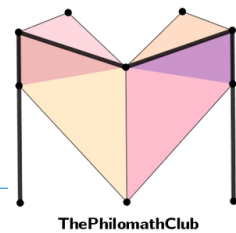


22.07.22

# Modular Arithmetic



→ What happens when we divide two +ve Integers?

$$\rightarrow 100 \div 30$$

↳ Quotient and remainder

$$\frac{A}{B} = Q \text{ and remainder } (R)$$

→ Introduction to  $\equiv$  symbol

$$A \equiv B \pmod{C}$$

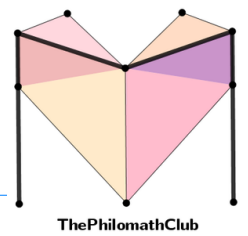
IF  $C$  divides  $A - B$ .

↳  $\frac{A-B}{C}$ , the remainder is zero

For example :-  $2 \mid 4$

$3 \mid 6$  because 6 is a multiple of 3  
ie the remainder is zero

We say  $X \mid Y$  if  $Y$  is a multiple of  $X$ ,



$$A \equiv B \pmod{C}$$

$$\text{IF } C \mid A - B.$$

Ex 1:  $\rightarrow$  "congruent" or "equivalent" to

$$5 \equiv 3 \pmod{2}$$

because  $2 \mid 5 - 3$ .

$$\text{Ex 2: } 100 \equiv 10 \pmod{30}$$

because  $30 \mid 100 - 10 = 90$

$\Rightarrow$  definition.

$A \equiv B \pmod{C}$  if and only if  $C \mid A - B$ .

ie if  $A \equiv B \pmod{C}$  then  $C \mid A - B$

& if  $C \mid A - B$  then  $A \equiv B \pmod{C}$

Ex 3:- Given  $100 \equiv x \pmod{70}$  and  $0 < x < 70$ .  
Find  $x$ .

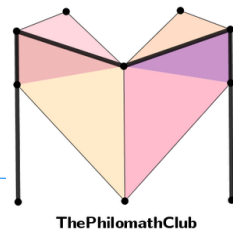
Solution  $\rightarrow$  Since  $100 \equiv x \pmod{70} \Rightarrow 70 \mid 100 - x$ .

$100 - x = 70, 140, 210, \dots$

or

$$100 - x = -70, -140, -210, \dots$$

$$x = 30$$



$$70 \mid 100 - x.$$

Now we find the range of  $100 - x$ .

$$\text{So when } x = 1, \quad 100 - x = 99$$

$$x = 2, \quad 100 - x = 98$$

⋮

$$x = 69, \quad 100 - x = 31$$

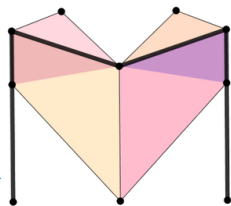
So possible values of  $100 - x$ , when  $0 < x < 70$

are  $99, 98, \dots, 31$

we want  $100 - x$  as a multiple of  $70$ .

Now  $99, 98, \dots, 31$ , there is only one multiple of  $70$ , which is  $70$  itself.

And that is possible when  $x = 30$ .



ThePhilomathClub

EXM :- Given  $1000 \equiv x \pmod{70}$  and  $71 < x < 140$ .  
Find  $x$ .

$x = 72, \dots, 139$   
↷

Solution:- Since  $1000 \equiv x \pmod{70}$ ,

$$70 \mid 1000 - x.$$

Hence  $1000 - x$  is a multiple of 70.

So the possible values of  $1000 - x$  are

$$1000 - x = 70, 140, 210, \dots$$

$$1000 - x = -70, -140, -210, \dots$$

$$\text{Now, when } x = 72, \quad 1000 - x = 928$$

$$\text{when } x = 73, \quad 1000 - x = 927$$

,

,

.

$$x = 139, \quad 1000 - x = 861$$

So the possible values of  $1000 - x$ , when  $71 < x < 140$

is  $928, 927, \dots, 861$ .

We want  $1000 - x$  a multiple of 70.

We have a multiple of 70 in 928,  $\dots$ , 861.

Note that  $70 \mid 910$ .

$$1000 - x = 910, \text{ when } x = 90.$$

So 90 is the  $x$ .

Simple day to day example of modular arithmetic :-

24 hr format

12 hr format

1:00 pm in 12 hr format clock  $\rightarrow$  13:00 in 24 hr

19:49 pm

$\rightarrow$

7:49 pm

$$19 \equiv 7 \pmod{12}$$

$$13 \equiv 1 \pmod{12}$$

|

$$23 \equiv 11 \pmod{12}$$

# Modular Arithmetic & Subtraction

Theorem :- Given

$$A \equiv B \pmod{C}$$

$$E \equiv F \pmod{C}$$

Then

$$(i) \quad A + E \equiv B + F \pmod{C}$$

(W)

$$(ii) \quad A - E \equiv B - F \pmod{C}$$

Proof :- (i) Given  $A \equiv B \pmod{C}$

$$E \equiv F \pmod{C}$$

We want to show  $A + E \equiv B + F \pmod{C}$ .

Note that, since  $A \equiv B \pmod{C} \Rightarrow C \mid A - B$

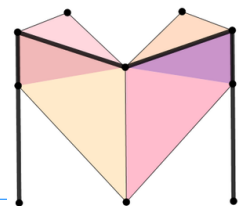
$\Rightarrow A - B$  is a multiple of  $C$ . Since  $A - B$  is a multiple of  $C$ ,  $A - B = C \times k$ ,  $k$  is an integer.

Note that, since  $E \equiv F \pmod{C} \Rightarrow C \mid E - F$

$\Rightarrow E - F$  is a multiple of  $C$ . Since  $E - F$  is a multiple of  $C$ ,  $E - F = C \times l$ ,  $l$  is an integer.

We need to show  $A + E \equiv B + F \pmod{C}$

or it is enough to show



ThePhilomathClub

$$C \mid A + E - (B + F)$$

We need to show

$$C \mid A - B + E - F$$

We need to show

$$C \mid C \times k + C \times l$$

or we need to show

$$C \mid C(k + l)$$

which is true

Ex:

$$C = 25, \quad A = 41, \quad B = 16$$

$$E = 76, \quad F = 1$$

$$41 \equiv 16 \pmod{25}$$

$$\begin{aligned} 41 - 16 &= 25 \\ \text{and } 25 &= 25 \times 1 \\ &\downarrow \\ k &= 1 \end{aligned}$$

$$76 \equiv 1 \pmod{25}$$

$$\begin{aligned} 76 - 1 &= 75 \\ 2 \times 75 &= 25 \times 3 \\ &\downarrow \\ l &= 3 \end{aligned}$$

$$\text{So, } 41 + 76 \equiv 16 + 1 \pmod{25}$$

$$117 \equiv 17 \pmod{25}$$

$$41 - 76 \equiv 16 - 1 \pmod{25}$$

$$-35 \equiv 15 \pmod{25}$$

$$\begin{array}{l} \text{Then} \quad 25 \mid -35 - 15 \\ \quad \quad 25 \mid -50 \end{array}$$

