

Theorem

$$a \equiv b \pmod{n} \iff n|(b - a).$$

Proof, part 1.

\implies Let us assume that $a \equiv b \pmod{n}$. Then

$$a = q_1n + r,$$

$$b = q_2n + r.$$

Then we compute

$$b - a = (q_1n + r) - (q_2n + r) = q_1n - q_2n + r - r = n(q_1 - q_2).$$

Therefore $(b - a)$ is a multiple of n .