

**1.28 Theorem.** Let  $a, b, n \in \mathbb{Z}$  with  $n > 0$ . Then  $a \equiv b \pmod{n}$  if and only if  $a$  and  $b$  have the same remainder when divided by  $n$ . Equivalently,  $a \equiv b \pmod{n}$  if and only if when  $a = nq + r$  ( $0 \leq r < n$ ) and  $b = nq' + r'$  ( $0 \leq r' < n$ ), then  $r = r'$ .

**Proof.** Let  $a, b, n \in \mathbb{Z}$  with  $n > 0$  be given, and let  $a \equiv b \pmod{n}$ . By definition,  $a - b = nk$  for some  $k \in \mathbb{Z}$ . Thus,

$$\begin{aligned} a &= nk + b \\ &= nk + nq' + r' \\ &= n(k + q') + r'. \end{aligned}$$

Examining  $a = nq + r$  and  $a = n(k + q') + r'$ , by uniqueness of TDA,  $r = r'$ .

Let  $r = r', a = nq + r$ , and  $b = nq' + r'$  be given. Then,

$$\begin{aligned} a - nq &= b - nq', \text{ and} \\ a - b &= nq - nq' \\ &= n(q - q'). \end{aligned}$$

Thus,  $a - b = nt$  where  $q - q' = t$  for some  $t \in \mathbb{Z}$ , and  $a \equiv b \pmod{n}$ .  $\square$