Modular Arithmetic

Divisibility

If a and b are integers, a **divides** b if there is an integer c such that

$$ac = b.$$

The notation $a \mid b$ means that a divides b.

For example, $3 \mid 6$, since $3 \cdot 2 = 6$.

GO CLASSES

a divides b

English

↳ 3 divides 6

$3 \times 2 = 6$

math

↳ $3 \mid 6$

GO CLASSES

$\neg\ 2 \mid 4$ T / F True

$\neg\ 2 \mid 5$ T / F False

$\neg\ 4 \mid 2$ T / F False

The notation "$a \mid b$" is read "a divides b", which is a **statement**

— a complete sentence which could be either true or false.

Check Your Understanding. Which of the following are true?

5 | 1 F

25 | 5 F

5 | 0 T

3 | 2 F

1 | 5 T

5 | 25 T

0 | 5 F

2 | 3 F

https://courses.cs.washington.edu/courses/cse311/18sp/slides/lecture10-setsmod.pdf

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k

circle is true

The Division Algorithm

The Division Algorithm

THE DIVISION ALGORITHM Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

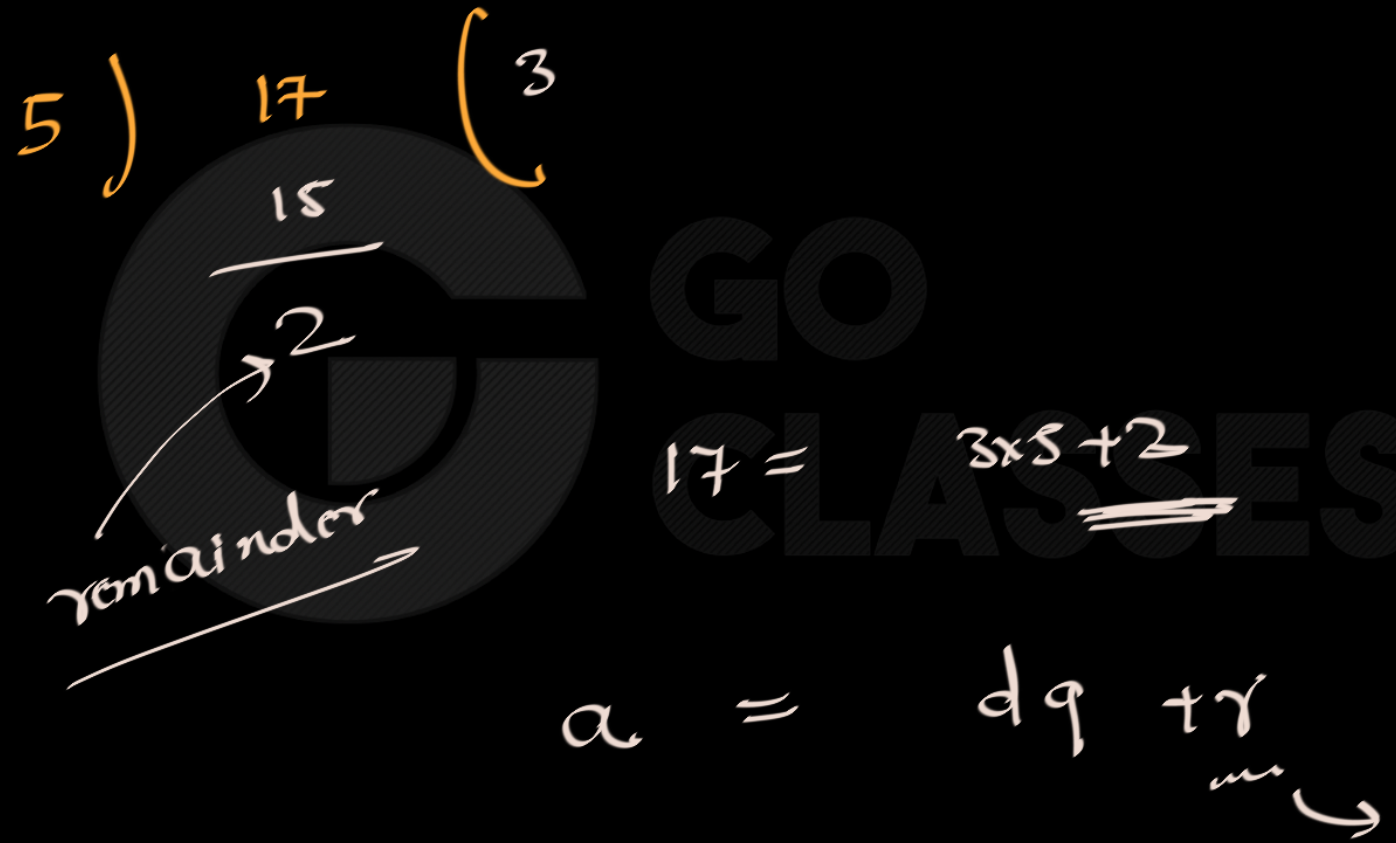
$r = a \bmod d$

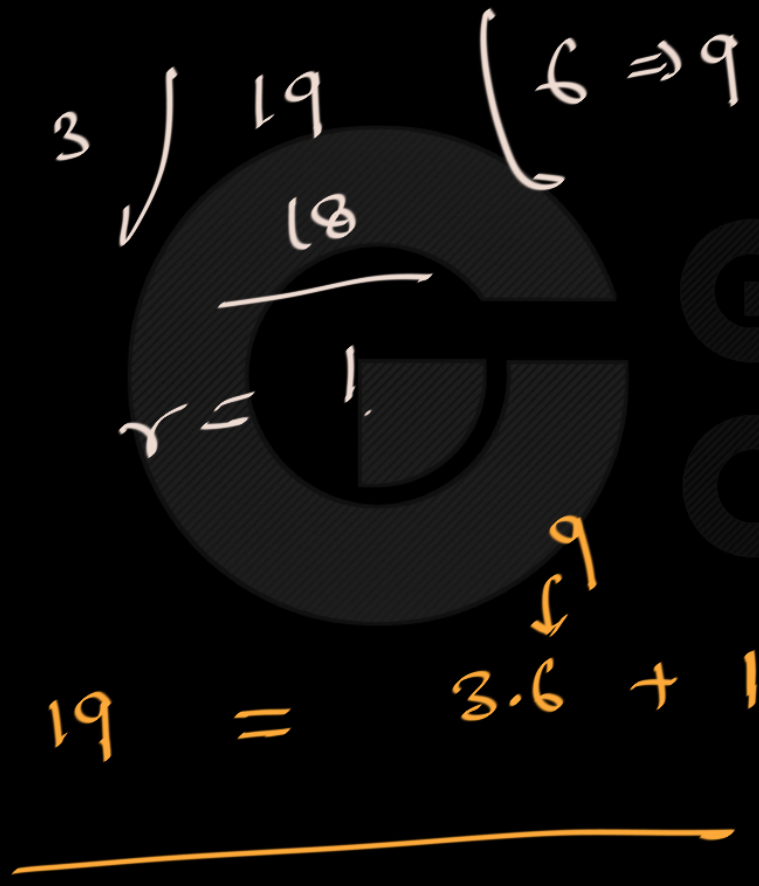
$a = dq + r$

$d \overline{)\, a \quad (q}$

$\underline{\quad\quad\quad}$

r


5) 17 (3
15
2
remainder
17 = 3×5 + 2
a = dq + r


3 | 19
18
r = 1
6 ⇒ 9
19 = 3.6 + 1
9
r

Question:

What are the quotient and remainder when 101 is divided by 11?

$r = 2$

$q = 9$

$11) \; 101 \; (9$

99

2

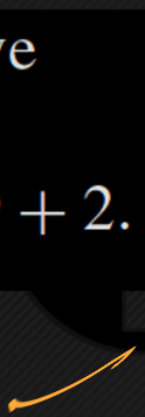
$\therefore r$

$101 = 9 \cdot 11 + 2$

Solution

Solution: We have

$$101 = 11 \cdot 9 + 2.$$



Question

What are the quotient and remainder when −11 is divided by 3?

option1

$-11 = -4 \cdot 3 + 1$ $\quad r = 1$

$q = -4$

option2

$-11 = -3 \cdot 3 - 2$ $\quad r = -2$

$q = -3$

$r \geq 0$

$\boxed{0 \leq r < d}$

$-11 = -4 \cdot 3 + 1$ $\quad r = 1$, $q = -4$

$$11 = 3 \cdot 3 + 2$$

From now on, for us remainder is always non negative

16 divide by 7

$16 = 7 \cdot 2 + 2$

21 divide by 9

$21 = 2 \cdot 9 + 3$

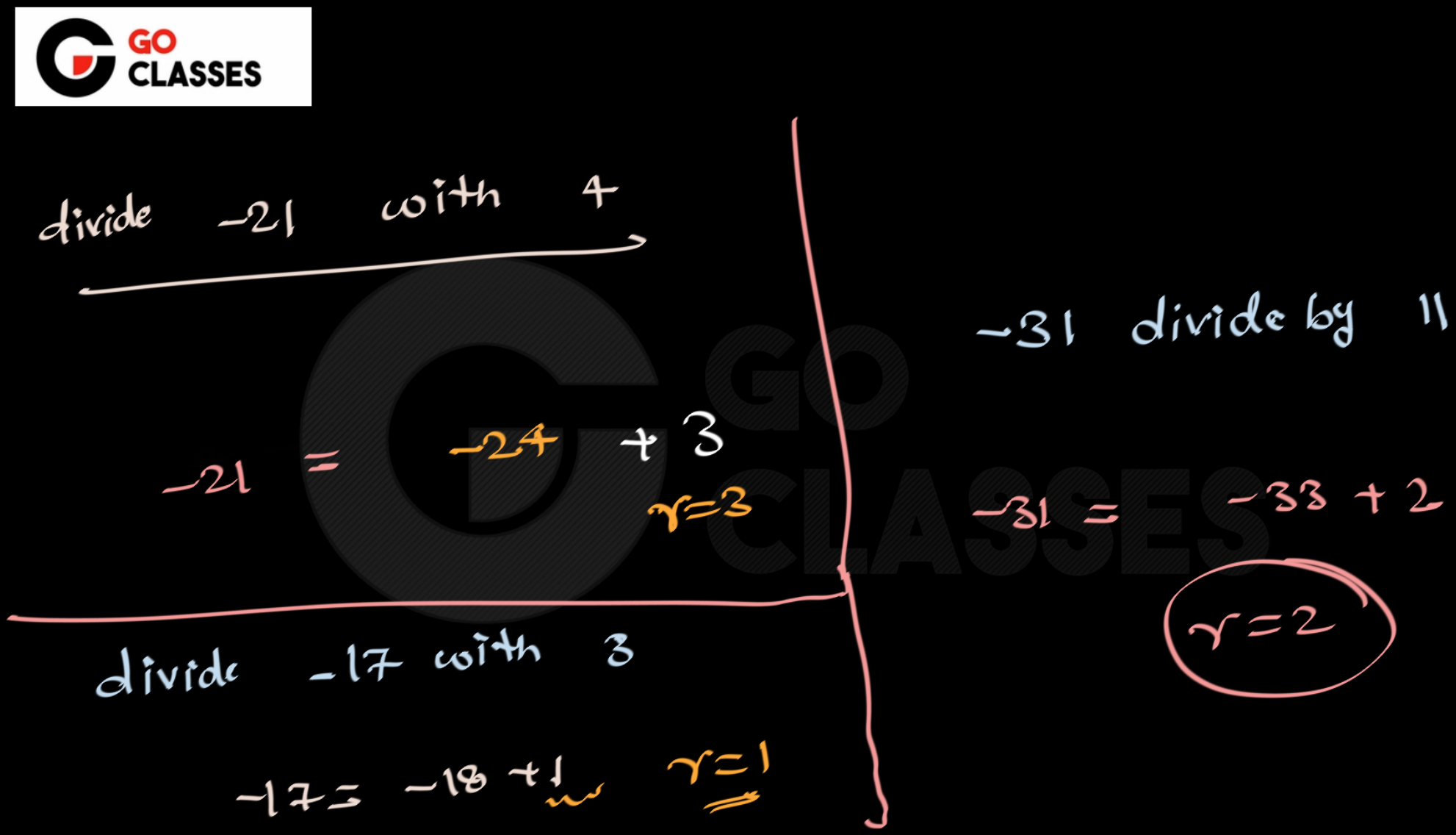
-16 divide by 7

$-16 = -21 + 5$

$= -3 \cdot 7 + 5$

-11 divided by 3

$-11 = -3 \cdot 4 + 1$


divide -21 with 4
-21 = -24 + 3
r=3
divide -17 with 3
-17 = -18 + 1
r=1
-31 divide by 11
-31 = -33 + 2
r=2

Solution: We have

$$-11 = 3(-4) + 1.$$

Note that the remainder cannot be negative. Consequently, the remainder is *not* -2, even though

$$-11 = 3(-3) - 2,$$

because $r = -2$ does not satisfy $0 \leq r < 3$.

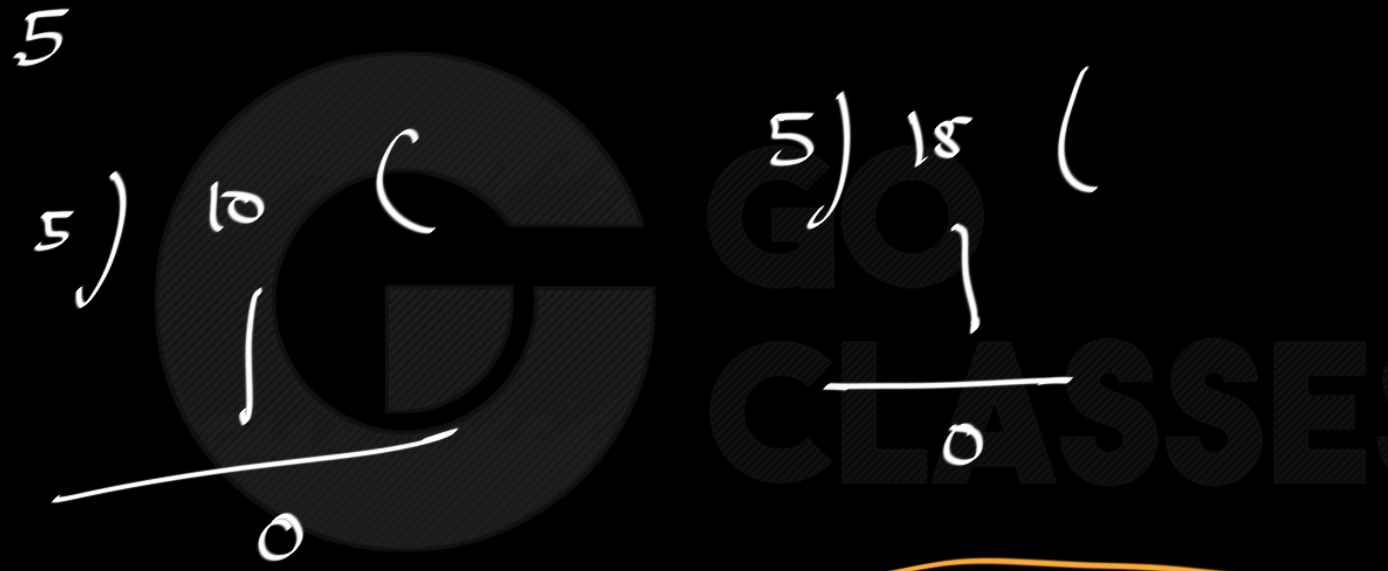
Modular Arithmetic

What does a **mod** m represent ?

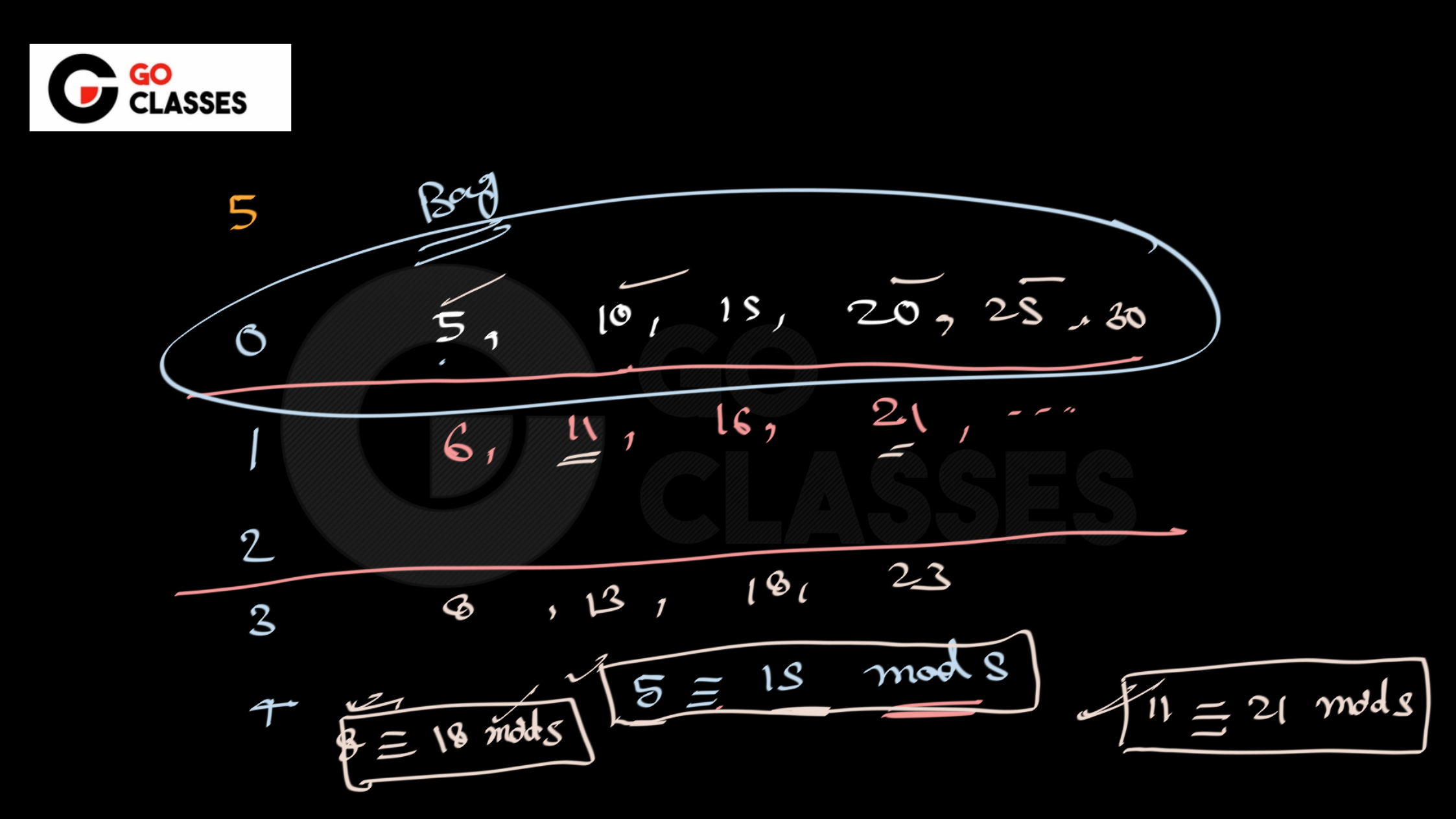
If two numbers a and b leave the same remainder when divided by a third number m, then we say "a is congruent to b modulo m", and write $a \equiv b \pmod{m}$.

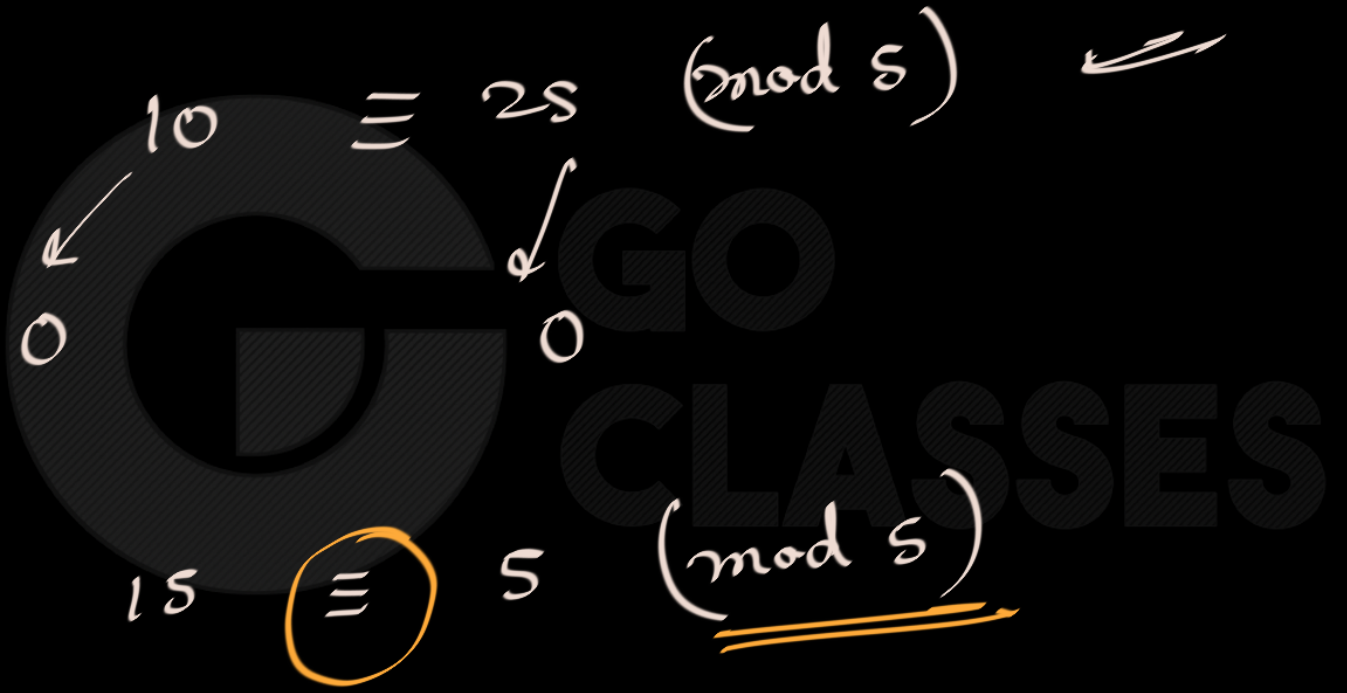
$$a \equiv b \pmod{m}$$

https://www.math.toronto.edu/rosent/Mat246Y/PDF/cong.pdf



$$10 \equiv 15 \pmod 5$$


GO CLASSES
5
Bag
0
5, 10, 15, 20, 25, 30
1
6, 11, 16, 21, ...
2
3
8, 13, 18, 23
4
8 ≡ 18 mod 5
5 ≡ 15 mod 5
11 ≡ 21 mod 5


10 ≡ 25 (mod 5)
0 0
15 ≡ 5 (mod 5)

$5 \mod 3 = 2$

$5 \equiv 15$

this kind of statements are not valid

$5 \equiv 15 \pmod 5$ valid

$5 \equiv 1 \pmod 3$ is False

$5 \equiv 1 \pmod 5$ is true.

Gauss came up with the congruence notation to indicate the relationship between all integers that leave the same remainder when divided by a particular integer. This particular integer is called the modulus, and the arithmetic we do with this type of relationships is called the Modular Arithmetic. For example, the integers 2, 9, 16, all leave the same remainder when divided by 7. The special relationship between the numbers 2, 9, 16 with respect to the number 7 is indicated by saying these numbers are congruent to each other modulo 7, and writing,

$16 \equiv 9 \equiv 2 \ (\mathrm{mod} 7)$.

$-7 = -9 + 2$

$-9 = -9 + 0$

$5 \equiv -2 \mod 3$

$5 \equiv 8 \mod 3$

GO CLASSES

T/F

$5 \equiv -2 \pmod 3$

1

False

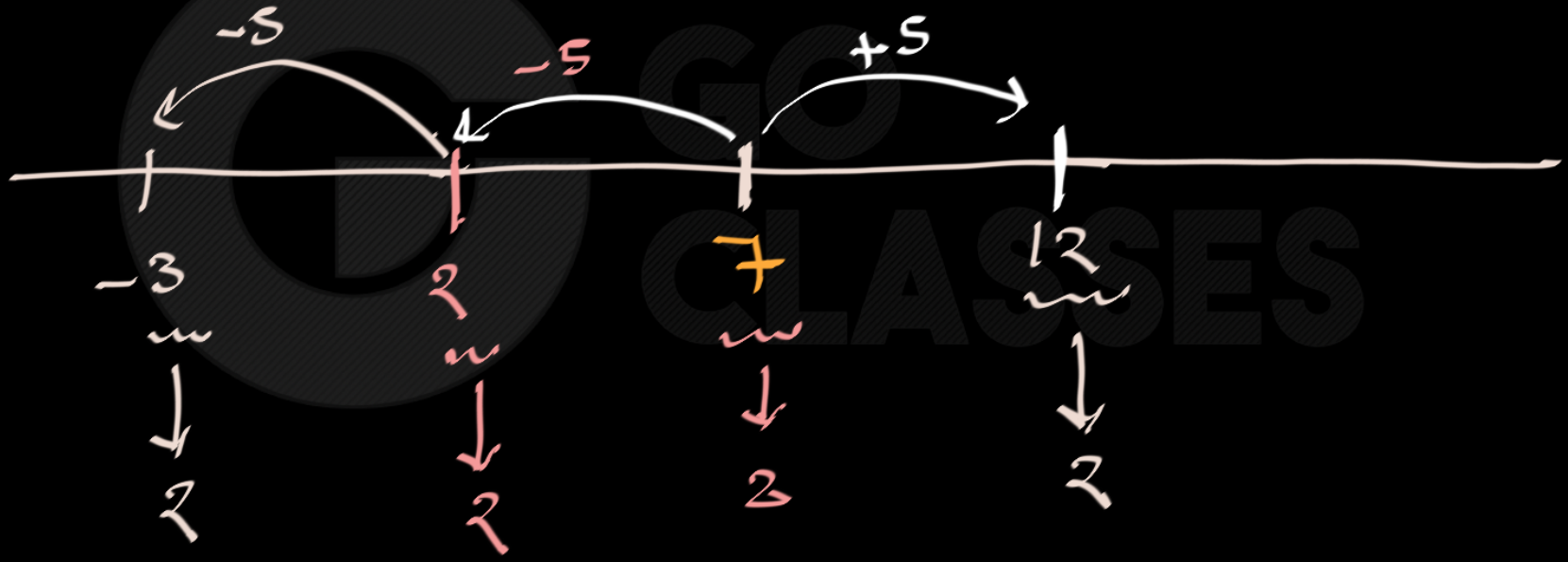
2

$-2 = -3 + 1$

$= -1 \times 3 + 1$

GO CLASSES

mod 5



$a \mod n = r$

$\frac{a}{n} = r$ ← remainder

$a \,\%\, n = r$

$\frac{a+n}{n} = r$

$\frac{a+2n}{n} = r$

$\frac{a-n}{n} = r$

$a \mod n = r$

$a - nk \mod n = r$

Difference b/w

= 2

vs

5 mod 2

= 1

Given

Suppose $a \equiv b \pmod n$

then $a + n \equiv b + n \pmod n$

Given $a \bmod n = r$

$b \bmod n = r$

Given

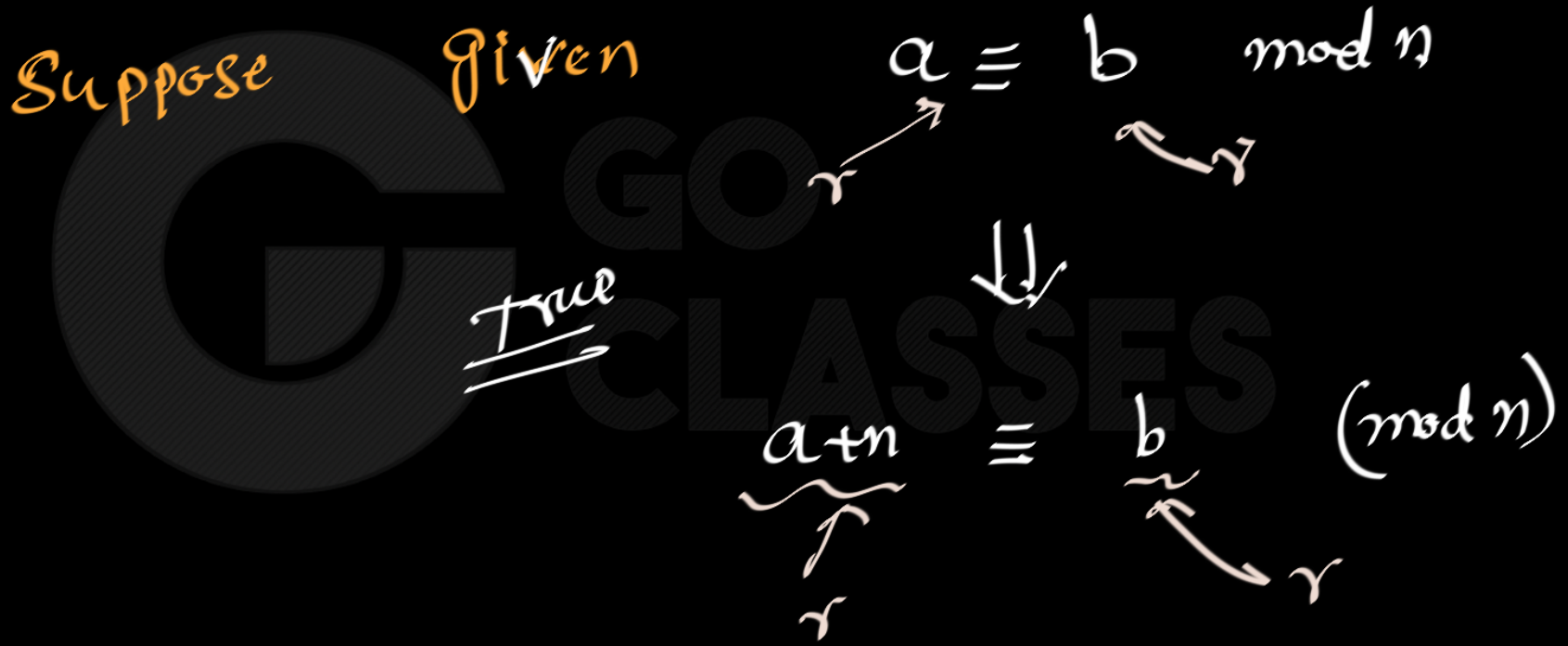
$46 \equiv 31 \pmod 5$

$16 + 5 \equiv 31 + 5 \pmod 5$

$21 \equiv 36 \pmod 5$

$21 \to 1$

$36 \to 1$


Suppose
Given
a ≡ b mod n
r
r
True
a+n ≡ b (mod n)
r
r

Suppose Given $a \equiv b \pmod{n}$

True ⇓

$a+n \equiv b+100n \pmod{n}$

Suppose Given $a \equiv b \pmod{n}$

True

$\Downarrow$

$a + nk_1 \equiv b + nk_2 \pmod{n}$

True/False

Every number is congruent to itself for any modulus; that is,

$a \equiv a \ (mod\ m)$ for any $a, \mathrm{m} \in Z$

Every number is congruent to any other number mod 1; that is,

$a \equiv b \ (mod\ 1)$ for any $a, \mathrm{b} \in Z$

True/False

Every number is congruent to itself for any modulus; that is,

True

$a \equiv a \ (mod\ m)$ for any $a, \mathrm{m} \in Z$

Every number is congruent to any other number mod 1; that is,

True

$a \equiv b \ (mod\ 1)$ for any $a, \mathrm{b} \in Z$

0 0

Check Your Understanding. What do each of these mean? When are they true?

$x \equiv 0 \pmod 2$ ⟶ x must be even

$-1 \equiv 19 \pmod 5$ TRUE

$0 \equiv 20 \pmod 5$

$-1 \equiv 19 \pmod 5$

$y \equiv 2 \pmod 7$

2, 9, 16, ...

$-1 + 5 \equiv 19 \pmod 5$

$-1 = -5 + 4$

$4 \equiv 19 \pmod 5$

$y \equiv 2 \pmod 7$

GO CLASSES

2 ⇒ Possible remainders are 0, 1

d ⇒ Possible remainders are 0, ..., d-1

1 ⇒ Possible remainder = 0

$a \equiv b \pmod{d}$

1) 19 (19

0

1) 20 (20

0

Check Your Understanding. What do each of these mean? When are they true?

$x \equiv 0 \pmod 2$

This statement is the same as saying “x is even”; so, any x that is even (including negative even numbers) will work.

$-1 \equiv 19 \pmod 5$

This statement is true. 19 - (-1) = 20 which is divisible by 5

$y \equiv 2 \pmod 7$

This statement is true for y in { ..., -12, -5, 2, 9, 16, ...}. In other words, all y of the form 2+7k for k an integer.

$y \equiv 9 \pmod 7$

Ex. 1 The equation

$x \equiv 16 (\mathrm{mod} 10)$

$x \equiv 6 \pmod{10}$

6

$-14, -4, 6, 16, 26$

Ex. 1 The equation

$$x \equiv 16 (\mathrm{mod} 10)$$

has solutions $x = \ldots, -24 - 14, -4, 6, 16, 26, 36, 46$

$a \equiv b \mod n$

$10 \equiv 22 \mod 3$

↳ $a \equiv 4 \mod 10$

$a \equiv 14 \mod 10$

↳ $a \equiv 4 \mod 10$

$a \equiv 14 \mod 10$

↳ $a \equiv 4 \mod 10$

$a \equiv 14 \pmod{10}$

$14 \equiv 4 \pmod{10}$

4 is the remainder when 14 is divided by 10

$a \equiv r \pmod{n}$

r is the remainder when a is divided by n

$a \equiv r + nk \pmod{n}$

we get r as remainder on dividing a with n

$$a = nq + r$$

we get r as remainder on dividing b with n

$$b = nK + r$$

GO CLASSES

we get r as remainder on dividing a with n

$$a = nq + r$$

we get r as remainder on dividing b with n

$$b = nk + r$$

$$\therefore \quad a \equiv b \pmod{n}$$

GO CLASSES

$$a \equiv b \pmod{n}$$

$$a = nk_1 + r$$

$$b = nk_2 + r$$

$$a - b = n(k_1 - k_2)$$

$$a - b = nk$$

$\Rightarrow$ $a - b$ is multiple of n.

$a \equiv b \mod n$

$a - b \mod n = 0$

$\Downarrow$

$a - b$ is multiple of n.

$\Downarrow$

$a - b = nk$

$n \mid a - b$

GO CLASSES

① $a \equiv b \mod n$

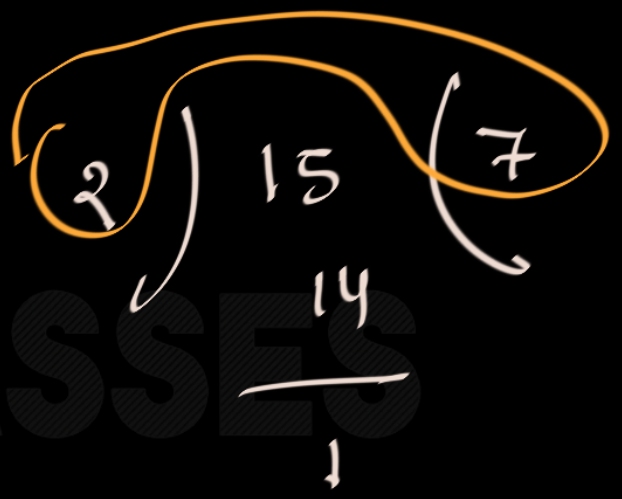
② $a \bmod n = b \bmod n$ (a and b leaves the same remainder)

③ $n \mid a-b$

GO CLASSES

Given $a \equiv b \pmod{n}$, where r is the remainder.

$\hookrightarrow a = q_1 n + r$



$15 = (2)7 + 1$

$$a \equiv b \,(mod\, n)$$

$$\Updownarrow$$

$$n \mid (a - b)$$

$$\Updownarrow$$

$$a \bmod n = b \bmod n$$

n divides a-b

$27 \equiv 15 \mod 4$

$27 - 15 = 12$

Which is/are true ?

$12 \equiv 8 \ (mod\ 4)$

$15 \equiv 12 \ (mod\ 3)$

$0 \equiv 12 \ (mod\ 13)$

$-1 \equiv 2 \ (mod\ 3)$

Which is/are true ?

$7 = 4\ (mod\ 3)$ ✗

$7 \equiv 4\ (mod\ 3)$ ✓

$a = b$

$7 = 4\ (mod\ 3)$

$7 = 1$ ✗ False

GO CLASSES

given $a \equiv b \pmod{n}$

$a \bmod n \equiv b \pmod{n}$

$r \equiv b \pmod{n}$

$$23 \equiv 33 \mod 10$$

$$(23 \mod 10) \equiv 33 \mod 10$$

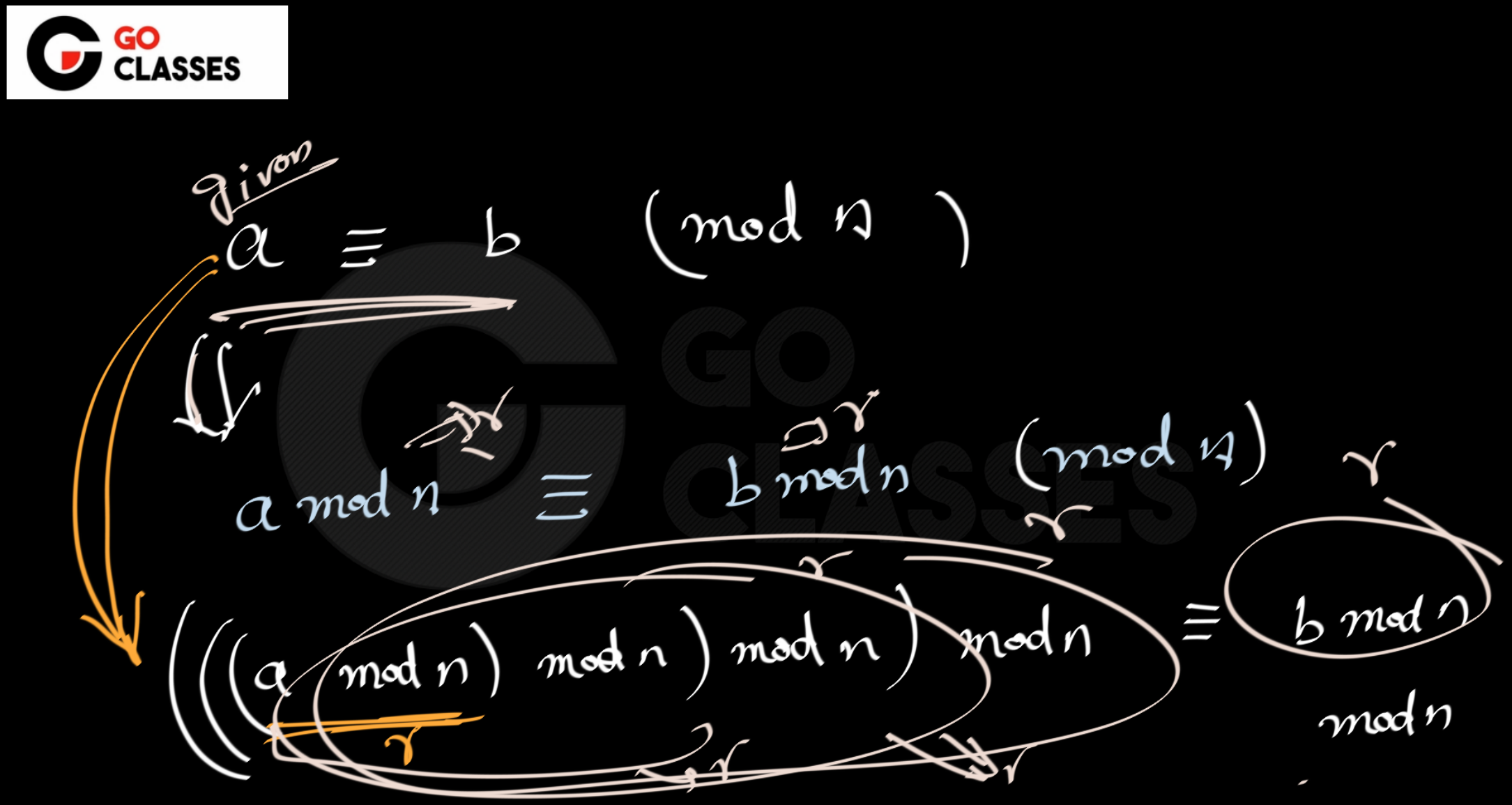
$$3 \equiv 33 \mod 10$$

$$3 \equiv 3 \mod 10$$

$$23 \equiv 33 \pmod{10}$$

$$(23 \bmod 10) \bmod 10 \equiv 33 \pmod{10}$$

$$3 \equiv 33 \pmod{10}$$


GO CLASSES
Given
$a \equiv b \pmod n$
$a \bmod n \equiv b \bmod n \pmod n$
r
$(((a \bmod n) \bmod n) \bmod n) \bmod n \equiv b \bmod n \bmod n$

We say that a *is congruent to* b *modulo* n , written $a \equiv b \pmod{n}$

if $n \mid (a - b)$.

Example

- ★ $23 \equiv 3 \pmod{10}$ since $10 \mid (23 - 3)$.
- ★ $23 \equiv 7 \pmod{8}$ since $8 \mid (23 - 7)$.
- ★ $10000 \equiv 4 \pmod{7}$ since $(10000 - 4) = 9996 = 1428 \cdot 7$.

True/False

$a \equiv a \,(mod\, n)$

$a \equiv -a \,(mod\, n)$

If $a \equiv b \,(mod\, n)$ then $b \equiv a \,(mod\, n)$.

If $a \equiv b \,(mod\, n)$ and $b \equiv c \,(mod\, n)$ then $a \equiv c \,(mod\, n)$.

True/False

$3 \equiv -3 \pmod 5$

$3 \equiv 3 \pmod 5$ ✓

$3 \equiv 2 \pmod 5$ ✓

$a \equiv a \pmod n$ ✓

$a \equiv -a \pmod n$ ✗

If $a \equiv b \pmod n$ then $b \equiv a \pmod n$. ✓

If $a \equiv b \pmod n$ and $b \equiv c \pmod n$ then $a \equiv c \pmod n$. ✓

$a \equiv b \pmod n \Rightarrow n \mid a-b$

$b \equiv c \pmod n \Rightarrow n \mid b-c$

$\Rightarrow n \mid a-c$

$\Rightarrow a \equiv c \pmod n$

$n \mid a-(-a)$

$\Rightarrow n \mid 2a$

$a = 10$

$n = 7$

$7 \mid 20$ ✗

$3 \equiv -3 \mod 5$ T/F