Linear Congruences

A congruence of the form

$$ax \equiv b \pmod{m} \quad \text{--- (1)}$$

where x is an unknown integer is called a linear congruence in one variable.

Suppose x_0 is a solution of (1).

Then, $ax_0 \equiv b \pmod{m}$.

Suppose $x_1 \equiv x_0 \pmod{m}$.

Then, $ax_1 \equiv ax_0 \equiv b \pmod{m}$

$\therefore ax_1 \equiv b \pmod{m}$

$\therefore x_1$ is a solution.

Note that,

$a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$

$\Rightarrow a \equiv c \pmod{m}$.

In this situation, we may write

$$a \equiv b \equiv c \pmod{m}$$

For example, $12 \equiv 2 \equiv -3 \equiv \pmod{5}$

ex: $3x \equiv 2 \pmod{5}$

$x=4$ is a solution.
Since $9 \equiv 4 \pmod 5$, it follows that $x=9$ is also a solution

<u>Theorem 4.11</u>: Let $a, b \in \mathbb{Z}$, $m \in \mathbb{Z}^+$ and $d = \gcd(a,m)$.

(i) If $d \nmid b$ then $ax \equiv b \pmod m$ has no solutions.

(ii) If $d \mid b$, then $ax \equiv b \pmod m$ has exactly d incongruent solutions modulo m.

Proof: (a) First note that

$$ax \equiv b \pmod m \iff \exists\, y \text{ s.t. } ax - my = b$$

This implies that,

"$ax \equiv b \pmod m$ has a solution for x if and only if $ax - my = b$ has solutions for x and y".

By Theorem 3.23, $ax - my = b$ has a solution if and only if $d = \gcd(a,m)$ divides b.
Hence, if $d \nmid b$, then $ax \equiv b \pmod m$ has no solutions and if $d \mid b$ then

$ax - my = b$ has infinitely many solutions given by

$$x = x_0 + \left(\frac{m}{d}\right)t, \quad y = y_0 + \left(\frac{m}{d}\right)t$$

where $x = x_0$, $y = y_0$ is any solution of $ax - my = b$.

Then, $x = x_0 + \left(\frac{m}{d}\right)t$ is a solution of

$ax \equiv b \pmod{m}$.

$\therefore$ if $d \mid b$, then $ax \equiv b \pmod{m}$ has infinitely many solutions. Next we show that only d of these solutions are incongruent.

Consider 2 solutions $x_0 + \left(\frac{m}{d}\right)t_1$ and $x_0 + \left(\frac{m}{d}\right)t_2$.

Then $x_0 + \left(\frac{m}{d}\right)t_1 \equiv x_0 + \left(\frac{m}{d}\right)t_2 \pmod{m}$

$$\iff \left(\frac{m}{d}\right)t_1 \equiv \left(\frac{m}{d}\right)t_2 \pmod{m}$$

$$\iff t_1 \equiv t_2 \left(\bmod \frac{m}{d_0}\right)$$

where $d_0 = \gcd\left(\frac{m}{d}, m\right) = \frac{m}{d}$ since $\frac{m}{d}$ divides m. (Note: $m \mid n \Rightarrow \gcd(m,n) = m$)

$$\iff t_1 \equiv t_2 \pmod{d}$$

Hence, a complete set of incongruent solutions can be obtained by taking $x = x_0 + \left(\frac{m}{d}\right)t$, where t ranges through a complete system of

residues modulo d. One such set is
$x = x_0 + \left(\frac{m}{d}\right)t \;;\; t = 0, 1, 2, \dots, d-1.$

ex: Consider $4x \equiv 9 \pmod{8}$.
Since $\gcd(4,8) = 4 \nmid 9$, there are no solutions.

ex: $9x \equiv 21 \pmod{6}$
$\gcd(9,6) = \underset{\overset{\parallel}{d}}{3} \mid 21$, so it has solutions.
Let's find a set of incongruent solutions.
First, a particular solution is $x = 1$.
$\therefore$ solutions are given by

$$x = 1 + 2t \;;\; t \in \mathbb{Z}.$$

An incongruent set of solutions is

$$x = 1 + \underset{\uparrow = \frac{d}{m}}{2}t \;;\; t = 0, 1, 2$$

$\therefore x = 1, 3, 5$ is a set of incongruent solutions.

<u>Corollary</u> 4.11.1: Let $\gcd(a,m) = 1$ and $m > 0$. Then, $ax \equiv b \pmod{m}$ has a unique solution modulo m.

Proof: Since $\gcd(a,m) = 1$, the number of incongruent solutions is 1 (by Theorem 4.11). Hence, the solution is unique.

ex: Solve $9x \equiv 7 \pmod{13}$.

Note that $\gcd(9,13)=1$

$\therefore$ there is a unique solution modulo 13.

To find the solution, we can use Theorem 4.11. We should solve

$$9x - 13y = 7$$

Let's use the Euclidean algorithm.

$$13 = 9(1) + 4$$
$$9 = 4(2) + 1$$
$$4 = 1(4) + 0$$

$$\therefore 1 = 9 - 4(2)$$
$$= 9 - (13 - 9(1))(2)$$
$$= 9(3) - 13(2)$$

$$\therefore 9(3) - 13(2) = 1$$
$$\therefore 9(21) - 13(14) = 7$$

$\therefore x_0 = 21,\ y_0 = 14$ is a solution of the equation $9x - 13y = 7$.

$\therefore$ the unique solution (modulo 13) of the equation $9x \equiv 7 \pmod{13}$ is given by $x = 21$.

The smallest nonnegative solution (modulo 13) is given by $x=8$ since

$$21 \equiv 8 \pmod{13}$$

* If there is a unique solution modulo m, then all solutions are congruent modulo m.

Definition: The solutions of

$$ax \equiv 1 \pmod{m}$$

where $\gcd(a, m) = 1$, are called the inverses of the integer a modulo m.

* Note that, all inverses of an integer modulo m are congruent modulo m, since there is a unique solution modulo m.

ex: Consider $7x \equiv 1 \pmod{31}$.

Then, $x = 9$ is a solution.

$\therefore$ 9 is an inverse of 7 modulo 31.

Other inverses are all integers congruent to 9 modulo 31. For example, 40 and -22 are two such inverses.

* Said in a different way, an inverse of an integer x modulo m is an integer $\bar{x}$ such that $x\bar{x} \equiv 1 \pmod{m}$.

If we know an inverse of an integer a modulo m, then we can solve any congruence of the form

$$ax \equiv b \pmod{m}$$

as follows.

Let $\bar{a}$ be an inverse of a modulo m.

Then,

$$\bar{a}(ax) \equiv \bar{a}\,b \pmod{m}$$

$$\Rightarrow (\bar{a}a)x \equiv \bar{a}\,b \pmod{m}$$

$$\Rightarrow x \equiv \bar{a}\,b \pmod{m} \quad (\because \bar{a}a \equiv 1 \pmod{m})$$

<u>ex</u>: Solve $7x \equiv 22 \pmod{31}$.

We found in the previous example that

$$\bar{7} = 9 \text{ modulo } 31.$$

$$\therefore x \equiv 9 \times 22 \pmod{31}$$
$$\equiv 198 \pmod{31}$$
$$\equiv 12 \pmod{31}$$

Following theorem will be used later.

Theorem 4.12: Let p be a prime. The positive integer a is its own inverse modulo p if and only if

$$a \equiv 1 \pmod{p} \quad \text{or} \quad a \equiv -1 \pmod{p}.$$

Proof: exercise

ex: For any p, 1 is its own inverse modulo p. So is $p-1$.

For example, when $p = 5$,

$$1 \cdot 1 = 1 \pmod{5}$$

$$4 \cdot 4 \equiv 1 \pmod{5}$$

$\therefore$ 1 is its own inverse and 4 is its own inverse modulo 5.

ex: Solve $13x \equiv 1 \pmod{7}$

Note that, this is equivalent to

$$6x \equiv 1 \pmod{7}$$

since $13x = 6x + 7x \equiv 6x \pmod{7}$.

Multiply both sides by $\overline{6}$ to get

$$\overline{6}6x = \overline{6} \pmod{7}.$$

$$\Rightarrow \quad x = \overline{6} \pmod{7}$$

We can find $\bar{6}$ by trial and error, or by solving the equivalent equation

$$6x - 1 = 7y,$$

or by using Theorem 4.12 because 7 is prime and

$$6 \equiv -1 \pmod{7}$$

so that

$$\bar{6} = 6.$$

Hence, the solutions of $13x \equiv 1 \pmod{7}$ are

$$x \equiv 6 \pmod{7}.$$

The smallest positive solution is 6.