

Divisibility

Definition: Let m, n be integers (short: $m, n \in \mathbb{Z}$).

Then m divides n (notation: $m|n$) if

$$n = m \cdot k, \text{ for some } k \in \mathbb{Z}.$$

We then also say that m is a divisor of n .

Thus: $m|n$ if and only if $k = \frac{n}{m} \in \mathbb{Z}$.

Properties of Divisibility (for future use):

D1 (Transitivity): $a|b, b|c \Rightarrow a|c$.

D2 (Product): $a|b, c|d \Rightarrow ac|bd$.

D3 (Linearity): $d|a, d|b \Rightarrow d|ax + by$,
for all $x, y \in \mathbb{Z}$.

D4 (Boundedness): $a|b$ and $a, b > 0 \Rightarrow a \leq b$.

Remarks: 1) Property **D3** is perhaps the most important property, for we shall use it time and again throughout the course.

2) Note that property **D4** tells us that in order to find the divisors of b , we only have to check finitely many numbers a .