3.3 Greatest Common Divisors

Recall that, for $a, b \in \mathbb{Z}$, both nonzero,

$$\gcd(a,b) = \text{largest integer that divides both } a \text{ and } b$$

We also define $\gcd(0,0) = 0$.

* Note that $\gcd(a,b) = \gcd(|a|, |b|)$. Therefore, we can pay attention to the gcd of positive integers.

Theorem 3.6: Let $d = \gcd(a,b) > 0$. Then,

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Proof: Let $e = \gcd(a/d, b/d)$.
We show that $e = 1$.

We've, $e \mid \frac{a}{d}$ and $e \mid \frac{b}{d}$

$\Rightarrow \frac{a}{d} = ke$ and $\frac{b}{d} = \ell e$
$\Rightarrow a = k(ed)$ and $b = \ell(ed)$
$\Rightarrow ed \mid a$ and $ed \mid b$
$\Rightarrow ed \leq d$ ($\because$ any divisor of a and b should be $\leq$ largest divisor)
$\Rightarrow e \leq 1$ ($\because d > 0$)

But $e \geq 1$ (always), so $e = 1$
and the theorem follows.

<u>Corollary 3.6.1</u>: Let $a, b \in \mathbb{Z}$ with $a, b \neq 0$.
Then, $\frac{a}{b} = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$
with $\gcd(p, q) = 1$.

Proof: Let $d = \gcd(a, b)$.
Set $p = a/d$ and $q = b/d$.

Then, $p/q = a/b$ and, by Theorem 3.6,

$\gcd(p, q) = 1$.

<u>Theorem 3.7</u>: Let $a, b, c \in \mathbb{Z}$. Then
$\gcd(a + cb, b) = \gcd(a, b)$.

<u>Proof</u>: Let $d_1 = \gcd(a, b)$ and $d_2 = \gcd(a + cb, b)$.
We show that $d_1 \leq d_2$ and $d_2 \leq d_1$.

First,
$d_1 = \gcd(a, b) \Rightarrow d_1 \mid a$ and $d_1 \mid b$
$\Rightarrow d_1 \mid (a + cb) + d_1 \mid b$ (Theorem 1.9)
$\Rightarrow d_1 \leq d_2$ ($\because$ any divisor of $a + cb$ and b is less than or equal to their gcd)

Next,
$d_2 = \gcd(a + cb, b) \Rightarrow d_2 \mid a + cb$ and $d_2 \mid b$

$\Rightarrow d_2 \mid (a+cb-cb)$ and $d_2 \mid b$ (Theorem 1.9)

$\Rightarrow d_2 \mid a$ and $d_2 \mid b$

$\Rightarrow d_2 \leq d_1$ ($\because$ any divisor of a and b is less than or equal to their gcd.)

Hence $d_1 = d_2$ and the theorem follows

Theorem 3.8: Let $a, b \in \mathbb{Z}$ where not both a and b are zero. Then,

$$\gcd(a,b) = \min\{ma+nb : m, n \in \mathbb{Z},\ ma+nb>0\}$$

Ex: $\gcd(\underset{a}{9}, \underset{b}{21}) = 3 = \overset{m}{-2}(\underset{a}{9}) + \overset{n}{1}(\underset{b}{21})$

Proof: Let $S = \{ma+nb : m, n \in \mathbb{Z},\ ma+nb>0\}$

Then, S is nonempty. To see this, assume $a \neq 0$. Then, either $1a+0b$ or $(-1)a+0b$ should be positive.

By the well-ordering property, S has a least element.

Let it be d.
Then, $d = m_0 a + n_0 b$ for some $m_0, n_0 \in \mathbb{Z}$.

We show that $d = \gcd(a,b)$

First, we show that $d|a$.

By the division algorithm,

$$a = dq + r \text{ with } 0 \le r < d.$$

Then,

$$a = (m_0 a + n_0 b)q + r$$

$$\therefore \quad r = (1 - m_0 q)a + (-n_0 q)b$$

$\therefore$ r is of the form $ma + nb$.

Since $r < d$ and d is the minimum positive integer of the form $ma+nb$, it follows that $r > 0$ is not possible.

Hence $r = 0$.

$\therefore$ $a = dq$ and thus $d|a$.

Similarly, we can show that $d|b$.
It remains to show that d is the largest common divisor.

Let c be another common divisor of a and b. We show that $c \le d$.
If $c|a$ and $c|b$, then $c | m_0 a + n_0 b$.

$$\therefore \quad c|d$$

$\therefore$ $c \le d$ and the theorem follows.

* This theorem says that the greatest common divisor of two integers, not both zero, is a linear combination of the two integers. It further says that the gcd is the linear combination of a and b that gives the least positive integer.

Corollary 3.8.1 (Bezout's Theorem)

Let $a, b \in \mathbb{Z}$. Then, $\exists$ $m, n \in \mathbb{Z}$ such that

$$\gcd(a,b) = ma + nb$$

Proof: This is just a restatement of the above theorem, except that the case $a = b = 0$ is included.

Ex:

Corollary 3.8.2: The integers a and b are relatively prime if and only if there exist $m, n \in \mathbb{Z}$ s.t. $ma + nb = 1$.

Proof: If a and b are relatively prime, then, $\gcd(a,b)=1$ and hence $\exists$ $m, n \in \mathbb{Z}$ s.t. $ma+nb=1$ (by Corollary 3.8.1).

Conversely, if $ma+nb=1$ for some $m,n\in\mathbb{Z}$, and $d=\gcd(a,b)$, then $d \mid (ma+nb)$, so $d \mid (ma+nb)$, i.e., $d \mid 1$.
Hence, $d=1$.
$\therefore$ a and b are relatively prime.

(Note that $d \neq 0$ since not both a and b are zero when $ma+nb=1$ is given.)

Theorem 3.9: Let $a,b\in\mathbb{Z}$. Then, the set of all linear combinations of a and b is the set of all multiples of $\gcd(a,b)$.

Proof: Let $d=\gcd(a,b)$.
Then, since $d \mid a$ and $d \mid b$, for any $m,n\in\mathbb{Z}$, by Theorem 1.9, $d \mid (ma+nb)$.
$\therefore$ any linear combination is a multiple of d.
Conversely, we show that every multiple of d is a linear combination of a and b.
By Corollary 3.8.1, $\exists$ $m,n\in\mathbb{Z}$ s.t.

$$d = ma+nb.$$

Consider any multiple jd of d, where $j \in \mathbb{Z}$.
Then,

$$jd = (jm)a + (jn)b$$
$$= \text{a linear combination of } a \text{ and } b$$

$\therefore$ any multiple of $\gcd(a,b)$ is a linear combination of a and b.

Hence the theorem.

Ex: $a=12$, $b=10$. Then, $d = \gcd(12,10) = 2$.

$\therefore$ $12m + 10n = 2(6m+5n)$ gives all multiples of 2.

There is an equivalent way to define the gcd of two integers. It is given in the following theorem.

Theorem 3.10: Let $a, b \in \mathbb{Z}$, not both zero. Then $d \in \mathbb{Z}^+$ is a the gcd of a and b if and only if

(i) $d \mid a$ and $d \mid b$

(ii) $c \mid a$ and $c \mid b \Rightarrow c \mid d$ $(c \in \mathbb{Z})$

Proof: Exercise

Definition: Let $a_1, a_2, \cdots, a_n \in \mathbb{Z}$, not all zero. The gcd of these integers is the largest integer that is a divisor of all these integers. It is denoted by

$$\gcd(a_1, a_2, \cdots, a_n)$$

Following lemma gives a way to find the gcd of more than 2 integers.

Lemma 3.2:

$$\gcd(a_1, a_2, \cdots, a_{n-1}, a_n) = \gcd(a_1, a_2, \cdots, a_{n-2}, \gcd(a_{n-1}, a_n))$$

Ex: $\gcd(12, 15, 21) =$

$\gcd(18, 65, 10) =$

Definition: If $\gcd(a_1, a_2, \cdots, a_n) = 1$, then $a_1, a_2, \cdots, a_n$ are said to be mutually, relatively prime.

If $\gcd(a_i, a_j) = 1$ for all $i \neq j$, then they are said to be pairwise relatively prime.

Ex: