§ Modular Arithmetic: In many Problems (involving a fixed number n) to answer it we treat all numbers that leave the same remainder (when divided by n) as the same.

e.g. If it is Wed. today what day will it be in 100 days from it

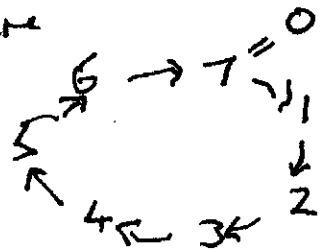
$100 = 7(14) + \underline{2}$ → is important Not so much the 100

ANS = Fri = Wed + 2

Since eg. 30 days from Today is also Fri as $30 = 7(4) + \underline{2}$ & 9 days From now is Also Fri as.

$9 = 7(1) + 2$

So to Solve This Problem we have a "7 day-clock" Picture

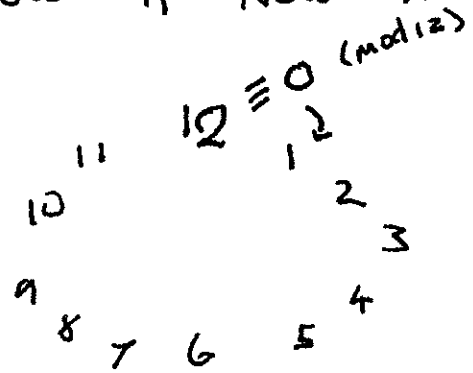


When we reach $7 = 0$ as next day = 1 not 8

of course $8 \neq 1$ So

Write $8 \equiv 1 \mod 7$

Ex 2: At what hour will the clock (12 hr clock) Point to 40 or 52 or 64 OR 28 or 16 hrs from now if Now it is 3 o'clock



$40 = 12(3) + 4$

Ans. 7 o' clock & same

ans for 52 64, 28, 16, 4 etc.
Are All the same or equal for solving this problem involving the $n = 12$ hour clock)

Write eg. $52 \equiv 40 \mod 12$ Because

$$52 = 12(4) + 4$$
$$40 = 12(3) + 4$$

Note $\Leftrightarrow$ $52 - 40 = 12[4-3]$ has zero remainder when divided By 12

ie $12 \mid 52-40 \iff 52 \equiv 40 \mod 12$

General defn: Let $n \in \mathbb{N}$, $n > 1$ & $a, b \in \mathbb{Z}$
We say that a is congruent to b modulo n and write $a \equiv b \mod n$ if $n \mid b-a$ ($\iff$) a & b leave the Same remainder when divided By n ($a, b > 0$)

Ex: $n = 6$:

$7 \equiv 1 \bmod 6 \equiv 13 \bmod 6 \equiv 19 \bmod 6$

$n = 5$

$7 \equiv 2 \bmod 5$ ($7 = 5(1) + 2$

($82 = 5(0) + 2$

$n = 11$

$15 \equiv 4 \bmod 11$ ⌒ ($15 = 11(1) + 4$

$26 \equiv 4 \bmod 11$ ⟶ $26 = 11(2) + 4$

$15 \equiv 26 \bmod 11$ as $26 - 15$ is divisible by 11

or 26 & 15 leave same remainder (4) when divided By 11

So when dealing with situations where we consider 2 integers "the same" if they leave the same remainder when divided By n. we do our ARithmetic on the set of Remainders instead of $\mathbb{Z}$. e.g

$n = 7$ The POSSIBLE remainders are:

$\mathbb{Z}_7 := \{0, 1, 2, 3, 4, 5, 6\}$

OR $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

? subtraction and "division":

(A) Subtraction: Note $0 \in \mathbb{Z}_7$

and As with ordinary integers e.g

$3 \in \mathbb{Z}$, -3 is the integer (unique)

s.t. $3 + (-3) = 0$ in $\mathbb{Z}$.

Now in $\mathbb{Z}_7$; $-3 \in \mathbb{Z}_7$ is the element we add to 3 to get 0 in $\mathbb{Z}_7$. But $0 \equiv 7 \bmod 7$

AND $3 + 4 = 0$ in $\mathbb{Z}_7$

(ie $3+4 = 7 \equiv 0 \bmod 7$)

So $-3 = 4$ in $\mathbb{Z}_7$

So e.g. $1 - 3 = 1 + (-3)$

$= 1 + 4 = 5$ in $\mathbb{Z}_7$

(OR $1 - 3 = -2 = 5$ in $\mathbb{Z}_7$

Because $5 + 2 = 0$ in $\mathbb{Z}_7$

So $-2 = 5$ in $\mathbb{Z}_7$)

Of Course $5 - 3 = 2$ still in $\mathbb{Z}_7$

Because $5 - 3 = 5 + (-3) = 5 + 4 = 9 \equiv 2 \bmod 7$)

Ex: $2 - 6 = 2 + (-6) = 2 + 1 = 3$ in $\mathbb{Z}_7$

(Because $1 + 6 = 0$ in $\mathbb{Z}_7$)

OR $2 - 6 = -4 = 3$ in $\mathbb{Z}_7$ (as $3 + 4 = 0$ in $\mathbb{Z}_7$)

Similarly: As with ordinary multiplication & "division"

$\frac{6}{2} = 6 \times 2^{-1}$ where

2^{-1} is the number s.t.

$2^{-1} \times 2 = 1$ ie $2^{-1} = 1/2$

So $6/2 = 6 \times 2^{-1} = 6 \times \frac{1}{2} = 3$

Now in $\mathbb{Z}_7$ e.g. 3^{-1} is the element in $\mathbb{Z}_7$ s.t. $3^{-1} \times 3 = 1$ in $\mathbb{Z}_7$

ie $3^{-1} \times 3 \equiv 1 \bmod 7$

But $5 \times 3 = 15 \equiv 1 \bmod 7$ $(15 = 7(2)+1)$

so $5 \times 3 = 1$ in $\mathbb{Z}_7$

ie $3^{-1} = 5$ ($\&\ 5^{-1} = 3$) in $\mathbb{Z}_7$

Ex: Find 4^{-1} in $\mathbb{Z}_7$ ie $4^{-1} \times 4 = 1$ in $\mathbb{Z}_7$

$2 \times 4 = 8 \equiv 1 \bmod 7$

ie $2 \times 4 = 1$ in $\mathbb{Z}_7$ so $4^{-1} = 2$ in $\mathbb{Z}_7$

($\&\ 2^{-1} = 4$ in $\mathbb{Z}_7$)

So a general way to get inverses (mod n) ie in $\mathbb{Z}_n$ if the exist is as follows:

$n = 7$: Find 5^{-1} in $\mathbb{Z}_7$

Note: $\gcd(7, 5) = 1$ so can find m & $n \in \mathbb{Z}$ s.t.

$$1 = m7 + n5$$

But $(m)(7) = 0$ in $\mathbb{Z}_7$ (remainder = 0 when div by 7)

so $1 = 0 + n5 \Rightarrow 1 = n5$

So n OR its Remainder when divided By 7 is 5^{-1} in $\mathbb{Z}_7$.

$$7 = 5(1) + 2$$
$$5 = 2(2) + 1$$
$$\Rightarrow 1 = 5 - 2(2)$$
$$= 5 - 2[7 - 5]$$
$$= \underbrace{(-2)7}_{\text{a Multiple of 7}} + (3)5$$
$$1 = 0 + (3)(5)$$
$$\Rightarrow 5^{-1} = 3 \text{ in } \mathbb{Z}_7.$$