

**1.11 Theorem.** Let  $a, b, c, n \in \mathbb{Z}$  with  $n > 0$ . If  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ , then  $a \equiv c \pmod{n}$ .

**Proof.** Let  $a, b, c, n \in \mathbb{Z}$  with  $n > 0$  be given such that  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ . Then by definition,  $n \mid (a-b)$  and  $n \mid (b-c)$ . We may choose  $t, u \in \mathbb{Z}$  such that  $a - b = nt$  and  $b - c = nu$ , by definition of divisibility. Using algebra,  $b = nu + c$ , and by substitution,

$$\begin{aligned} a - (nu + c) &= nt, \\ a - nu - c &= nt, \\ a - c &= nt + nu \\ &= n(t + u). \end{aligned}$$

By CPI, we may choose  $k \in \mathbb{Z}$  such that  $t+u = k$ . Therefore,  $a - c = nk$ , and by definition of divisibility,  $n \mid (a - c)$ . Lastly, by definition of congruence of modulo,  $a \equiv c \pmod{n}$ .  $\square$