Definition. Suppose that a, b, n are integers, where $n > 0$. We say that a and b are congruent modulo n if and only if $n|(a-b)$. We write

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

and say "a is congruent to b modulo n".

Example.

$$\begin{aligned} 7 &\equiv 3 \pmod{4} \\ 18 &\equiv 0 \pmod{3} \\ 20 &\equiv 10 \pmod{5} \\ 9 &\equiv 27 \pmod{6} \end{aligned}$$

(1) Determine if the following statements are true.

(a) $2 \equiv 2 \pmod{5}$
(b) $19 \equiv 3 \pmod{7}$
(c) $19 \equiv 5 \pmod{7}$
(d) $0 \equiv 5 \pmod{1}$
(e) $18 \equiv 0 \pmod{2}$
(f) $25 \equiv 51 \pmod{13}$
(g) $25 \equiv -14 \pmod{13}$
(h) $-11 \equiv 17 \pmod{4}$
(i) $-18 \equiv -24 \pmod{5}$

(2) Find 10 numbers that can fill in the following blank

$$23 \equiv \underline{\qquad} \pmod{12}$$

(3) Find 5 numbers that can fill in the following blank

$$\underline{\qquad} \equiv -10 \pmod{7}$$

How many answers are there in a general question like this one? Can you *generalize* the answers that you got (that is, provide a formula)?

(4) Can you describe the integers m that satisfy the following congruences?

(a) $m \equiv 0 \pmod{4}$
(b) $m \equiv 1 \pmod{4}$
(c) $m \equiv 2 \pmod{4}$
(d) $m \equiv 3 \pmod{4}$
(e) $m \equiv 4 \pmod{4}$
(f) $m \equiv 5 \pmod{4}$
(g) $m \equiv -1 \pmod{4}$
(h) $m \equiv -2 \pmod{4}$
(i) $m \equiv -3 \pmod{4}$

What observations can you get here?

(5) True or false: $a \equiv a \pmod{n}$ for any values of a and any $n > 0$.

(6) True or false: If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

(7) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, is $a \equiv c \pmod{n}$? Can you give a reason?

(8) Let a, b, c, d, n be integers and $n > 0$. Give numeric examples to each statement. Then, give an argument why each statement is true.

(a) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.

(b) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a - c \equiv b - d \pmod{n}$.

(c) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

(9) Let $a \equiv b \pmod{n}$.

(a) Is it true that $a^2 \equiv b^2 \pmod{n}$?

(b) Is it true that $a^3 \equiv b^3 \pmod{n}$?

(c) Can these statements be generalized?

(10) We can code the English alphabet by assigning $A \to 1$, $B \to 2$, $C \to 3$, etc. Then, the Caesar cipher can be described using modular arithmetic. How would the equation be set?