# LNIII a



## §1.5

$$[a]_n = \{a, a+n, a+2n, \ldots \\ a-n, a-2n, \ldots\}.$$

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}.$$

$+ :\quad [a]_n + [b]_n = [a+b]_n$

$\times :\quad [a]_n [b]_n = [ab]_n$

$0 \neq [a]_n$ is invertible iff $\exists\, [b]_n$ with

$$[a]_n [b]_n = [1]_n.$$

## How to calculate $[a]_n^{-1}$?

$[a]_n^{-1}$ exists $\iff (a,n) = 1$

$(a,n) = 1 \iff \exists\, t, s \quad \boxed{at + ns = 1}$

So

$$[a]_n [t]_n = [at]_n = [1 - ns]_n = [1]_n$$

Ex] Determine $[72]_{91}^{-1}$

First check $(91,72) \overset{?}{=} 1$

$$91 = 72 + 19$$
$$72 = 3 \cdot 19 + 15$$
$$19 = 1 \cdot 15 + 4$$
$$15 = 3 \cdot 4 + 3$$
$$4 = 1 \cdot 3 + \boxed{1}$$
$$3 = 3 \cdot 1 + 0$$

$(91,72) = (72,19) = (19,15) = (15,4) = (4,3) = (3,1) = (3,0) = 1$

OK

Second express $1 = (91,72)$ as a linear combination of 91 and 72.

$$1 = 4 - 3$$
$$= 4 - (15 - 3\cdot 4) = 4 \cdot 4 - 15$$
$$= 4(19 - 15) - 15 = 4 \cdot 19 - 5 \cdot 15$$
$$= 4 \cdot 19 - 5(72 - 3\cdot 19) = 19 \cdot 19 - 5 \cdot 72$$
$$= \cancel{19 \cdot 19 - 5 \cdot 72}\ 19(91 - 72) - 5 \cdot 72$$
$$= 19 \cdot 91 - 24 \cdot 72$$

So $-24 \cdot 72 + 19 \cdot 91 = 1$

$$[72]_{91}^{-1} = [-24]_{91} = [67]_{91}.$$

---

## Linear Congruences

Solve (Given $a, b, n$)

$$\boxed{ax \equiv b \mod n.} \quad (*)$$

$\Longleftrightarrow$ Find $k, t$ s.t.

$$ak + nt = b.$$

$\Longleftrightarrow$ Find $[x]_n$ Congruence Class

$$[a]_n [x]_n = [b]_n.$$

Remark: The solutions of $(*)$ form congruence classes.

**Thm** $[a]_n[x]_n = [b]_n$ has a solution iff $d=(a,n) \mid b$.

**If** $d \mid b$ there are $d$ solutions.

These solutions are congruent $\frac{n}{d}$.

- **Pf** $\Rightarrow$) Suppose $c$ is a solution: $\exists k \in \mathbb{Z}$.

- $$ac - b = n \cdot k$$

Or $\quad b = ac + nk$

So $d=(a,n) \mid b$.

$\Leftarrow$) Suppose $d \mid b$, $\quad b = d \cdot e$.

We have $\quad d = ak + nt$ $\quad \Longrightarrow$

- $$b = ake + nt \cdot e.$$

That is, $ke$ is a solution of

$$ax \equiv b \mod n.$$

---

Suppose $c$ is a solution.

$$ac = b + n \cdot k$$

$d | b$. Divide by $d$.

$$\frac{a}{d} \cdot c = \frac{b}{d} + \frac{n}{d} \cdot k.$$

So $c$ is a solution of

$$\frac{a}{d} x \equiv \frac{b}{d} \bmod \frac{n}{d}$$

And visa versa.

This implies

$$c, \; c + \frac{n}{d}, \; c + 2\left(\frac{n}{d}\right), \; \ldots, \; c + (d-1)\frac{n}{d}$$

are also solutions $\square$.

## Algorithm to Solve Lin. Cong.

1. Calculate $(a, n) = d$.
2. $d \nmid b$ : no solutions <u>Done</u>

   $d | b$ : there are $d$ solutions.

(3) Divide the equation by d.

$$\left[\frac{a}{d}\right]_{\frac{n}{d}} x = \left[\frac{b}{d}\right]_{\frac{n}{d}}.$$

(4) Find $\left[\frac{a}{d}\right]_{\frac{n}{d}}^{-1}$.

(5) $x = \left[\frac{a}{d}\right]_{\frac{n}{d}}^{-1} \cdot \left[\frac{b}{d}\right]_{\frac{n}{d}}.$

(6) Solutions:

$$x,\ x+\frac{n}{d},\ x+2\frac{n}{d} + \cdots + (d-1)\frac{n}{d}.$$

<u>Example</u>

$$6x = 9 \mod 15$$

$d = (6,15) = 3$ There are 3 solutions.

divide by 3

$$2x = 3 \mod 5$$

Find $[2]_5^{-1} = [3]_5$

(Easy to see).

$$x = [3]_5 [3]_5 = [9]_5 = [4]_5$$

All solutions.

$[4]_{15}$, $[9]_{15}$, $[14]_{15}$.

§1.5

## Solving Linear Congruences

Ex) $6x \equiv 5 \mod 15$

$(15,6) = 3$  $\cancel{3 \mid 5}$ : no sol.

- Ex) $432x \equiv 12 \mod 546$ ⊛

$$546 = 1 \cdot 432 + 114 \qquad (546,432)$$
$$432 = 3 \cdot 114 + 90 \qquad (432,114)$$
$$114 = 1 \cdot 90 + 24 \qquad (90,24)$$
$$90 = 3 \cdot 24 + 18 \qquad (24,18)$$
$$24 = 1 \cdot 18 + 6 \qquad (6,0) = 6$$
$$18 = 3 \cdot 6 + 0$$

$$\boxed{(546,432) = 6}$$

- Divide by 6.

$$\boxed{72x \equiv 2 \mod 91} \quad ⊛⊛$$

Multiply by $[72]_{91}^{-1}$

We need $[72]_{91}^{-1}$

$$91 = 1\cdot 72 + 19 \qquad 1 = 4 - 3$$
$$72 = 3\cdot 19 + 15 \qquad = 4 - (15 - 3\cdot 4)$$
$$19 = 1\cdot 15 + 4 \qquad = -15 + 4\cdot 4$$
$$15 = 3\cdot 4 + 3 \qquad = -15 + 4(19 - 15)$$
$$4 = 1\cdot 3 + \boxed{1}. \qquad = -5\cdot 15 + 4\cdot 19$$

$$= -5(72 - 3\cdot 19) + 4\cdot 19 = -5\cdot 72 + 19\cdot 19$$
$$= -5\cdot 72 + 19(91 - 72) = 19\cdot 91 - 24\cdot 72$$

So $[72]_{91}^{-1} = [-24]_{91} = [67]_{91}$

Multiply ⊛⊛ by $[72]_{91}^{-1} = [67]_{91}$

$$[x]_{91} = [2\cdot 67]_{91} = [43]_{91}$$

Sol of original equation ⊛ are.

$$[43]_{546},\ [134]_{546}\ [225]_{546}\ [316]_{546}$$

+91 +91 +91 +91

$$[407]_{546}\ [498]_{546}.$$

+91

## Thm (Chinese Remainder)

Let $(m,n)=1$ $a,b$

Then there are solutions to

$$\circledast \begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

The solution is unique up to congruence mod $mn$.

Pf) $(m,n)=1$ So $\exists\ k,t$.

$$mk+nt=1$$

Then

$$c = bmk + ant$$

is a solution to $\circledast$ Namely

$$c = bmk + a(1-mk) = a + (bk-ak)m$$

$$c = b(1-nt) + ant = b + (at-bt)n.$$

If ~~$c \equiv a \mod$~~ $c$ and $d$ are solutions to $\circledast$

Then

$c-d=0 \mod m$

$c-d=0 \mod n$

So $\left.\begin{array}{l} m \mid c-d \text{ and } n \mid c-d \\ (m,n)=1 \end{array}\right\} \Rightarrow$

- $mn \mid c-d$ . $[c]_{mn}=[d]_{mn}$.

- If $c$ is a solution to * and

  $c-d \equiv 0 \mod mn.$

  Then $d=c+kmn.$ and $d$ also solves ⊛

  $\square$.

- Example | Solve

- $\begin{cases} x \equiv 3 \mod 7 & (1) \\ x \equiv 6 \mod 25 & (2) \end{cases}$

$\left.\begin{array}{l} (1) \Rightarrow x = 3+k\cdot 7 \\ (2) \end{array}\right\} \Rightarrow [3+k\cdot 7]_{25}=[6]_{25}$

$[7]_{25}[k]_{25} = [6-3]_{25} = [3]_{25}$

$(25,7)=1$ So $[7]_{25}^{-1}$ exists. 

Namely $[7]_{25}^{-1} = [18]_{25}$

$(7 \cdot 18 = 126 = 1 \mod 25)$.

So $[k]_{25} = [3 \cdot 18]_{25} = [4]_{25}$

So $x = 3 + k \cdot 7 = 3 + 7(4 + t \cdot 25)$

$x = 31 + t \cdot 175$ $\boxed{x = [31]_{175}}$

Example Solve

$$\begin{cases} x \equiv 2 \mod 7 & (1) \\ x \equiv 0 \mod 9 & (2) \\ 2x \equiv 6 \mod 8 & (3) \end{cases}$$

First Clean (3)

$(2,8)=2$ : divide (3) by 2.

$$\begin{cases} x \equiv 2 \mod 7 & (1) \\ x \equiv 0 \mod 9 & (2) \\ x \equiv 3 \mod 4 & (3) \end{cases}$$

$$\left.\begin{array}{l} (2) \Longrightarrow \boxed{x = k \cdot 9} \\ (1). \end{array}\right\} \Longrightarrow [9]_7 [k]_7 = [2]_7$$

$$\left.\begin{array}{l} [2]_7 [k]_7 = [2]_7 \\ [2]_7^{-1} \text{ exists} \end{array}\right\} \Longrightarrow [k]_7 = [1]_7$$

So $$\left.\begin{array}{l} \boxed{k = 1 + t \cdot 7} \\ (3) \end{array}\right\} \Longrightarrow [7]_4 [t]_4 = [2]_4$$

$$\left.\begin{array}{l} [3]_4 [t]_4 = [2]_4 \\ [3]_4^{-1} = [3]_4 \end{array}\right\} \Longrightarrow [t]_4 = [6]_4 = [2]_4$$

$$\boxed{t = 2 + r \cdot 4}$$

So $$k = 1 + (2 + r4)7 = 15 + r \cdot 28$$

$$x = (15 + r \cdot 28)9 = 135 + r \cdot 252$$

$$x = [135]_{252}$$