Divisibility

Division of integers is problematic because it involves an apparent jump to rational numbers. In order to avoid this, division of integers is defined in terms of multiplication:

Definition

Let $n, m \in \mathbb{Z}, n \neq 0$. To say that n *divides* m, denoted $n \mid m$, means:

$$\exists\, k \in \mathbb{Z}, m = kn$$

The integer n is called a *divisor* or *factor* of m and m is called a *multiple* of n.

Theorem

$$\forall\, a, b \in \mathbb{Z}^+, a \mid b \implies a \leq b$$

Proof

Assume $a, b \in \mathbb{Z}^+$
Assume $a \mid b$
$\exists\, k \in \mathbb{Z}^+, b = ka$
ABC: $a > b$
$a > ka$
CONTRADICTION!
$\therefore a \leq b$

Theorem

Divisibility is transitive:

$$\forall, a, b, c \in \mathbb{Z}, a \mid b \text{ and } b \mid c \implies a \mid c$$

Proof

Assume $a, b, c \in \mathbb{Z}$
Assume $a \mid b$ and $b \mid c$
$\exists\, h, k, b = ha$ and $c = kb$
$c = k(ha) = (kh)a$
But, by closure, $kh \in \mathbb{Z}$
$\therefore a \mid c$

<u>Theorem</u>

$\forall\, a, b, c \in \mathbb{Z}, c \mid a$ and $c \mid b \implies \forall\, m, n \in \mathbb{Z}, c \mid (ma + nb)$

<u>Proof</u>

Assume $a, b, c \in \mathbb{Z}$
Assume $c \mid a$ and $c \mid b$
$\exists\, h, k \in \mathbb{Z}, a = hc$ and $b = kc$
Assume $m, n \in \mathbb{Z}$
$ma = m(hc) = (mh)c$
$nb = n(kc) = (nk)c$
$ma + nb = (mh)c + (nk)c = (mh + nk)c$
But, by closure, $mh + nk \in \mathbb{Z}$
$\therefore c \mid ma + nb$