Linear Congruences $\quad ax \equiv b \mod m$

Theorem 1. *If $(a, m) = 1$, then the congruence $ax \equiv b \mod m$ phas exactly one solution modulo m.*

Constructive. Solve the linear system

$$sa + tm = 1.$$

Then

$$sba + tbm = b.$$

So

$$sba \equiv b \pmod m$$

gives the solution $x = sb$.

If u_1 and u_2 are solutions, then

$$\begin{aligned} & au_1 \equiv b \pmod m \text{ and } au_2 \equiv b \pmod m \\ \Longrightarrow\ & au_1 \equiv au_2 \pmod m \\ \Longrightarrow\ & u_1 \equiv u_2 \pmod m \quad \text{since } (a, m) = 1. \end{aligned}$$

So there is only one solution. $\square$ $\square$

Example 1. $3x \equiv 50 \pmod{113}$

Note that $ax \equiv b \pmod m$ implies $ax = b + qm$ for some integer q. So a common divisor of a, m also divides b.

Example 2. $5x \equiv 1 \pmod{15}$ is not solvable.

Theorem 2. *Consider the congruence $ax \equiv b \pmod m$.*

1. *The congruence has a solution if and only if $(a, m) \mid b$.*

2. *If u_0 is any particular solution, then a complete set of solutions is:*

$$u_0, u_0 + \frac{m}{g}, u_0 + \frac{2m}{g}, \ldots, u_0 + \frac{(g-1)m}{g}$$

where $g = (a, m)$. Thus there are g solutions.

3. *A particular solution u_0 can be obtained by solving the congruence*

$$\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{m}{g}}$$

This is possible since $\left(\frac{a}{g}, \frac{m}{g}\right) = 1$. (See last theorem.)

Example 3. $42x \equiv 12 \pmod{78}$

Proof.
1. If $ax \equiv b \pmod{m}$ has a solution and $g = (a, m)$, then clearly $g|b$. $\square$

3. Suppose $g = (a, m)$ and $g|b$.
Then $\left(\frac{a}{g}, \frac{m}{g}\right) = 1$. So we can find a u_0 such that
$\dfrac{a}{g}u_0 \equiv \dfrac{b}{g} \pmod{\dfrac{m}{g}}$
Therefore, $au_0 \equiv b \pmod{m}$. $\square$

2. Suppose u_0 is a solution. Then

$$\begin{aligned}
&u = u_0 + t\frac{m}{g} \\
\Longrightarrow\ &au = au_0 + at\frac{m}{g} \\
\Longrightarrow\ &au = au_0 + \frac{a}{g}tm \\
\Longrightarrow\ &au = au_0 \pmod{m} \\
\Longrightarrow\ &au = b \pmod{m}.
\end{aligned}$$

So u is a solution.

Suppose, on the other hand, that u is a solution. Then

$$\begin{aligned}
&au \equiv au_0 \equiv b \pmod{m} \\
\Longrightarrow\ &a(u - u_0) \equiv 0 \pmod{m} \\
\Longrightarrow\ &\frac{a}{g}(u - u_0) \equiv 0 \pmod{\frac{m}{g}} \\
\Longrightarrow\ &u - u_0 \equiv 0 \pmod{\frac{m}{g}} \\
\Longrightarrow\ &u - u_0 = t\frac{m}{g}.
\end{aligned}$$

Let $j \equiv t \pmod{g}$ where $0 \le j \le g - 1$. Then

$$\begin{aligned}
&t\frac{m}{g} \equiv j\frac{m}{g} \pmod{m} \\
\Longrightarrow\ &u - u_0 \equiv j\frac{m}{g} \pmod{m} \\
\Longrightarrow\ &u \equiv u_0 + j\frac{m}{g} \pmod{m},
\end{aligned}$$

where $0 \le j \le g - 1$.

It is easy to check that no two of the numbers $u_0 + j\dfrac{m}{g} \quad (0 \le j < g)$ are congruent modulo m. $\square$