Number Theory (D)

Prove:

Prove that $m =_{(n)} p$ if and only if $m\%n = p\%n$.

proof

I will prove that $m =_{(n)} p$ if and only if $m\%n = p\%n$, by showing that

(a) if $m =_{(n)} p$, then $m\%n = p\%n$,

(b) if $m\%n = p\%n$, then $m =_{(n)} p$.

proof of (a)

By definition of %,

$$m\%n = m - (m \div n)n;$$
$$p\%n = p - (p \div n)n.$$

Therefore, $m\%n - p\%n = (m - p) - ((m \div n) - (p \div n))n$.
By definition of mod, if $m =_{(n)} p$, then $n|(m - p)$.Plus, $n|((m \div n) - (p \div n))n$.
Therefore, $n|(m\%n - p\%n)$. From fact, we know that $0 \leq m\%n < n$, so $m\%n - p\%n$ can only be 0.
Therefore, $m\%n = p\%n$.

proof of (b)

Let $m\%n = p\%n = p'$,
so $m = \lfloor \frac{m}{n} \rfloor n + p'$ and $p = \lfloor \frac{p}{n} \rfloor n + p'$.
so $m - p = (\lfloor \frac{m}{n} \rfloor - \lfloor \frac{p}{n} \rfloor)n$.
so $m = (\lfloor \frac{m}{n} \rfloor - \lfloor \frac{p}{n} \rfloor)n + p$.
Therefore, $n|(m - p)$.
Therefore, $m =_{(n)} p$.
Therefore,$m =_{(n)} p$ if and only if $m\%n = p\%n$.