Week 4

In week 3, we defined

$+$, $-$, $\times$

on $\mathbb{Z}_n$ = the set of equiv classes $[a]_n$ w.r.t $\equiv$ on $\mathbb{Z}$ mod n.

Def We say that an element $[a]$ in $\mathbb{Z}_n$

has a multiplicative inverse

if $\exists\, b$ s.t. $[a][b] = [1]$

$[ab]$

$a \equiv b \mod n$

$\Leftrightarrow$

$[a] = [b]$

$\Leftrightarrow$

$ab \equiv 1 \mod n$

Rk The multiplicative inverse of $[a]$, if exists, is unique.

Suppose we have $[b]$ in $\mathbb{Z}_n$
$[c]$

satisfying $[a][b] = [1]$

$[a][c] = [1]$.

GOAL $[b] = [c]$

Firstly, observe that

$$[a][c] = [1]$$
$$\parallel$$
$$[ac] = \{ d \equiv ac \mod n \}$$

$\|$ $\qquad\qquad$ $\|$

$$[ca] = \{d \equiv ca \mod n\}$$

$$\Rightarrow \quad [c][a] = [1].$$

Multiplying both sides of by $[b]$,

$$[c]\underbrace{[a][b]}_{\substack{\| \;\Leftarrow\; \text{by assumption} \\ [1]}} = \underbrace{[1][b]}_{\substack{\| \;\Leftarrow\; \text{by def of } X \\ [b]}}$$

$\parallel \Leftarrow$ by def^n of X

$[c]$

Therefore $[c] = [b]$.

Theorem 12

$[a]$ in $\mathbb{Z}_n$ has a multiplicatio inverse in $\mathbb{Z}_n$

$\Longleftrightarrow \gcd(a, n) = 1$.

I proved: if $\gcd(a,n) = 1$,

then $[a]$ has a multiplicative inverse.

If $\gcd(a,n) = 1$,

then Theorem 7 (Bezout) gives

$r, s' \in \mathbb{Z}$ s.t.

$$ar + ns' = \gcd(a,n)$$
$$= 1.$$

$\Rightarrow ar - 1 = -ns'$

$\Rightarrow \quad ar \equiv 1 \mod n$

$\Rightarrow \quad [ar] = [1] \quad \text{in } \mathbb{Z}_n$

$\Rightarrow \quad \underbrace{[a][r]}_{} = [1]$

this is what we are looking for $[\,]$.

Example

What is the multiplicative inverse of $[23]_{2023}$?

What is the multiplicative inverse of $[9]_{2023}$?

$$\begin{array}{r} 224 \\ 9\overline{)2023} \\ 18 \\ \hline 22 \\ 18 \\ \hline 43 \\ 36 \\ \hline 7 \end{array}$$

$a = 9 \quad n = 2023$

$$2023 = 9 \cdot 224 + 7$$

$$9 = 7 \cdot 1 + 2$$

$$7 = 2 \cdot 3 + 1$$

$$1 = 7 - 2 \cdot 3$$

$$= 7 - (9 - 1 \cdot 7) \cdot 3$$

$$= 4 \cdot 7 - 3 \cdot 9$$

$$= 4 \cdot (2023 - 9 \cdot 224) - 3 \cdot 9$$

$$= \underset{=}{4} \cdot 2023 + \underline{(-899)} \cdot 9$$

So $[-899]_{2023}$

$\shortparallel$

$[1124]_{2023}$

$$\begin{array}{r} \cancel{2023} \\ 899 \\ \hline 1124 \end{array}$$

Example Let p be a prime number.

Then $\mathbb{Z}_p = \mathbb{F}_p$

$$= \{ [0], [1], \dots, [p-1] \}$$

Which

$[a]$ in have

multiplicative inverse?

Theorem 12 says

all $[a]$ $\gcd(a, p) = 1$.

In fact $\Leftrightarrow$ p does NOT divide a.

$[1], [2], \cdots, [p-1]$

satisfy this condition.

Prop 13

$[a]$ in $\mathbb{Z}_n$ has no multiplicative inverse

$\iff$ there exists an integer b, not divisible by n, s.t. $[a][b] = [0]$.

Example $n=6$

Both $[2]_6$, $[3]_6$ do NOT

have multiplicative inverses.

$$[2]_6 [3]_6 = [2\cdot 3]_6 = [6]_6 = [0]_6$$

typed-up

Pf See Lecture notes

in Week 2 tab.

Given $n>1$, how many

elements in $\mathbb{Z}_n$ have multiplicative

Inverse?

In theory, we need to count $0 \le a \le n-1$

s.t. $\gcd(a, n) = 1$.

Ex $n = 24$.

$\gcd(a, 24) = 1$

$\cancel{0}$ 1 $\cancel{2}$ $\cancel{3}$ $\cancel{4}$ 5 $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$

11 $\cancel{12}$ 13 $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$

$\cancel{21}$ $\cancel{22}$ 23

8

If n is really big,

this approch seems rather

inpractical.

There is a formula to compute

the size of $\{ 0 \le a \le n-1 \mid \gcd(a,n) = 1 \}$

Recall from the fundamental

theorem of arithmetic

that any positive integer

n is of the form

$$= \prod_{p} p^{r_p}$$

the product of p^{r_p}

$0 \le r_p$

$$\phi(n) = \prod_{p} (p-1)\, p^{r_p - 1}$$

computes the number.

Example $n = 24$

$$= 2^3 \cdot 3$$

$$\begin{cases} r_p = 0 & \text{if } p \neq 2, 3 \\ r_2 = 3 \\ r_3 = 1 \end{cases}$$

$$\phi(24) = (2-1)\, 2^{3-1} \cdot (3-1) \cdot 3^{1-0}$$

$$= 1 \cdot 4 \cdot 2 \cdot 1$$

$$= \underline{\underline{8}}.$$

What is multip inverse useful for?

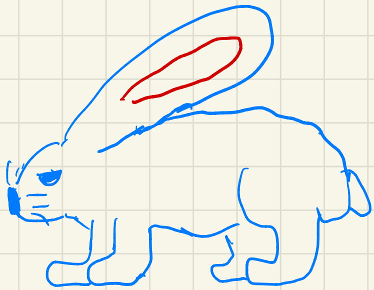
Example Solve

$$7x \equiv 1 \mod 11$$

in $x \in \mathbb{Z}$.

$$\Leftrightarrow \quad [7]_{11}[x]_{11} = [1]_{11}$$

What is $[x]_{11}$??



Approach #1

Since $\mathbb{Z}_{11} = \mathbb{F}_{11}$

$= \{[0], \ldots, [10]\}.$

$[x]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$7[x]$ $[7x]$	$[0]$	$[7]$	$[3]$	$[10]$	$[6]$	$[3]$	$[9]$	$[5]$	$[1]$	$[8]$	$[4]$
$7[x] - [1]$									$[0]$		

$$[7]_{11}[x]_{11} = [1]_{11}$$

$\Leftrightarrow \quad [7x] - [1] = [0]$

Approach #2

Find the multiplicative inverse of $[7]_{11}$

By Euclid's algorithm, we find that $\gcd(7, 11) = 1$

$$\gcd(7,11) = 1 = 2 \cdot 11 - 3 \cdot 7$$

$\Rightarrow \quad [-3]_{11} = [8]_{11}$

is the multiplicative inverse of $[7]_{11}$

Multiply both sides of

$$[7]_{11}[x]_{11} = [1]_{11}$$

by $[8]_{11}$

$$\Rightarrow \quad \underbrace{[8]_{11}\,[7]_{11}}_{= [1]}\,[x]_{11} = [8]_{11}\,[1]_{11}$$

$$\Rightarrow \qquad [1][x] = [8][1]$$

$$\Rightarrow \qquad [x] = [8] \qquad . \square$$

In general, you'll be able to solve

$$ax + b \equiv c \mod n$$

if $\gcd(a, n) = 1$.

How?

$$[a][x] + [b] = [c]$$

Step 1 Find the multiplicative inverse

$$[a]^{-1} \quad \left(\neq 1/[a]\right)$$

of $[a]$.

Step 2

$$[a][x] = [c] - [b]$$

$$= [c-b].$$

Step 3 Multiply $[a]^{-1}$

$$\underbrace{[a]^{-1}[a]}_{=[1]}[x] = [a]^{-1}[c-b]$$

$$[x] = [a]^{-1} \cdot [c-b].$$