Modular Arithmetic

Wednesday, September 10, 2025 10:04 AM

Missing.
100# (Ex) 2, 4, 5, 6, 7, 13, 14,
200# 3, 6, 7, 8, 10, 18, 28

1] Def^n $a \equiv b \pmod n$
if $n \mid (a-b)$

2] Facts:

① $a \equiv b \pmod n$
$\Rightarrow$ $a \bmod n = b \bmod n$

② $a \equiv b$ and $b \equiv c \pmod n$
$\Rightarrow$ $a \equiv c \pmod n$

3] Modular Arithmetic

Thrm: if $a \equiv b \pmod n$
and $c \equiv d \pmod n$

then $a \pm c \equiv b \pm d \pmod n$

$a \cdot c = b \cdot d \pmod n$

4] e.g.

① $128 + 27 \pmod 5$

$\equiv 3 + 2$

$\equiv 0$

② $2147 \cdot 3520 \pmod 7$

$= (2100 + 49 - 2) \cdot (3500 + 21 - 1)$

$\equiv (0 + 0 - 2) \cdot (0 + 0 - 1)$

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

$\equiv 2 \pmod 7$