Last Monday, I introduced

a relation $\mathcal{R}$ on $S = \mathbb{Z}$

by $a, b \in S = \mathbb{Z}$

$$a \equiv b \mod n$$

("a is congruent to

b modulo n")

if and only if

$b - a$ is divisible by n.

Example $n = 11$

$$12 \equiv 1 \mod 11$$

$$3 \equiv 25 \mod 11$$

Why?

$1 - 12 = (-11)$ is divisible by 11

$25 - 3 = 22$ is divisible by 11

4 is NOT congruent to

25 mod 11

because $25 - 4 = 21$

and this is NOT divisible by 11!

$$\cancel{4 \equiv 25 \mod 11}$$

I proved that

$\equiv$ on $\mathbb{Z}$

is an equivalence relation.

Recall given an equivalence relation

$\mathcal{R}$ on S,

we write $[a]$ for

$a \in S$ $\quad \{ b \in S \mid$

$a \mathcal{R} b \}$

Specialising this to

$(\mathcal{R}, S) = (\equiv, \mathbb{Z})$

$a \in \mathbb{Z}$

$[a] = [a]_n = \{ b \in \mathbb{Z} \mid$

$a \equiv b \bmod n \}$

<u>Example</u> $n = 11$

$$[3]_{11} = \{ b \in \mathbb{Z} \mid 3 \equiv b \bmod 11 \}$$

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

$$[3] \qquad \{ 14, 25, 36 \ldots, -8, -19, \ldots \}$$

$$\|$$

$$\{ 3 + 11k \mid k \in \mathbb{Z} \}$$

We defined addition

subtraction

multiplication

on the set $\mathbb{Z}_n$ of equivalence classes $[a]_n$

$$[a] + [b] \overset{def}{=} [a+b]$$

$$[a] - [b] \overset{def}{=} [a-b]$$

$$[a][b] \overset{def}{=} [ab]$$

$$[a] + [b] \neq [a] \cup [b]$$

I didn't define "division".

In particular: $\dfrac{[a]}{[b]} \not\equiv \left[\dfrac{a}{b}\right]$

How do we think about division?

Recall that $a, b \in \mathbb{Z}$

" a divides b in $\mathbb{Z}$ "

if there exists $c \in \mathbb{Z}$

s.t. $b = ac$

We see c as $\frac{b}{a}$.

Def Let $[a] \in \mathbb{Z}_n$

If there exists $b \in \mathbb{Z}$

s.t. $$\boxed{\underset{\underset{[ab]}{\parallel}}{[a][b]} = [1],}$$

then we call this $[b]$

the multiplicative inverse of $[a]$

$[b]$ plays the role of $[1]/[a]$.

(but literally).

Example $n = 5$

What is the multiplicative inverse of $[2]_5$ in $\mathbb{Z}_5$?

I need to find $b \in \mathbb{Z}$

s.t. $[2][b] = [1]$.

Since $\mathbb{Z}_5 = \{ [0], [1], [2], [3], [4] \}$

try and error!

$\cancel{[b] = [0]}$? $[2][0] = [2 \cdot 0] = [0] \neq [1]$

$\cancel{[b] = [1]}$? $[2][1] = [2] \neq [1]$

$\cancel{[b] = [2]}$

$$[2][2] = [2 \cdot 2]$$
$$= [4] \neq [1]$$

$[b] = [3]$

$$[2][3] = [6]$$
$$= [1].$$

so $[3]$ is the multiplicative inverse of $[2]$.

Ex $n = 6$ $\mathbb{Z}_6$

what is the multiplicate

inverse of $[-1]$?

$$[-1][-1] = [(-1)\cdot(-1)]$$
$$= [1]$$

so

$[-1]$ is the multiplicative

inverse of $[-1]_6$.

$$\shortparallel$$

$$[5]_6$$

What is the multiplicative inverse

of $[2]_6$ in $\mathbb{Z}_6$?

No multiplicate inverse

Why? If it did, there

would be $b \in \mathbb{Z}$

s.t. $[2][b] = [1]$

$r \equiv s \mod n$

$\Leftrightarrow [r] = [s]$

$$[2][b] = [2b]$$

$\Rightarrow 2b \equiv 1 \mod 6$

$\Rightarrow 6$ divides $2b - 1$

However the even integer b can not divide the odd integer $2b-1$.

This is a contradiction!

Theorem 12

The equivalence class $[a]$ in $\mathbb{Z}_n$ has multiplicative inverse if and only if

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

Pf Let's prove "if bit"

of the assertion.

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

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

Since $\gcd(\underline{\underline{a}}, \underline{\underline{n}}) = 1$, it follows from Theorem 7 (Bezout) that

$\exists\, b, c \in \mathbb{Z}$

s.t. $\quad ab + nc = \gcd(a, n) = 1$ (*)

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

because $ab - 1 = nc$ (*) is divisible by n.

$$\Rightarrow \quad [1] = [ab] = [a][b].$$

$\square$

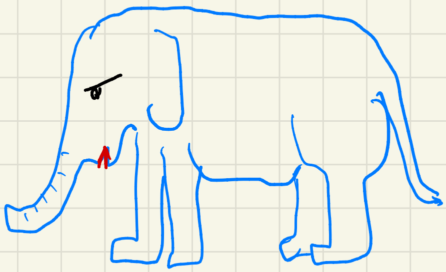
This bit of the proof explains how to work out the multiplicative inverse of $[a]$.

<u>Example</u> $\quad n = 2023$

What is the multiplicative inverse

of $[23]_{2023}$

in $\mathbb{Z}_{2023}$?



I need to work out

$$r, s \in \mathbb{Z}$$

s.t. $$2023 \cdot r + 23 s$$

$$= \gcd(2023, 23)$$

Euclid's algorithm:

$$\underline{\underline{2023}} = \underline{\underline{23}} \cdot 87 + 22$$

$$23 = 22 + \underline{\underline{1}}$$

$$\|$$

$$\gcd(2023, 23)$$

$$1 = 23 - 1 \cdot 22$$

$$= 23 - 1 \cdot (2023 - 23 \cdot 87)$$

$$= 88 \cdot 23 + (-1) \cdot 2023$$

so $[88]$ is the multiplicative

inverse in $\mathbb{Z}_{2023}$.