Linear congruences

Recall that $a \equiv b \bmod m$ if and only if $a - b$ is divisible by m, which we abbreviate as $m|\left(a-b\right)$.

Definition. A **linear congruence** is an equation of the form

$$ax \equiv b \text{ mod } m.$$

We wish to find all integers x which satisfy this equation.

First some basic results about congruence.

Lemma 1. If $b \equiv c$ mod m and $n|m$, then $b \equiv c$ mod n.

Example 1. $27 \equiv 7$ mod 10 implies $27 \equiv 7$ mod 5 and $27 \equiv 7$ mod 2.

Proof. $m|\left(b-c\right)$ and $n|m$ implies $n|\left(b-c\right)$. (basic property about division)

Lemma 2. If $b \equiv c$ mod n, then $ab \equiv ac$ mod an.

Example 2. $27 \equiv 7$ mod 10 implies $108 \equiv 28$ mod 40.

Proof. $n|\left(b-c\right)$ and implies $an|a\left(b-c\right)$, so that $an|\left(ab-ac\right)$.

Facts:

(a) $a, m \in \mathbb{Z}^+$ and $g = \gcd\left(a,m\right)$ implies $\gcd\left(\frac{a}{g}, \frac{m}{g}\right) = 1$.

Example a. $\gcd\left(\frac{15}{3}, \frac{21}{3}\right) = 1$.

(b) $a|bc$ and $\gcd\left(a,b\right) = 1$ implies $a|c$.

Proposition 3. Suppose $a, m \in \mathbb{Z}^+$, $g = \gcd\left(a,m\right)$, and $b, c \in \mathbb{Z}$. Then $ab \equiv ac$ mod m if and only if $b \equiv c$ mod $\frac{m}{g}$.

Example 3. $4x \equiv 12$ mod 14 if and only if $x \equiv 3$ mod 7. Thus the solutions to this equation are $\{\ldots, -11, -4, 3, 10, 17, \ldots\}$.

Proof. **(⇐)** $b \equiv c$ mod $\frac{m}{g}$ implies (Lemma 2) $ab \equiv ac$ mod $\frac{a}{g}m$. This implies (Lemma 1) $ab \equiv ac$ mod m.

(⇒) $ab \equiv ac$ mod m implies $m|\left(ab-ac\right)$, which implies $m|a\left(b-c\right)$, which implies $\frac{m}{g}|\frac{a}{g}\left(b-c\right)$. Since $\gcd\left(\frac{a}{g}, \frac{m}{g}\right) = 1$ (Fact a), we conclude $\frac{m}{g}|\left(b-c\right)$ (by Fact b).

Special cases of this proposition:

Corollary 4. Suppose $a|m$. Then $ab \equiv ac$ mod m if and only if $b \equiv c$ mod $\frac{m}{a}$.

Example 4. $3b \equiv 3c$ mod 12 if and only if $b \equiv c$ mod 4.

Corollary 5. Suppose $\gcd\left(a,m\right) = 1$. Then $ab \equiv ac$ mod m if and only if $b \equiv c$ mod m.

Example 5. $3b \equiv 3c$ mod 10 if and only if $b \equiv c$ mod 10.

Lemma 6. Let $k \in \mathbb{Z}$. Then $ax \equiv b$ mod m if and only if $ax \equiv b + km$ mod m. (proof is easy)

Example 6. $2x \equiv 5$ mod 7 if and only if $2x \equiv 12$ mod 7 (we saw this earlier).

Now we solve a linear congruence: Consider

$$6x \equiv 15 \bmod 21.$$

This is equivalent to

$$\begin{gathered} 2x \equiv 5 \mod 7 \\ \Leftrightarrow \\ 2x \equiv 2 \cdot 6 \mod 7 \\ \Leftrightarrow \\ x \equiv 6 \mod 7. \end{gathered}$$

Consider the general method for solving a linear congruence

$$ax \equiv b \mod m.$$

Let $g = \gcd(a, m)$.

CASE 1. g does not divide b.

Lemma 7. If g does not divide b, then there are no solutions. In other words, if there exists a solution, then $g|b$.

Example 7. The linear congruence $6x \equiv 4 \bmod 21$ has no solutions since 3 does not divide 4.

Proof. Suppose there exists a solution x. Then $m|(ax - b)$, which implies there exists $y \in \mathbb{Z}$ such that

$$my = ax - b,$$

which implies there exists $y \in \mathbb{Z}$, $b = ax - my$, which implies $g|b$.

CASE 2. g divides b.

Then

$$\frac{a}{g}x \equiv \frac{b}{g} \mod \frac{m}{g}.$$

Note that $\gcd\left(\frac{a}{g}, \frac{m}{g}\right) = 1$.

Thus we are reduced to considering how to solve $ax \equiv b \bmod m$ when $\gcd(a, m) = 1$.

Lemma 8. If $\gcd(a, m) = 1$, then there exists $c \in \mathbb{Z}$ such that

$$b \equiv ac \mod m.$$

How to use the lemma: Consider $2x \equiv 5 \bmod 7$. Since $\gcd(2, 7) = 1$, there exists $c \in \mathbb{Z}$, $5 \equiv 2c \bmod 7$. Indeed, take $c = 6$.

Proof. Since $\gcd(a, m) = 1$, there exist $x, y \in \mathbb{Z}$ such that $ax + my = 1$. Hence

$$axb + myb = b.$$

This implies that

$$a \cdot xb \equiv b \mod m.$$

Now take $c = xb$.