Divisibility

Definition: Let $a, b \in \mathbb{Z}$, $a \neq 0$. We say that a divides b if $\exists\, c \in \mathbb{Z}$ s.t. $b = ac$.

* If $a|b$, then a is called a divisor (or factor) of b and b is called a multiple of a.

Notation: $a|b$ means a divides b
$a \nmid b$ " a does not divide b

* $a|b$ is a statement whereas a/b is a rational number.

ex: $2|6$, $7|21$, $4\nmid 9$, $\underbrace{1|a \ \forall a \in \mathbb{Z}}$, $\because a = 1 \times \underbrace{a}_{c}$

$\underbrace{a|0}$ for all $a \neq 0$.

$0 = a \times \underbrace{0}_{c}$

$\underbrace{a|a}$ $\forall$ $a \neq 0$

$a = a \times \underbrace{1}_{c}$

Theorem 1.8: Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $b|c$ then $a|c$

Proof: Since $a|b$ and $b|c$, we've $b = ka$ and $c = \ell b$ for some $k, \ell \in \mathbb{Z}$.

Then, $c = l(ka) \Rightarrow c = (lk)a$
$\Rightarrow a \mid c$ (by def.)

ex: $3 \mid 9$ and $9 \mid 18$, so $3 \mid 18$

<u>Theorem 1.9</u>: Let $a, b, c \in \mathbb{Z}$, $c \neq 0$. If $c \mid a$ and $c \mid b$ then $c \mid (ma + nb)$ for any $m, n \in \mathbb{Z}$.

<u>Proof</u>: Since $c \mid a$ and $c \mid b$, we get
$a = ck$ and $b = cl$.
Then,

$$ma + nb = m(ck) + n(cl)$$
$$ma + nb = c\,(\underbrace{mk + nl}_{\in \mathbb{Z}})$$
$$\therefore\ c \mid (ma + nb)$$

ex: $3 \mid 12$ and $3 \mid 27$, so $3 \mid (\underbrace{2 \times 12 + 5 \times 27}_{24 + 135 = 159})$

ex: $c \mid a$ and $c \mid b \Rightarrow c \mid (a \pm b)$

<u>Theorem 1.10 (The Division Algorithm)</u>

Let $a, b \in \mathbb{Z}$ and $b > 0$. Then, $\exists$ unique integers q and r such that

$$a = bq + r \quad \text{with } 0 \leq r < b$$

ex: Divide 25 by 3

$$\underset{a}{\overset{\shortparallel}{25}} = \underset{b}{\overset{\shortparallel}{3}} \times \underset{q}{\overset{\shortparallel}{8}} + \underset{r}{\overset{\shortparallel}{1}} \qquad 0 \le \underset{r}{\overset{\shortparallel}{1}} < \underset{b}{\overset{\shortparallel}{3}}$$

$$\underset{a}{\overset{\shortparallel}{53}} = \underset{b}{\overset{\shortparallel}{8}} \times \underset{q}{\overset{\shortparallel}{6}} + \underset{r}{\overset{\shortparallel}{5}} \qquad 0 \le \underset{r}{\overset{\shortparallel}{5}} < \underset{b}{\overset{\shortparallel}{8}}$$

* q is called the quotient
r " " " remainder
a " " " dividend
b " " " divisor

Proof: We use well-ordering property.
Consider the set

$$S = \{ a - bk : k \in \mathbb{Z} \}$$

Let T be the subset of S such that

$$T = \{ a - bk : k \in \mathbb{Z},\ a - bk \geq 0 \}$$

Then, T is nonempty, since, for any integer k such such that $k < a/b$,

$a - bk > 0$.
By the well-ordering property, T has a least element. Let it be r.

Then,

$$r = a - bq \text{ for some } q \in \mathbb{Z}.$$

Let's show that $0 \leq r < b$.

By construction of T, it follows that $r \geq 0$.

To prove that $r < b$, assume that $r \geq b$.

Then,
$$r > \underbrace{r-b}_{\geq 0} = a - bq - b$$
$$= a - b(q+1)$$
$$\geq 0 \text{ (by assumption)}$$

This is a contradiction since $a-bq$ is the least nonnegative integer of the form $a-bk$ and $a-b(q+1) < a-bq$.

Hence $0 \leq r < b$.

Hence, $r = a - bq$ or

$$a = bq + r \text{ for some } q, r \in \mathbb{Z}$$
$$\text{with } 0 \leq r < b.$$

Next, we show that q and r are unique. Assume that they are not unique. Then,

$$\exists\ q_1, r_1, q_2, r_2 \text{ s.t.}$$

$$a = bq_1 + r_1 \quad \text{--- (1)}$$
$$a = bq_2 + r_2 \quad \text{--- (2)}$$

with $q_1 \neq q_2$, $r_1 \neq r_2$,

$$0 \leq r_1 < b, \quad \text{--- (3)}$$
$$0 \leq r_2 < b \quad \text{--- (4)}$$

(1) and (2) $\Rightarrow r_1 - r_2 = b(q_2 - q_1)$ --- (5)

$\Rightarrow b \mid (r_1 - r_2)$

Also,

(3) and (4) $\Rightarrow -b < r_1 - r_2 < b$

Hence, the only possibility is that

$$r_1 - r_2 = 0$$

because b does not divide any integer between $-b$ and b other than 0.

$\therefore r_1 = r_2$

$\therefore$ from (5), we get $q_1 = q_2$ ($\because b \neq 0$)

Hence, a contradiction to the fact that $r_1 \neq r_2$ and $q_1 \neq q_2$.

Hence, r and q are unique.

* q is the largest integer such that $bq \le a$, i.e., $q \le a/b$. Hence,

$$[a/b] = q, \quad r = a - [a/b]$$

ex: Let $n \in \mathbb{Z}^+$ and $x \in \mathbb{R}$. Show that

$$\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right].$$

By the division algorithm

$$[x] = nq + r \text{ for some } q, r \in \mathbb{Z} \text{ with } 0 \le r < n.$$

$$\therefore \frac{[x]}{n} = q + \frac{r}{n}$$

Note that, $\frac{r}{n} < 1$ and since q is an integer, $\left[q + \frac{r}{n}\right] = q$

$$\therefore \left[\frac{[x]}{n}\right] = [q] = q$$

We show that $q = \left[\frac{x}{n}\right]$.

First, notice that, we can write

$$x = [x] + \varepsilon \text{ for some } 0 \le \varepsilon < 1.$$

$\Rightarrow \quad x = nq + r + \varepsilon$

$\Rightarrow \quad \dfrac{x}{n} = q + \dfrac{r+\varepsilon}{n}$

$\therefore \left[\dfrac{x}{n}\right] = \left[q + \dfrac{r+\varepsilon}{n}\right]$

$= [q] = q \quad (\because q$ is an integer$)$

$\left.\begin{array}{l} 0 \le r \le n-1 \\ 0 \le \varepsilon < 1 \end{array}\right\} \Rightarrow \dfrac{r+\varepsilon}{n} < 1$

Hence,
$$\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right]$$

Definition: Let $n \in \mathbb{Z}$. If $2 \mid n$ then n is said to be even and otherwise n is said to be odd.

* If n is even, $n = 2k$ for some $k \in \mathbb{Z}$.
If n is odd, $n = 2k+1$ " " "

ex: Any integer n can be written in one of the following forms.
$3k$, $3k+1$, $3k+2$

This is because
$n = 3q + r$ for some $q, r \in \mathbb{Z}$
with $\underbrace{0 \le r < 3}$

$\therefore r = 0, 1$ or 2

Nothing special with 3.

We could say "any integer n can be written in one of the forms $4k$, $4k+1$, $4k+2$ and $4k+3$".

<u>ex</u>: Show that the square of any integer is of the form $4k$ or $4k+1$.
Let n be any integer.
Then,

$$n = 4k \text{ or}$$
$$n = 4k+1 \text{ or}$$
$$n = 4k+2 \text{ or}$$
$$n = 4k+3.$$

Then, $n^2 = 16k^2 = 4(4k^2) = 4\ell$ or
$n^2 = (4k+1)^2 = 4(4k^2+2k)+1 = 4\ell+1$ or
$n^2 = (4k+2)^2 = 4(4k^2+4k+1) = 4\ell$ or

$n^2 = (4k+3)^2 = 4(4k^2+6k+2)+1 = 4\ell+1$.

Hence the result.

<u>Definition</u>: Let $a, b \in \mathbb{Z}$ and not both a and b be zero (i.e., $a^2+b^2 \neq 0$). The greatest common divisor of a and b is the largest integer that divides both a and b.

We use the notation $\gcd(a,b)$ or simply (a,b) to denote the greatest common divisor of a and b.

Note that, if $d = \gcd(a,b)$, then

* $d \mid a$, $d \mid b$
* if $c \mid a$ and $c \mid b$ then $c \leq d$.

<u>ex:</u> $\gcd(8,12) = 4$
$\gcd(6,12) = 6$
$\gcd(4,9) = 1$

$\gcd(0,a) = a$ for any $a \neq 0$.

$\gcd(a,b) = \gcd(b,a)$
$\gcd(-12,9) = 3$
$\gcd(-20,-30) = 10$

<u>Definition:</u> Let $a, b \in \mathbb{Z}$, $a \neq 0$ and $b \neq 0$. a and b are said to be $\underbrace{\text{relatively prime}}_{=\text{coprime}}$ if $\gcd(a,b) = 1$.

<u>ex:</u> $\gcd(6,25) = 1$, so 6 and 25 are relatively prime