3.27 Theorem. Let $a, b, m, n \in \mathbb{Z}$ with $m, n > 0$. Then the system

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

has a solution if and only if $(n, m)|(a - b)$.

Proof. Let the system

$$\begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

have a solution. Since $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$,
$x = a + nt = b + mu$ for $t, u \in \mathbb{Z}$. Thus,

$$\begin{aligned} nt + a &= mu + b, \\ a - b &= mu - nt. \end{aligned}$$

By Theorem 1.48, $(n, m)|(a - b)$.

Now let $(n, m)|(a - b)$ be given. By definition, $a - b = (n, m)k$ for $k \in \mathbb{Z}$. By Theorem 1.40, there exists $t', u' \in \mathbb{Z}$ such that $(n, m) = nt' + mu'$. Thus,

$$\begin{aligned} a - b &= (nt' + mu')k \\ &= nt'k + mu'k, \\ a - nt'k &= b + mu'k. \end{aligned}$$

By CPI, let integers $x = a - nt'k = b + mu'k$, $T = -t'k$, and $U = u'k$. We have

$$\begin{aligned} x &= nT + a & \qquad x &= mU + b, \\ x - a &= nT & \qquad x - b &= mU. \end{aligned}$$

By definition, $x \equiv a \pmod{n}$ and $x \equiv b \pmod{m}$. Thus, the system has a solution if and only if $(n, m)|(a - b)$. $\square$