4B - Modular Arithmetic

Friday, 17 July 2026 19:55

$-7 \equiv -57 \pmod{10}$

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

Properties

If $a \equiv c \pmod{m}$
$b \equiv d \pmod{m}$

Then: $a + b \equiv c + d \pmod{m}$ — A

$a - b \equiv c - d \pmod{m}$ — B

$a \cdot b \equiv c \cdot d \pmod{m}$ — C

Q/ Prove given $a \equiv b \pmod{m}$

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

Proof: $a \equiv b \pmod{m}$ — 1

We can also say $\Rightarrow k \equiv k \pmod{m}$ — 2

Adding 1 & 2 using A.

$a + k \equiv b + k \pmod{m}$.

Q. Given $a \equiv b \pmod{n}$, which of these are true:

1. $a + n \equiv b \pmod{n} \rightarrow$ True

2. $a + 3n \equiv b + 2n \pmod{n} \rightarrow$ True

3. $a + k \equiv b + n \pmod{n} \rightarrow$ False

4. $a + k + 3n \equiv b + k \pmod{n} \rightarrow$ True

5. $a + 2k \equiv b + k \pmod{n} \rightarrow$ False

Q. $2 \equiv 7 \pmod{8}$ — (1)

$17 \equiv 25 \pmod{8}$ — (2)

$\therefore$ (1) $\times$ (2)

$= 34 \equiv 150 \pmod{8} \rightarrow$ True

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

$c \equiv d \pmod{n}$

So, $a \cdot c \equiv b \cdot d \pmod{n}$

Does it hold for division?

$8 \cdot \cancel{2} \equiv 3 \cdot \cancel{2} \pmod{10}$

$\Rightarrow \cancel{8} \equiv 3 \pmod{10} \rightarrow$ False.

Division by arbitrary no. is not possible.

If last digit is same for a, b, then c can be cancelled from both sides

$$8 \cdot \cancel{3} \equiv 88 \cdot \cancel{3} \pmod{10}$$

$$\Rightarrow 8 \equiv 88 \pmod{10}.$$

Solving a congruence:

Solve $3x + 4 \equiv 2x + 8 \pmod 9$

$$\Rightarrow 3x \equiv 2x + 4 \pmod 9$$

$$\Rightarrow x \equiv 4 \pmod 9$$

$$\therefore x = 4 + 9n, \quad n = \{-\infty, \infty\}$$

True / False

a) $101 \equiv 2 \pmod 3$ True

$\sqrt{99/3}$

b) $-101 \equiv 1 \pmod 3$

$(3 \times 34) - 101$
$= 102 - 101$

$\Rightarrow 1 \equiv 1 \pmod 3$ | $= 1$

True

Q. Reduce $100^5 \pmod 7$ to an element in standard residue system $\{0, 1, \ldots 6\}$

Standard Residue System: Set of all possible remainders when dividing a number by n.

eg: $n = 7$, $r = \{0, 1, 2, 3, 4, 5, 6\}$

Answer: $100^5 \pmod 7$

Step 1: Find $100 \pmod 7$

Step 2: Give power of 5 to output of step 1.

$\therefore\ 100^5 \pmod 7$

$= (100 \bmod 7)^5 \bmod 7$

$= (2)^5 \bmod 7$

$= 28 + 4 \pmod 7$

$$\begin{array}{r} 7\,)\,100\,(\,14 \\ 7 \\ \hline 30 \\ 28 \\ \hline 2 \end{array}$$

$= 4$ — Ans

Other method

$(2)^5 \bmod 7$

$= 2^3 \cdot 2^2 \bmod 7$

$= 1 \cdot 4$

$= 4$ — Ans.

Q. $994 \cdot 996 \cdot 997 \cdot 998 \pmod{1000}$

$= 994 \pmod{1000} \cdot 996 \pmod{1000} \cdot 997 \pmod{1000} \cdot 998 \pmod{1000}$.

$= (-6 \bmod 1000)(-4 \bmod 1000)(-3 \bmod 1000)(-2 \bmod 1000)$

$= (-6)(-4)(-3)(-2) \bmod 1000$

$= 144 \pmod{1000}$

Note: $994 \pmod{1000} = -6 \pmod{1000}$

Solve: $994 \equiv -6 \pmod{1000}$

$\Rightarrow 996 \equiv -6 + 1000 \pmod{1000}$

$\Rightarrow 996 \equiv 996 \pmod{1000}$

~ True

$\therefore 996 \pmod{1000} = -6 \pmod{1000}$.

Q) Can we simplify $17^{753} \pmod 9$

$17^{753} \pmod 9$

$\Rightarrow (17 \bmod 9)^{753}$

$\Rightarrow (8 \bmod 9)^{753}$

$\Rightarrow (-1 \bmod 9)^{753}$

Ans) 8 ($\because$ ans of r should be $0 \leq r < n$)

$\because 8 \equiv -1 \pmod 9$

$\Rightarrow 8 \equiv 8 \pmod 9$

Q) $13^{99} \pmod{17}$

$= (-4^{99}) \pmod{17}$

$= -4 (-4)^{98} \bmod 17$

$= -4 . ((-4)^2)^{49} \pmod{17}$

$= -4 . (16)^{49} \pmod{17}$

$= -4 \cdot (-1)^{49} \pmod{17}$

$= 4 \mod 17$

$= 4$ — Ans.

Q $3^{51} \pmod 5$

$= 3 \cdot (3^{50}) \pmod 5$

$= 3 \cdot (3^2)^{25} \pmod 5$

$5) 9 (2$
$\underline{10}$
-1

$= 3 \cdot (9)^{25} \pmod 5$

$= 3(-1) \mod 5$

$= -3 \mod 5$

$5) -3 (-1$
$\underline{+5}$
2

$= 2$ — Ans

No negative option.

$3 \cdot 9^{25} \pmod 5$

$= 3 \cdot (9 \mod 5)^{25} \mod 5$

$5) 9 (1$
$\underline{5}$
4

$= 3 \cdot (4^{25}) \mod 5$

$= 3 \cdot 4 \cdot (4^{24}) \mod 5$

$= 12 \cdot (4^2)^{24} \mod 5$

$= 12 \cdot (16 \mod 5)^{24}$

$= 12 \cdot (1^{24}) \mod 5$

$= 12 \mod 5$

$= 2$ — Ans.

Q. $17 \times 18 \mod 19$

$(-2)(-1) \pmod{19}$

$= 2 \mod 19$ — Ans.

Q. $18^{489312} \mod 19$

$= (-1)^{\text{even}} \mod 19$

$= 1$

Q. Find last digit of 7^{100}

To get last digit, divide num by 10 & get remainder.

$\therefore\ 7^{100} \pmod{10}$

$= (7 \bmod 10)^{100}$

$= (-3)^{100} \bmod 10$

$= 9^{50} \bmod 10$

$= (-1)^{50} \bmod 10$

$= 1$ — Ans.

Q. Last digit of 2017^{2017}

$2017^{2017} \bmod 10$

$= 7^{2017} \bmod 10$ $\quad\Big|\ \because\ 2017 \equiv 7 \pmod{10}$

$= (-3)^{2017} \bmod 10$

$= -3 \cdot (-3)^{2016} \bmod 10$

$= -3\ (9)^{1008} \bmod 10$

$= -3\ (-1)^{1008} \bmod 10$

$= -3 \bmod 10 \quad = 7$ — Ans.

Q. as $7 \cdot 9 \pmod{36}$

$= 63 \pmod{36} \equiv 27 \pmod{36}$

b) $8 - 21 \pmod{31}$

$= -13 \pmod{31} \equiv 18 \pmod{31}$

c) $68 \cdot 69 \cdot 71 \pmod{72}$

$= -4 \cdot -3 \cdot -1 \pmod{72}$

$= -12 \pmod{72} \equiv 60 \pmod{72}$

d) $108! \bmod 83$

$108! \,\%\, 83 = 0$

Ans) $0 \longrightarrow 108! \equiv 0 \pmod{83}$

Theorem: A number is divisible by 9 if only sum of digits in base 10 is divisible by 9.