 \pmod{m}$. So $ay - 1 = km$ for some integer k . Rearranging $1 = ay - km$. Therefore, $\gcd(a, m) | 1$ and $\gcd(a, m) > 1$, a contradiction.

4. Show that $ac \equiv bc \pmod{m}$, where a, b, c and m are integers with $m \geq 2$, does not necessarily imply $a \equiv b \pmod{m}$.

Solution: Let $a = 3, b = 1, c = 2$ and $m = 4$, we have $3 \times 2 \equiv 1 \times 2 \pmod{4}$ but $3 \equiv 1 \pmod{4}$ is not true.

It is true only when $\gcd(c, m) = 1$.

5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then we have $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$. The following is also true:
 $a^k \equiv b^k \pmod{m}$ for positive integer k .

This is very useful.

6. $a_k \equiv b_k \pmod{m}$ for $1 \leq k \leq n$, then
 $a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{m}$
 $a_1 \times \cdots \times a_n \equiv b_1 \times \cdots \times b_n \pmod{m}$.