22·07·22

Modular Arithmetic

ThePhilomathClub

- What happen when we divide two +ve Integers?

→ $100 \div 30$

↳ Quoteint and remainder

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

- Introduction to $\equiv$ symbol

$A \equiv B \mod C$

if C divides $A - B$.

ie $\frac{A-B}{C}$, 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.

ThePhilomathClub

$A \equiv B \mod C$

if $C \mid A - B$.

Ex1: "congruent" or "equivalent" to

$5 \equiv 3 \mod 2$

because $2 \mid 5 - 3$.

Ex 2: $100 \equiv 10 \mod 30$

because $30 \mid 100 - 10 = 90$

• $\equiv$ definition.

$A \equiv B \mod C$ if and only if $C \mid A - B$.

ie if $A \equiv B \mod C$ then $C \mid A - B$

& if $C \mid A - B$ then $A \equiv B \mod C$

Ex 3:- Given $100 \equiv x \mod 70$ and $0 < x < 70$. ($x = 1, \ldots, 69$)

Find x.

solution → Since $100 \equiv x \mod 70 \Rightarrow 70 \mid 100 - x$.

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

or

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

$\boxed{x = 30}$

$70 \mid 100 - x$.

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

So when $x = 1$, $100 - x = 99$

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

$\vdots$

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

So possible value of $100 - x$, when $0 < x < 70$ are $99, 98, \cdots, 31$

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

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

And that is possible when $x = 30$.

Ex4 :- Given $1000 \equiv x \bmod 70$ and $71 < x < 140$. $x = 72, \ldots, 139$

Find x.

Solution :- Since $1000 \equiv x \bmod 70$,

$70 \mid 1000 - x$.

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

So the possible values of $1000 - x$ are

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

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

Now, when $x = 72$, $1000 - x = 928$

when $x = 73$, $1000 - x = 927$

⋮

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

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

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

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

We have a multiple of 70 in 928, .. ,861.

Note that $70 \mid 910$.

$1000 - x = 910$, 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

$19 \equiv 7 \bmod 12$ | $23 \equiv 11 \bmod 12$

$13 \equiv 1 \bmod 12$

Modular Arithmetic & Subtraction

Theorem :- Given

$A \equiv B \bmod C$

$E \equiv F \bmod C$

Then

(i) $A + E \equiv B + F \bmod C$

HW (ii) $A - E \equiv B - F \bmod C$

Proof :- (i) Given $A \equiv B \bmod C$

$E \equiv F \bmod C$

We want to show $A + E \equiv B + F \bmod C$.

Note that, since $A \equiv B \bmod C \Rightarrow C \mid A - B$

$\Rightarrow$ $A - B$ 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 $E \equiv F \bmod C \Rightarrow C \mid E - F$

$\Rightarrow$ $E - F$ 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 $A + E \equiv B + F \mod C$

or it is enough to show

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

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:- $C = 25$, $A = 41$, $B = 16$

$E = 76$, $F = 1$

$41 \equiv 16 \mod 25$ $\rightarrow$ $41 - 16 = 25$ and $25 = 25 \times 1$ $\downarrow$ $K = 1$

$76 \equiv 1 \mod 25$ $\rightarrow$ $76 - 1 = 75$ & $75 = 25 \times 3$ $\rightarrow$ $l = 3$

So, $41 + 76 \equiv 16 + 1 \mod 25$

$117 \equiv 17 \mod 25$

$41 - 76 \equiv 16 - 1 \mod 25$

$-35 \equiv 15 \mod 25$

Then $25 \mid -35 - 15$

$25 \mid -50$