# 4A - Modular Arithmetics

Wednesday, 3 June 2026 11:06

## Divisibility

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

$a | b$ means $a$ divides $b$

$\therefore$ $3|6 \rightarrow$ 3 divides 6.

### Examples:

$5|1$ False

$5|0$ True

$1|5$ True

$0|5$ False

$25|5$ False $\rightarrow$ $5/25$

$3|2$ False $\rightarrow$ $2/3$

$5|25$ True $\rightarrow$ $25/5$

$2|3$ False $\rightarrow$ $3/2$

## The division algorithm

$5 \overline{) 17} \quad (3$

$15$

$2$

$\therefore$ $17 = 3 \times 5 + 2$

$\Rightarrow a = dq + r$

where $a, d, q, \& r$ are all integers

Also $\quad 0 \leq r < d$

eg

$$
\begin{array}{r|l}
3 \,)\, 19 & (\, 6 \\
\underline{18} & \\
1 &
\end{array}
$$

$\therefore r = 1, \quad q = 6$

So $\quad 19 = 3 \times 6 + 1$

$\qquad a = d \times q + r$

Q What are quotient & remainder when 101 is divided by 11

$$
\begin{array}{r|l}
11 \,)\, 101 & (\, 9 \\
\underline{99} & \\
2 &
\end{array}
$$

$\therefore \quad 101 = 9 \times 11 + 2$

$\qquad a = q \times d + r$

Q What are the quotient & remainder when $-11$ is divided by 3

$$
\begin{array}{r|l}
3 \,)\, -11 & (\, -3 \\
\underline{(-)\,-9} & \\
-2 &
\end{array}
$$

$\therefore \quad -11 = 3 \times (-3) + (-2)$

$\qquad a = d \times q + r$

So $q = -3$, $r = -2$

But we can also take values of
$q = -4$, $r = 1$

$\therefore \; -11 = -4(3) + (-1)$

Opt 1

$-11 = -4(3) + 1$ $\quad r = 1$
$\quad q = -4$

Opt 2

$-11 = -3(3) + (-2)$ $\quad r = -2$
$\quad q = -3$

But, $0 \leq r < d$

So, we take $r = 1$

$\therefore$ We take option 1.

Q – $-16$ divides by 7

$$7\,)\,-16\,(\,-3$$
$$(-)\,-21$$
$$\overline{\quad 6 \quad}$$

$\therefore \; -16 = 7(-3) + 5$

$\Rightarrow a = d \cdot q + r$

Q – divide $-21$ with 4

$-21 = 4 \times (-6) + 3$

$\therefore q = -6, \quad r = 3.$

Q divide $-17$ with 3

$-17 = 3(-6) + 1$

$q = -6, \; r = 1.$

Q divide $-31$ by 11

$-31 = 11 \times (-3) + 2$

$q = -3, \quad r = 2$

## Modulo

a mod m

$5 \overline{)\, 3 \,(} \, 0$
$\underline{0}$
$3$

3 mod 5 ← remainder

$\therefore$ 3 mod 5 = 3

$a \equiv b \bmod m$
↳ congruent

If 2 no's a & b leave the same remainder on being divided by a no. m, then both a & b are congruent.

5 ) 10 ( 2
   10
   ---
    0

5 ) 15 ( 3
   15
   ---
    0

$\therefore 10 \equiv 15 \pmod 5$

So for 5

remainders of 5:

| | | | | |
|---|---|---|---|---|
| 0 | 5 | 10 | 15 | 20 |
| 1 | 6 | 11 | 16 | 21 |
| 2 | | | | |
| 3 | 8 | 13 | 18 | 23 |
| 4 | | | | |

$5 \equiv 10 \bmod 5$

$6 \equiv 21 \bmod 5$

$8 \equiv 18 \bmod 5$

nos on both sides get same remainder on division by 5 (m)

$16 \equiv 9 \equiv 2 \pmod 7$

Q $5 \equiv -2 \pmod 3$

$5 \bmod 3 = 2$

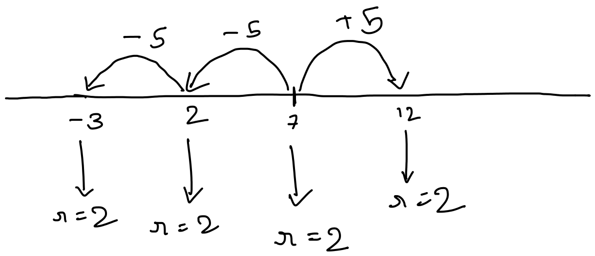
$-2 \bmod 3 = 1$

$-2 = 3 \times (-1) + 1$

Ans) False.

## Converting the (-)ve to (+)ve

lets take $7 \bmod 5 = 2$




So adding, or subtracting the n to m from m (mod n), and doing (mod n) to new no, the results will remain same.

Proof

$a \bmod n = r$

$\therefore a \% n = r$ — (1)

now $(a+n) \% n = r$ — (2)

$\because a \% n = r$ & $n \% n = 0$

now $(a+2n) \% n = r$ — (3)

$\because a \% n = r$ & $2n \% n = 0$

For negatives,

$$(a-n) \% n = r$$

$\because$ $a \% n = r$ & $(-n) \% n = -0$

Hence, if $a \bmod n = r$
$(a+nk) \bmod n = r$

Q Suppose $a \equiv b \pmod n$
then, is $a+n \equiv b+n \pmod n$

$\because$ $a \% n = b \% n$

$\Rightarrow (a+n) \% n = (b+n) \% n$

$\because$ $a \% n = r$, $b \% n = r$, $n \% n = 0$

$\therefore$ $(a+n) \equiv (b+n) \bmod n$ is True

Q) Every no. is congruent to itself for any modulus

i.e. $a \equiv a \pmod m$ for any $a, m \in \mathbb{Z}$

$a \equiv a \pmod m$

$\Rightarrow a \% m = a \% m$

— True

Q) Every no. is congruent to any other no. mod 1.

$$m \equiv n \pmod 1$$

$\therefore \Rightarrow m \% 1 = n \% 1 = 0$

— True.

Q// When are the following true

i) $x \equiv 0 \pmod 2 \Rightarrow x \% 2 = 0 \% 2$

$0 \% 2 = 0 \quad \therefore x \% 2 = 0$

So $x$ is even

ii) $-1 \equiv 19 \pmod 5 \Rightarrow -1 \% 5 = 19 \% 5$

$(-1 + 5 \times 4) = 19 \% 5 \quad = 19 \% 5$

— True

iii) $y \equiv 2 \pmod 7$

$\therefore \quad y \% 7 = 2 \% 7$

$\Rightarrow y \% 7 = 9 \% 7$

$\therefore \quad y$ can be $= \{2, 9, 16, \ldots (2 + 7n)\}$

iv) $x \equiv 16 \pmod{10}$

$x \% 10 = 16 \% 10$

$\Rightarrow x = \{\ldots -6, 6, 16, 26, 36 \ldots\}$

$= 16 + 10n, \quad n = \{-\infty, \infty\}$

$a \equiv r \pmod{n}$

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

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

$\therefore$ $a \bmod n = b \bmod n$ (a, b leave the same remainder).

So $(a - b) \bmod n = 0.$

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

True / False

(i) $12 \equiv 8 \pmod{4}$

$\Rightarrow 0 = 0 \rightarrow$ True

(ii) $15 \equiv 12 \pmod{3}$

$\Rightarrow 3 \mid 5 = 3 \mid 12 \rightarrow$ True

(iii) $0 \equiv 12 \pmod{13}$

$13 \mid 0 \Rightarrow 0$ $13 \mid 12 \rightarrow$ False

(iv) $-1 \equiv 2 \pmod{3}$

$$2 \equiv 2 \pmod 3 \rightarrow \text{True.}$$

**Q** $(23 \bmod 10) \bmod 10 \equiv 33 \bmod 10$

$\therefore\ 23 \bmod 10 = 3$ | $10\overline{)23}(2$, $\ \underline{20}$, $\ 3$

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

$\Rightarrow 3 = 33 \pmod{10}$

$10\overline{)3}(0$, $\ \underline{0}$, $\ 3$

$\therefore\ \dfrac{33-3}{10} = \dfrac{30}{10} \Rightarrow \text{True.}$

We say if $a \equiv b \bmod n$, if $n \mid (a-b)$