Divisibility & modular Arithmetic

Def: If $a, b \in \mathbb{Z}$ $a \neq 0$ we say a *divides* b if $\exists\ c \in \mathbb{Z}$ s.t. $b = a \cdot c$.
When a divides b we say a is a *factor* of b, or b is a multiple of a.
We use $a|b$ to denote a divides b, or $a \nmid b$ for a does not divide b.

Ex: $3 \nmid 7$ but $3 | 12$

$7/3$ is not an integer but $12 = 3 \cdot 4$.

Ex: Let $n, d \in \mathbb{Z}^+$ How many positive integers not exceeding n divide d?

To divide d we need to be of the form $d \cdot k$ $k \in \mathbb{Z}^+$ Thus we need the number of integers dk of the form $0 < dk \leq n$. or $0 < k \leq \frac{n}{d}$

Thus there are $\lfloor \frac{n}{d} \rfloor$ positive integers dividing d.

Theorem: Let $a, b, c \in \mathbb{Z}$, $a \neq 0$. Then:

(i) If $a|b$ & $a|c$ then $a|(b+c)$

(ii) If $a|b$ then $a|bc$ $\forall c \in \mathbb{Z}$.

(iii) If $a|b$ & $b|c$ then $a|c$.

pf: (i) $a|c \Rightarrow \exists\ d \in \mathbb{Z}$ s.t. $c = d \cdot a$ $a|b \Rightarrow \exists\ i \in \mathbb{Z}$ s.t.

$b = a \cdot i \Rightarrow$ $b + c = a + i + a \cdot d = a(i+d) \Rightarrow a|(b+c)$.

(ii). $a|b \Rightarrow \exists\ d \in \mathbb{Z}$ s.t. $b = a \cdot d$ then $\forall c \in \mathbb{Z}$ $bc = a \cdot d \cdot c$

$\Rightarrow a|bc$.

(iii) $a|b \Rightarrow \exists d \in \mathbb{Z}$ s.t. $b = a \cdot d$ $b|c \Rightarrow \exists i \in \mathbb{Z}$ s.t. $c = b \cdot i$

$\Rightarrow c = (a \cdot d) \cdot i = a \cdot p \Rightarrow a|c$.

□

Corollary: If $a, b, c \in \mathbb{Z}$ $a \neq 0$ s.t. $a|b$ & $a|c$ then $a|mb+nc$ $\forall m, n \in \mathbb{Z}$.
(combine (ii) & (i) of Theorem).

Theorem: Let $a \in \mathbb{Z}$, $d \in \mathbb{Z}^+$ then $\exists!$ (unique) $q, r \in \mathbb{Z}$ with $0 \leq r < d$ s.t.

$$a = dq + r.$$

This says, given any two integers we can do the division algorithm:

10, 3, $10 = 3 \cdot 3 + 1$ etc.

In the above d is called the divisor, q the quotient & r the remainder.

$$q = \left\lfloor \frac{a}{d} \right\rfloor \qquad r = a - qd.$$

e.g. 101, 11 $\qquad 101 = 9 \cdot 11 + 2.$

$-11, 3$ $-11 = 3(-4) + 1$

← super important! Some languages do this wrong!

Ex: In C, $-11 \% 3 = -2$ $\qquad -11 = 3(-3) + (-2)$

But this is **Incorrect** by definition of r, $0 \leq r < d$.