Greatest Common Divisor (GCD)

Theorem

$\forall\, a, b \in \mathbb{Z}$:

1). $D_a \cap D_b \neq \emptyset$, in fact: $1 \in D_a \cap D_b$

2). $a \neq 0$ or $b \neq 0 \implies D_a \cap D_b$ is finite

Proof

Assume $a, b \in \mathbb{Z}$

$1 \in D_a$ and $1 \in D_b$
$\therefore 1 \in D_a \cap D_b$ and $D_a \cap D_b \neq \emptyset$

AWLOG: $a \neq 0$
D_a is finite
$\therefore D_a \cap D_b$ is finite

Definition

Let $a, b \in Z$ and $a \neq 0$ or $b \neq 0$. To say that $d \in \mathbb{Z}$ is the *greatest common divisor* of a and b, denoted (a, b) or $\gcd(a, b)$, means:

1). $d \in D_a \cap D_b$

2). $\forall\, c \in D_a \cap D_b, c \leq d$

By convention, $(0, 0) = 0$.

Theorem

$$\forall\, a, b \in \mathbb{Z}, a \neq 0 \text{ or } b \neq 0 \implies (a, b) \in \mathbb{Z}+$$

Proof

Assume $a, b \in \mathbb{Z}$
AWLOG: $a \neq 0$
$1 \in D_a \cap D_b$
$(a, b) \geq 1$
$\therefore (a, b) \in \mathbb{Z}^+$

Theorem

$$\forall\, a, b \in \mathbb{Z}, (a, b) = (|a|\,, |b|)$$

Proof

Assume $a, b \in \mathbb{Z}$

Case 1: $a = b = 0$

$$|0| = 0$$
$$(0,0) = (|0|\,, |0|) = 0$$

Case 2: $a \neq 0$ or $b \neq 0$

$$D_a = D_{-a} = D_{|a|}$$
$$D_b = D_{-b} = D_{|b|}$$
$$D_a \cap D_b = D_{|a|} \cap D_{|b|}$$
$$\therefore (a,b) = (|a|\,, |b|)$$

Theorem

Let $a.b \in \mathbb{Z}, a \neq 0$ or $b \neq 0$. (a,b) is the least positive integer that is an integer linear combination of a and b:

$$(a,b) = \min\{ma + nb \in \mathbb{Z}^+ \mid m, n \in \mathbb{Z}\}$$

Proof

Let $d = \min\{ma + nb \in \mathbb{Z}^+ \mid m, n \in \mathbb{Z}\}$, which must exist because at least one of the following must be true:

$$\begin{aligned} 1a + 0b &> 0 \\ (-1)a + 0b &> 0 \\ 0a + 1b &> 0 \\ 0a + (-1)b &> 0 \end{aligned}$$

$\exists\, m, n \in \mathbb{Z}, d = ma + nb$
By the division algorithm, $\exists\, q, r \in \mathbb{Z}, a = qd + r$, where $0 \leq r < d$
$r = a - qd = a - q(ma + nb) = (1 - qm)a - (qn)b$
So r is also an integer linear combination of a and b
Thus, by the minimality of d, it must be the case that $r = 0$
$a = qd$
$d \mid a$
By similar argument, $d \mid b$

Now, assume $c \in \mathbb{Z}^+, c \mid a$ and $c \mid b$
$\forall\, m, n \in \mathbb{Z}, c \mid ma + nb$
So, $c \mid d$
Thus, $c \leq d$
$\therefore (a,b) = d$

Corollary: Bézout's Theorem

$$\forall\, a, b \in \mathbb{Z}, \exists\, m, n \in \mathbb{Z}, (a,b) = ma + nb$$

Proof

Assume $a, b \in \mathbb{Z}$

Case 1: $a = b = 0$

Assume $m, n \in \mathbb{Z}$
$(0, 0) = 0$
$m0 + n0 = 0 = (0, 0)$

Case 2: $a \neq 0$ or $b \neq 0$

$(a, b) = \min\{ma + nb \in \mathbb{Z}^+ \mid m, n \in \mathbb{Z}\}$
$\therefore \exists\, m, n \in \mathbb{Z}, (a, b) = ma + nb$

Given a and b, Euclid's algorithm can be used to find (a, b) and then reversed to find m and n.

Example

Let $a = 616$ and $b = 24$

$$\begin{aligned} 616 &= 25 \cdot 24 + 16 \\ 24 &= 1 \cdot 16 + 8 \\ 16 &= 2 \cdot 8 + 0 \end{aligned}$$

$$\begin{aligned} 8 &= 1 \cdot 24 - 1 \cdot 16 \\ &= 1 \cdot 24 - 1 \cdot (616 - 25 \cdot 24) \\ &= -1 \cdot 616 + 26 \cdot 24 \end{aligned}$$

$m = -1$ and $n = 26$

Theorem

$\forall\, a, b \in \mathbb{Z}$, the set of integer linear combinations of a and b is the same as the set of integer multiples of (a, b).

Proof

Assume $a, b \in \mathbb{Z}$
Let $d = (a, b)$
Let $L = \{ma + nb \mid m, n \in \mathbb{Z}\}$
Let $M = \{kd \mid k \in \mathbb{Z}\}$

Assume $\ell \in L$
$\exists\, m, n \in \mathbb{Z}, \ell = ma + nb$
$d \mid a$ and $d \mid b$
$d \mid ma + nb$
$d \mid \ell$
$\exists\, k \in \mathbb{Z}, kd = \ell$
$\therefore \ell \in M$

Assume $m \in M$
$\exists\, k \in \mathbb{Z}, kd = m$
$\exists\, r, s \in \mathbb{Z}, ra + sb = d$
$m = k(ra + sb) = (kr)a + (ks)b$
But, by closure, $kr, ks \in \mathbb{Z}$
$\therefore m \in L$

$\therefore L = M$

Theorem

Let $a, b \in \mathbb{Z}$ such that $a \neq 0$ or $b \neq 0$. $d = (a, b) \iff$

1). $d \mid a$ and $d \mid b$

2). $\forall\, c \in \mathbb{Z}, c \mid a$ and $c \mid b \implies c \mid d$

Proof

$\implies$ Assume $d = (a, b)$

By definition, $d \mid a$ and $d \mid b$
Assume $c \in \mathbb{Z}$
Assume $c \mid a$ and $c \mid b$
$\exists\, m, n \in \mathbb{Z}, ma + nb = d$
$c \mid ma + nb$
$\therefore c \mid d$

$\impliedby$ Assume the above two conditions hold.

$d \in D_a \cap D_b$
Let $c \in \mathbb{Z}, c \mid a$ and $c \mid b$
$c \mid d$
$c \leq d$
$\therefore d = (a, b)$

Theorem

$$\forall\, a, b, c \in \mathbb{Z}, (a + cb, b) = (a, b)$$

Proof

Assume $a, b, c \in \mathbb{Z}$

$\implies$ Assume $x \in D_{a+cb} \cap D_b$

$x \mid a + cb$ and $x \mid b$
$x \mid 1(a + cb) - cb$
$x \mid a$
$x \mid a$ and $x \mid b$
$\therefore x \in D_a \cap D_b$

$\impliedby$ Assume $x \in D_a \cap D_b$

$x \mid a$ and $x \mid b$
$x \mid 1a + cb$
$x \mid a + cb$ and $x \mid b$
$\therefore x \in D_{a+cb} \cap D_b$

So $D_{a+cb} \cap D_b = D_a \cap D_b$
$\therefore (a + cb, b) = (a, b)$

Theorem

Let $a, b \in \mathbb{Z}$ and $d = (a, b)$:

$$\forall\, c \in \mathbb{Z} - \{0\}, c \mid a \text{ and } c \mid b \implies (\frac{a}{c}, \frac{b}{c}) = \frac{d}{c}$$

Proof

Assume $c \in \mathbb{Z}, c \neq 0$
Assume $c \mid a$ and $c \mid b$

Case 1: $a = b = 0$

$(a, b) = (0, 0) = 0$
$0 = \frac{0}{c}$
$\therefore (\frac{0}{c}, \frac{0}{c}) = \frac{0}{c}$

Case 2: $a \neq 0$ or $b \neq 0$

Since $(a, b) = (|a|, |b|)$, AWLOG: $a, b \geq 0$
$c \mid d$, since $c \mid a$ and $c \mid b$
$\exists\, m, n \in \mathbb{Z}, ma + nb = d$
$\exists\, h, k, \ell \in \mathbb{Z}, a = hc, b = kc$, and $d = \ell c$
$m(hc) + n(kc) = \ell c$
$(mh + nk)c = \ell c$
$mh + nk = \ell$
Let $e = (h, k)$
$\exists r \in \mathbb{Z}, \ell = mh + nk = re$
$\exists s, t \in \mathbb{Z}, h = se$ and $k = te$
$mse + nte = re$
$msec + ntec = rec$
But $sec = hc = a$ and $tec = kc = b$ and $rec = \ell c = d$
So $ec \mid a$ and $ec \mid b$
So $ec \leq d$
So $ec \leq rec$
But $r \neq 0$, since $rec = d \neq 0$
So $r = 1$ and $\ell = e = (h, k)$
But $c \neq 0$, so $h = \frac{a}{c}, k = \frac{b}{c}$, and $\ell = \frac{d}{c}$
$\therefore (\frac{a}{c}, \frac{b}{c}) = \frac{d}{c}$