

1.2 Theorem. Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$, then $a \mid (b - c)$.

Proof. Let $a, b, c \in \mathbb{Z}$ be given such that $a \mid b$ and $a \mid c$. We may choose $k, m \in \mathbb{Z}$ such that $b = ka$ and $c = ma$. Subtracting, we find

$$\begin{aligned} b - c &= ka - ma \\ &= a(k - m). \end{aligned}$$

By CPI, we may choose $f \in \mathbb{Z}$ such that $k - m = f$. Therefore, $b - c = fa$, and by definition, $a \mid (b - c)$. \square