

## Theorem

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

## Proof, part 2.

$\Leftarrow$  Let us assume that  $n|(b-a)$ , or  $b-a = kn$ . Then if

$$a = q_1n + r_1,$$

$$b = q_2n + r_2,$$

we have

$$r_2 - r_1 = b - a + q_1n - q_2n = (k + q_1 - q_2)n.$$

This implies that  $n|(r_2 - r_1)$ . But we also have

$$\left. \begin{array}{l} r_2 < n, \\ r_1 \geq 0 \end{array} \right\} \implies r_2 - r_1 < n, \quad \left. \begin{array}{l} r_1 < n, \\ r_2 \geq 0 \end{array} \right\} \implies r_2 - r_1 > -n$$

and so

$$-n < r_2 - r_1 < n.$$

The only multiple of  $n$  that is strictly between  $-n$  and  $n$  is zero!