Prove: For integers a, b and positive integer m,
$a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$

Proof:

(Note: because this theorem is a biconditional, we must prove it in "both directions.")

First, assume $a \equiv b \pmod{m}$.

Then $m \mid (a - b)$, so there is $k \in \mathbf{Z}$ such that
$a - b = mk$.

Let $a \bmod m = r$.
Then, according to the division algorithm, there is $q \in \mathbf{Z}$ such that
$a = mq + r$, $0 \leq r < m$.

Using $a = mq + r$ to replace a in $a - b = mk$ we get

$mq + r - b = mk$

So

$mq - mk + r = b$

$m(q - k) + r = b$

This shows that r is the remainder when b is divided by m,
so $b \bmod m = r$ ($= a \bmod m$).

We have proven that if $a \equiv b \pmod{m}$ then $a \bmod m = b \bmod m$.

Conversely, assume $a \bmod m = b \bmod m$.

Let $r = a \bmod m = b \bmod m$.

Then, according to the division algorithm, there are $q_1, q_2 \in \mathbf{Z}$ such that
$a = mq_1 + r$,
$b = mq_2 + r$, $0 \leq r < m$.

Then
$a - b = mq_1 + r - (mq_2 + r)$

$= mq_1 + r - mq_2 - r$

$= mq_1 - mq_2$

$= m(q_1 - q_2)$

This shows that $m \mid (a - b)$, so $a \equiv b \pmod m$.

We have proven that
if $a \bmod m = b \bmod m$ then $a \equiv b \pmod m$.

This concludes the proof.