Quick! For $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, define what it means for a to be congruent to b modulo n.

We say that a is congruent to b modulo n and write $a \equiv b \pmod{n}$ if and only if $n \mid (a-b)$. This is equivalent to saying there exists an integer k such that $a - b = kn$ or $a = b + kn$.

Congruence is an Equivalence Relation (CER)
Let $n \in \mathbb{N}$. Let $a, b, c \in \mathbb{Z}$. Then

1. (Reflexivity) $a \equiv a \pmod{n}$.
2. (Symmetry) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.
3. (Transitivity) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Proofs:

1. Since $n \mid 0 = (a - a)$, we have that $a \equiv a \pmod{n}$.
2. Since $n \mid (a - b)$, there exists an integer k such that $nk = (a - b)$. This implies that $n(-k) = b - a$ and hence $n \mid (b - a)$ giving $b \equiv a \pmod{n}$.
3. Since $n \mid (a - b)$ and $n \mid (b - c)$, by Divisibility of Integer Combinations, $n \mid ((a - b) + (b - c))$. Thus $n \mid (a - c)$ and hence $a \equiv c \pmod{n}$

L25 P3

Without a calculator, is $167 \equiv 2015 \bmod 4$

Sol'n: $2015 \equiv 3 \bmod 4 \because 4 \mid 2012 = 2015-3$

$167 \equiv 3 \bmod 4 \because 4 \mid 164 = 167-3$

By symmetry $3 \equiv 2015 \bmod 4$

By transitivity $167 \equiv 2015 \bmod 4$.

Alt Sol'n: Does $4 \mid 2015-167 = 1848$

Properties of Congruence (PC) Let $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then

1. $a + b \equiv a' + b' \pmod{m}$
2. $a - b \equiv a' - b' \pmod{m}$
3. $ab \equiv a'b' \pmod{m}$

Proofs:

1. Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid (a - a' + (b - b'))$. Hence $m \mid (a + b - (a' + b')$ and so $a + b \equiv a' + b' \pmod{m}$.
2. Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid (a - a' - (b - b'))$. Hence $m \mid (a - b - (a' - b')$ and so $a - b \equiv a' - b' \pmod{m}$.
3. Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid ((a - a')b + (b - b')a')$. Hence $m \mid ab - a'b'$ and so $ab \equiv a'b' \pmod{m}$.

Corollary If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for $k \in \mathbb{N}$.

Example: Since $2 \equiv 6 \mod 4$, we have that $2^2 \equiv 6^2 \mod 4$, that is, $4 \equiv 36 \mod 4$.

Is $5^9 + 62^{2000} - 14$ divisible by 7?

Sol'n: Reduce mod 7. By (PC)

$$5^9 + 62^{2000} - 14 \equiv (-2)^9 + (-1)^{2000} - 0 \mod 7$$
$$\equiv -2^9 + 1 \mod 7$$
$$\equiv -(2^3)^3 + 1 \mod 7$$
$$\equiv -(8)^3 + 1 \mod 7$$
$$\equiv -(1)^3 + 1 \mod 7$$
$$\equiv 0 \mod 7$$

$\therefore$ the number is divisible by 7.