Linear Congruences

A linear congruence is of the form

$$ax \equiv b \mod m$$

This has a solution if and only if there are integers x and k such that

$$ax = b + km$$

$$\Leftrightarrow ax - km = b$$

These can be viewed as Diophantine equations.

If one integer satisfies $ax \equiv b \mod m$, then there are infinitely many.

The table below shows $5x \equiv 4 \mod 7$ has a solution of $x = 5$.

x	0	1	2	3	4	5	6
$5x$	0	5	3	1	6	4	2

Let $r \in \mathbb{Z}$, $y = x + rm$. Suppose $ax \equiv b \mod m$

$$\begin{aligned} ay &\equiv a(x + rm) \mod m \\ &\equiv ax + arm \mod m \\ &\equiv ax \mod m \\ &\equiv b \mod m \end{aligned}$$

The solutions of linear congruences are the solutions that are the least residues modulo m. Therefore, the only solution to $5x \equiv 4 \mod 7$ is $x = 5$.

The linear congruence $ax \equiv b \mod m$, may have no solutions, exactly one solution, or many solutions.

- $2x \equiv 1 \mod 5$ is satisfied by $x = 3$
- $2x \equiv 1 \mod 8$ has no solutions
- $2x \equiv 4 \mod 6$ has two solutions, $x = 2$, and $x = 5$.

Lemma : (5.1)

If $(a, m) \nmid b$, then $ax \equiv b \mod m$ has no solutions.

Proof. By contraposition, suppose there is a solution. Suppose that $ax \equiv b \mod m$. By the definition of congruence, $m \mid (ax - b)$. By divisibility, $ax - b = km$. Consider (a, m). $(a, m) \mid ax$, and $(a, m) \mid km$, thus, $(a, m) \mid b$. □

Lemma : (5.2)

If $(a, m) = 1$, then $ax \equiv b \mod m$ has exactly one solution.

Proof. Suppose that $(a, m) = 1$, we know there exists r and s such that:

$$ar + ms = 1$$

$$arb + msb = b$$

$$arb \mod m \equiv b \mod m$$

Let $x = rb$, then $ax \equiv b \mod m$.

Suppose p and q are solutions.

$$ap \equiv b \mod m \qquad aq \equiv b \mod m$$

$$ap \equiv aq \mod m$$

Since $(a, m) = 1$,

$$p \equiv q \mod m, \quad 0 \leq p < m, \quad 0 \leq q < m$$

$$m \mid (p - q) \qquad -m < p - q < m$$

Thus, $p = q$, so they are the same solution. Thus, the solution is unique. □

Example

How many solutions does each congruence have?
a) $3x \equiv 1 \mod 10$
b) $4x \equiv 1 \mod 10$
c) $5x \equiv 1 \mod 10$
d) $7x \equiv 1 \mod 10$

---

a) Since $(3, 10) = 1$, $3x \equiv 1 \mod 10$ has exactly one solution
b) Since $(4, 10) = 2$, and $2 \nmid 1$, $4x \equiv 1 \mod 10$ has no solutions
c) Since $(5, 10) = 5$, and $5 \nmid 1$, $5x \equiv 1 \mod 10$ has no solutions
d) Since $(7, 10) = 1$, $7x \equiv 1 \mod 10$ has exactly one solution.

Example

What is the solution of $14x \equiv 27 \mod 31$?

$(14, 31) = 1$, so there is one solution.

$$\begin{aligned} 14x &\equiv 27 \mod 31 \\ 7 \cdot 2 \cdot x &\equiv 27 \mod 31 \\ 7 \cdot 2 \cdot x &\equiv 58 \mod 31 \\ 7 \cdot x &\equiv 29 \mod 31 \\ 7 \cdot x &\equiv 60 \mod 31 \\ 7 \cdot x &\equiv 91 \mod 31 \\ x &\equiv 13 \mod 31 \end{aligned}$$

The equation $ax + by = c$ implies the two congruences:

$$ax \equiv c \mod b \quad \text{and} \quad by \equiv c \mod a$$

We can choose one equation, solve for the variable, and then substitute the result into the original equation to get all the solutions.

Example

Find all integer solutions of:

$$9x + 16y = 35$$

$$\begin{aligned} ax &\equiv c \mod b \\ 9x &\equiv 35 \mod 16 \\ 9x &\equiv 3 \mod 16 \\ 3x &\equiv 1 \mod 16 \\ 3x &\equiv 17 \mod 16 \\ 3x &\equiv 33 \mod 16 \\ x &\equiv 11 \mod 16 \end{aligned}$$

$$x = 11 + 16t$$

$$\begin{aligned} 9x + 16y &= 35 \\ 9(11 + 16t) + 16y &= 35 \\ 99 + 144t + 16y &= 35 \\ 16y &= -64 - 144t \\ y &= -4 - 9t \end{aligned}$$

Here, $(11, -4)$ is a particular solution.

Example

Find all integer solutions of:

$$9x + 10y = 11$$

$$\begin{aligned} by &\equiv c \mod a \\ 10y &\equiv 11 \mod 9 \\ 10y &\equiv 2 \mod 9 \\ 5y &\equiv 1 \mod 9 \\ 5y &\equiv 10 \mod 9 \\ y &\equiv 2 \mod 9 \end{aligned}$$

$$y = 2 + 9t$$

$$\begin{aligned} 9x + 10y &= 11 \\ 9x + 10(2 + 9t) &= 11 \\ 9x + 20 + 90t &= 11 \\ 9x &= -9 - 90t \\ x &= -1 - 10t \end{aligned}$$

Here, $(-1, 2)$ is a particular solution.