2. Consider positive integers a, b, n s.t. $(a,n)=1$ and $a \equiv b \pmod{n}$. Prove that $(b,n)=1$.

Pf By Bezout, $\exists\, s,t \in \mathbb{Z}$, $as+nt=(a,n)=1$.

Since $a \equiv b \pmod{n}$, $b = a+kn$ for some $k \in \mathbb{Z}$

So $(b,n)=(a+kn,n)$

So it suffices to prove $(a+kn,n)=1$

Assume for sake of contradiction that $(a+kn,n)=m>1$

then $m \mid (a+kn)$ and $m \mid n$

So $n = pm$ for some $p \in \mathbb{Z}$

$a+kn = qm$ for some $q \in \mathbb{Z}$

so $a = qm - kn = qm - kpm$
$= (q-kp)m$

Therefore $m \mid a$

So a, n has at least m as a common divisor, contradicting $(a,n)=1$

Therefore we have proved:
$(a+kn,n)=1$, that is, $(b,n)=1$

3. Given $a, b, n \in \mathbb{Z}^+$. If $[a]_n = [b]_n$, then $(a,n) = (b,n)$?

True.

<u>Pf</u>. Since $[a]_n = [b]_n$, by its definition $a \equiv b \pmod{n}$

So $b = a + kn$ for some $k \in \mathbb{Z}$.

Claim 1: $\boxed{(b,n) \geq (a,n)}$

Let d be arbitrary common divisor of b and n

Since $d \mid b$, $d \mid n$

$b = pd$, $n = qd$ for some $p, q \in \mathbb{Z}$

So $a = b - kn = pd - kqd = (p-kq)d$

Since $p - kq \in \mathbb{Z}$, $d \mid a$

Therefore any common divisor of b, n also divides a, so (b,n) divides a.

Since (b,n) also divides n

(b,n) is a common divisor of a, n

So $(b,n) \geq (a,n)$ by definition of greatest common divisor.

Claim 2: $(a,n) \geq (b,n)$

Let d_2 be arbitrary common divisor of a and n.

Since $d_2 | a$, $d_2 | n$

$a = p_2 d_2$, $n = q_2 d_2$ for some $p_2, q_2 \in \mathbb{Z}$.

So $b = a + kn = p_2 d_2 + k q_2 d_2$

$= (p_2 + k q_2) d_2$

Since $(p_2 + k q_2) \in \mathbb{Z}$, $d_2 | b$

Therefore any common divisor of a, n also divides b. So (a,n) divides b

Since (a,n) also divides n by definition, (a,n) is a common divisor of b, n.

So $(a,n) \geq (b,n)$ by definition of greatest common divisor.

Conclusion: Since $(b,n) \geq (a,n)$

$(a,n) \geq (b,n)$

We have proved $(a,n) = (b,n)$.