Proof of theorem

Proof.

- Assume that $a \equiv b \pmod{n}, \quad c \equiv d \pmod{n}$.
- Then $n|(b-a)$ and $n|(d-c)$, so $b-a = kn$ and $d-c = ln$ for some $k, l \in \mathbb{Z}$.
- Simplifiying gives $b = kn + a, d = ln + c$.
- Then we have

$$bd = (kn+a)(ln+c) = kln^2 + aln + kcn + ac,$$

or

$$bd - ac = n(kln + al + kc), \tag{1}$$

so $ac \equiv bd \pmod{n}$.

- Also,

$$b + d = (kn+a) + (ln+c) = (k+l)n + (a+c),$$
$$(b+d) - (a+c) = (k+l)n,$$

so $a + c \equiv b + d \pmod{n}$.

□