



Definition

Let $a, b \in \mathbf{Z}$. a is a *divisor* of b if there exists $k > 0$ so that $ak = b$.

If instead $b = ak + r$ where $r > 0$ and $r < a$, then we call r the *remainder* of dividing a into b .

Notation

We denote the remainder of dividing a into b by $b \bmod a$.

