The Definition of "(mod n)-congruence"

Definition: Let n be a positive integer.

Suppose a and b are any integers.

We say "a is congruent to b modulo n"

(and we write "$a \equiv b \pmod{n}$")

if and only if $a-b$ is an integer multiple of n.

That is, $a \equiv b \pmod{n} \iff a-b = nk$ for some integer k.

Note: If $a-b = nk$, then $b-a = n \times (-k)$, so

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

For example, $19 \equiv 7 \pmod{3}$, since $19-7=12$ and $12 = 3 \times 4$.

Also, $19 \not\equiv 8 \pmod{3}$, since $19-8 = 11$ and $11 \neq 3k$ for every integer k.

Theorem: For every positive integer n and every positive integer a, if r is the remainder when a is divided by n, then $a \equiv r \pmod{n}$.

Proof: Let n be any positive integer and let a be any positive integer. When a is divided by n, this division results in a quotient q and a remainder r.

$$\left[\begin{array}{r} q \\ n\,\overline{)\,a} \\ -qn \\ \hline r \end{array}\right]$$

Then $a = nq + r$ and $0 \le r < n$.

$\therefore a - r = nq$ and q is an integer.

$\therefore a \equiv r \pmod{n}$. QED, by Direct Proof.