Topic 2: Congruence Modulo

- Recall that the clock number is the additive identity (or zero). So, we can associate the integers with a particular clock by "wrapping" the integer number line around the clock. Therefore, there are infinitely many integers associated with each clock number. We express this symbolically as follows:

  Congruence Modulo m: Let a, b, and m be integers with $m \geq 2$. Then

  $$a \equiv b \pmod{m} \qquad \text{if and only if} \qquad m|\ (a-b).$$

  NOTE: To do this we need an extended version of "divides" which holds for integers. Namely,

  $$a|\ b \quad (a \neq 0) \ \text{ if there exists an integer } c \text{ such that } \ a \cdot c = b.$$

Example 1: True or False

(a) $8 \equiv 3 \pmod{5}$

(b) $7 \equiv 2 \pmod{6}$

(c) $14 \equiv 2 \pmod{6}$

(d) $25 \equiv 3 \pmod{13}$

Example 2: Describe all integers n, where $-20 \leq n \leq 20$, which make each of the following congruences true.

(a) $n \equiv 2 \pmod{9}$

(b) $5 \equiv n \pmod{4}$

(c) $12 \equiv 4 \pmod{n}$

- **Modular Arithmetic:** Congruences and equations have many similarities, as can be seen in the following results. For simplicity, the "mod m" will be omitted unless a particular m needs to be specified. As before, $m \geq 2$.

    1. $a \equiv a$ for all clock numbers a.
    2. If $a \equiv b$, then $b \equiv a$.
    3. If $a \equiv b$ and $b \equiv c$, then $a \equiv c$.
    4. If $a \equiv b$, then $a + c \equiv b + c$.
    5. If $a \equiv b$, then $ac \equiv bc$.
    6. If $a \equiv b$ and $c \equiv d$, then $ac \equiv bd$.
    7. If $a \equiv b$ and n is a whole number, then $a^n \equiv b^n$.

Example 3: Determine the remainder when 3^{100} is divided by 7.

Example 4: Find the remainder when 3^{98} is divided by 5.

Example 5: Find the last two digits of 4^{101}.