Linear Congruences

→ Existence

→ Complele Solutions

$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$

$\mathbb{Z}_5 = [3]+[4]=[2]$

$[3]\cdot[4]=[2]$

Inverse $[a]^{-1}$ $[a][a]^{-1}=[1]$

$[a]\cdot[x]=[1]$ in $\mathbb{Z}_m$.

$[ax]=[1] \Rightarrow ax \equiv 1 \pmod{m}$

Linear Congruences

Let $a, c \in \mathbb{Z}$, $m \in \mathbb{N}$. A linear congruence has the form $ax \equiv c \pmod{m}$.

Or, $[ax]=[c]$ in $\mathbb{Z}_m$.

Example: $2x \equiv 3 \pmod{5}$. $x=4$ is an integer solution.

$8 \equiv 3 \pmod{5}$

$x = 4+5n$ $\quad 2(4+5n) \equiv 8+10n \equiv 8 \equiv 3 \pmod{5}$

Any x where $x \in [4]$ in $\mathbb{Z}_5$ is a solution.

x is a solution iff anything in $[x]$ is in a solution.

Only need to check $x=0,1,2,3,4$ for all possible solns.

x	0	1	2	3	4
$2x$	0	2	4	6	8

$x \equiv 4 \pmod 5$ is the complete solution.

Example: $3x \equiv 4 \pmod 6$

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

No int sol^n exist.

<u>Existence</u>

When does $ax \equiv c \pmod m$ have an int solution?

$$ax \equiv c \pmod m$$

$\Leftrightarrow$ $m \mid (ax - c)$

$\Leftrightarrow$ $\exists y \in \mathbb{Z}, ax - c = my$

$\Leftrightarrow$ $\exists y \in \mathbb{Z}$, $\underline{ax + my = c}$

This LDE has an int sol^n if and only if $\gcd(a,m) \mid c$.

Preposition: $ax \equiv c \pmod m$ has an int solution if and only if $\gcd(a,m) \mid c$.

Inverses: $[a]^{-1}$ in $\mathbb{Z}_m$ exists if $ax \equiv 1 \pmod m$ for some $x \in \mathbb{Z}$. Need $\gcd(a,m) \mid 1$, so $\gcd(a,m) = 1$.

Proposition: The inverse of $[a]$ exists in $\mathbb{Z}_m$ iff $\gcd(a, m) = 1$.

$\mathbb{Z}_6$: $[1]$, $[5]$ have inverses, but none others have inverses.

$\varphi(n) = \#$ of int coprimes with n.

Complete Solutions

What are all int solutions?

$ax \equiv c \pmod{m} \iff \exists y \in \mathbb{Z}, ax + by = c$

If (x_0, y_0) is one soln, the complete soln of the LDE is:

$$\left\{\left(x_0 + \frac{m}{d}n, y_0 - \frac{a}{d}n\right) \middle| n \in \mathbb{Z}\right\}, d = \gcd(a, m)$$

So the complete soln to the lin. cong. is

$$\left\{x_0 + \frac{m}{d}n \middle| n \in \mathbb{Z}\right\}$$

Or, $x \equiv x_0 \left(\bmod \frac{m}{d}\right)$

Example. $6x \equiv 9 \pmod{21}$

$6x + 21y = 9$ Find one soln.

From EEA, $(5, -1)$ is one sol^n

So $x = 5$ is a soln to $6x \equiv 9 \pmod{21}$

complete soln: $x \equiv 5 \pmod{21/3}$

$\equiv 5 \pmod{7}$

Complete solutions mod 21:

check $x=0,1,2,\ldots,20$

See which ones are cong to 5 (mod 7)

$x = \underbrace{5, 12}_{+7}, \underbrace{12, 19}_{+7} \pmod{21}$

Generalize: $ax \equiv c \pmod{m}$, $d = \gcd(a,m)$

If x_0 is one soln, then comp. soln is $x \equiv x_0 \pmod{\frac{m}{d}}$

Mod m, $x \equiv x_0, x_0+\frac{m}{d}, x_0+2\frac{m}{d}, \ldots, \underbrace{x_0(d-1)\frac{m}{d}}_{\text{stop here since next term is } x_0+m \equiv x_0 \pmod{m}} \pmod{m}$

There are d incongruent solns mod m.

In cong classes: $[a][x]=[c]$ in $\mathbb{Z}_m$. x_0 is one soln.

Comp. Soln in $\mathbb{Z}_m$ is $\left\{[x_0], [x_0+\frac{m}{d}], \ldots, [x_0+(d-1)\frac{m}{d}]\right\}$