Solve $9x \equiv 6 \pmod{15}$.

Equivalent to solving the LDE

$$9x + 15y = 6.$$
$$3x + 5y = 2$$

By LDE T2 $x = -1 + 5n$
$y = 1 - 3n$ $\forall n \in \mathbb{Z}$.

$\therefore$ Soln is $x \equiv -1 \bmod 5$
OR $x \equiv 4 \bmod 5$
OR $x \equiv 4, 9, 14 \bmod 15$.

Ex: Show that there are no integer solutions to

$$x^2 + 4y = 2.$$

Sol'n: Assume towards a contradiction that $\exists\, x, y \in \mathbb{Z}$ s.t.

$$x^2 + 4y = 2.$$

$$\iff x^2 - 2 = -4y$$

$$\Rightarrow 4 \mid x^2 - 2 \quad \text{so } x^2 - 2 \equiv 0 \bmod 4$$

$$\underline{\text{or}} \quad x^2 \equiv 2 \bmod 4$$

x	0	1	2	3
$x^2 \bmod 4$	0	1	0	1

#

none equal 2.

$\therefore$ $x^2 - 4y = 2$ has no integer solutions. ∎

$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ Integers modulo m.

The congruence / equivalence class modulo m of an integer a is the set of integers:

$$[a] := \{x \in \mathbb{Z} : x \equiv a \bmod m\}$$

(":=" "defined as")

Further, define

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

We make $\mathbb{Z}_m$ a "ring" by defining addition, subtraction and multiplication by

$$[a] \pm [b] := [a \pm b] \qquad [a] \cdot [b] := [a \cdot b]$$

- $[a] \pm [b]$: adding sets
- $a \pm b$: adding integers
- $[a] \cdot [b]$: mult of sets
- $a \cdot b$: mult. integers

Issue: Well defined.

How do we know that this

addition didn't depend on our representation of $[a]$ & $[b]$?

Ex: Does $[2][5] = [14][-13]$ in $\mathbb{Z}_6$?

Sol'n: $[2] \cdot [5] = [2 \cdot 5] = [10] = [4]$ in $\mathbb{Z}_6$

$[14][-13] = [14 \cdot (-13)] = [-182] = [-2]$

$= [4]$ ✓

The members $0, 1, \ldots m-1$ are called representative members.

Addition table for $\mathbb{Z}_4$

$[+]$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Notes:

- We call $[0]$ the additive identity of $\mathbb{Z}_m$.
- We call $[1]$ the multiplicative identity of $\mathbb{Z}_m$.

Solve the following equations in $\mathbb{Z}_{14}$. Express answers as $[x]$ where $0 \leq x < 14$.

i) $[75] - [x] = [50]$

ii) $[10][x] = [1]$

iii) $[10][x] = [2]$

(i) $[75] - [x] + [x] - [50] = [50] + [x] - [50]$

$[25] = [x] \Rightarrow [x] = [11]$.

$[25] = \{\tilde{x} \in \mathbb{Z} : \tilde{x} \equiv 25 \bmod 14\}$

$= \{\tilde{x} \in \mathbb{Z} : \tilde{x} \equiv 11 \bmod 14\}$

$= [11]$.