Modular arithmetic

- What happens when we divide $100 \div 40$?

→ $100 = 40 \times 2 + 20$

$Q = 2$, Remainder $= 20$

- $\equiv$ → "congruent to"

- $A \equiv B \mod C$

when C divides A − B.

2 divides 4 because 4 is a multiple of 2.

$2 \mid 4$ → 2 divides 4

5 doesn't divide 7 → $5 \nmid 7$

Example :- $25 \equiv 3 \mod 11$

as $11 \mid 25 - 3 = 22$ so $25 \equiv 3 \mod 11$

Introduce a few notation.

- $A \mid B \longrightarrow$ B is a multiple of A.
- $\Rightarrow$ "implies"

Since $2 \times 4 = 8 \Rightarrow$ 8 is divisible by 2

- $\Leftrightarrow$ "if and only if"

Suhan eats icecream if and only if it is Sunday.

Suhan eats icecream $\Leftrightarrow$ if it is Sunday.

→ Modular arithmetic

We say $A \equiv B \bmod C \Leftrightarrow C \mid A - B$.

↳ if $C \mid A - B$, then $A \equiv B \bmod C$

if $A \equiv B \bmod C$, then $C \mid A -$

Exercise :- State T / F.

1) $24 \equiv 2 \mod 11$ (T)

↳ $11 \mid 24-2=22$

2) $25 \equiv 15 \mod 10$ (T)

↳ $10 \mid 25-15=10$

3) $100 \equiv 24 \mod 37$ (F)

↳ $37 \nmid 100-24=76$

4) $45 \equiv 568 \mod 523$ (T)

$45 - 568 = -523$

and $523 \mid -523$.

5) $24 \equiv 5 \mod 19$ (T)

$19 \mid 24-5=19$

$A \equiv B \mod C \iff C \mid A-B$

$A-B = -20-(-20) = -20+20 = 0$

6) $-20 \equiv -20 \mod 192$ (T)

$192 \mid -20-(-20)=0$

$x = 1, 2, \cdots, 69$

Ex 3:- Given $100 \equiv x \bmod 70$ and $0 < x < 70$.

Find x.

$2 < x < 15 \rightarrow x = 3, 4, \cdots, 14$

$\rightarrow$ Since $100 \equiv x \bmod 70 \Rightarrow 70 \mid 100 - x$

So $100 - x$ is a multiple of 70.

Since $0 < x < 70$, $x = 1, 2, 3, \cdots, 69$

$100 - x = 99, 98, \cdots, 32, 31.$

$99 > 100 - x > 31.$

$\downarrow$

has only 1 multiple of 70

which 70

So $100 - x = 70$

$\Rightarrow x = 100 - 70 = \boxed{30}$

→ 2017 cat II P1

Q. Two numbers when divided by a certain divisor have remainders 3 and 4 respectively. When the two numbers are added and their sum is divided by the same divisor the remainder is 2.
What is the divisor ?

→ A is divided by K, remainder is 3

B is divided by K, remainder is 4

A+B is divided by K, remainder must be 3+4 = 7

(For example, 39 is divided by 19, r = 1

44 is " " " r = 6

39+44 = 83 is divided by 19, r = 7
1+6)

$7 \equiv 2 \mod K$

$\Rightarrow K \mid 7-2 \Rightarrow K \mid 5 \Rightarrow K = 5$

The two numbers, when divided by a divisor leave remainders 3 and 4.
When we add the two numbers, their remainders add up to 3+4=7
But when divided by the original divisor this sum leaves remainder equal to 2.
Since 7=5×1+2, the divisor must be 5.