algorithms

divisibility ⇒

$a|b$ if $\exists c: ac = b$ $(a,b \in \mathbb{Z}, c \in \mathbb{Z}^+)$ (ex 3|15)

↳ prefix n

* reminder $0 \leq r < \text{divisior}$

modular arithmatic ⇒

if $a,b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then $a \equiv b \pmod m$ if $m \mid (a-b)$

congruent (uyum)

composite number ⇒

the number which is not prime.

$m \cdot n = \text{lcm}(m,n) \times \gcd(m,n)$