Greatest Common Divisor

Common Divisor

A positive integer ~~~~ that is a factor of two positive integer a and b is called common Divisor.

Ex:

	12	18
divisors	1, 2, 3, 4, 6, 12	1, 2, 3, 6, 9, 18
common divisor	1, 2, 3, 6	
greatest common divisor	6	

Greatest common divisor

The greatest common divisor (gcd) of 2 integers a and b is the largest positive integer that divides both a & b.

It is denoted by (a, b)

Ex: $(12, 18) = 6$

$(11, 19) = 1$

$(-15, 25) = 5$

* Why always the gcd of two numbers is positive?

Because $(a, -b) = (-a, b) = (-a, -b)$
$= (a, b)$

A Symbolic Definition of gcd

A positive integer d is the gcd of two positive integers a and b if

- $d \mid a$ & $d \mid b$;
- if $d' \mid a$ & $d' \mid b$, then $d' \leq d$, where d' is a also a positive integer.

Thus, $(a, b) = d$ is satisfied:

- d must be a common factor of a & b.
- d must be largest common factor of a & b or $d \geq d'$.

Relatively Prime Integers

Two positive integers a and b are relatively prime if their gcd is 1

ie $(a, b) = 1$.

Ex: $(11, 24) = 1$
$(6, 35) = 1$.

Not relatively prime eg: $(12, 18) = 6$
$(3, 0) = 3$

Therom

Let $(a, b) = d$, then

To prove that: 1) $(a/d, b/d) = 1$

2) $(a, a-b) = d$.

Proof: 1

Let $d' = (a/d, b/d)$

To show that: $d' = 1$

Since d' is common factor of a/d & b/d

$a/d = l d'$ & $b/d = m d'$ for some integer l & m.

Then, $\frac{a}{d} = l d'$ & $\frac{b}{d} = m d'$

$a = l d d'$ & $b = m d d'$

So dd' is a common divisor of both a & b

$\therefore$ By definition $dd' \leq d$.

$\Rightarrow d' \leq 1$

d' is a positive integer such that $d' \leq 1$

So $d' = 1$

Proof: 2

Let $d' = (a, a-b)$

To show that: $d = d'$

To prove: $d \leq d'$ & $d' \leq d$

~~let~~ $(a,b)=d$, ~~d~~ and let $(a, a-b) = d'$

Since d is the common divisor of a and b

$a = md$ & $b = nd$

$a-b = md - nd$

$a-b = (m-n)d$

Thus d/a and $d \mid (a-b)$

$\Rightarrow d = (a, a-b)$

$\therefore$ d is a common divisor of a & $a-b$

$d \leq d'$ — ①

To show that $d' \leq d$

Since d' is a common factor of a & $a-b$,
$a = md'$ & $a-b = nd'$ for some integer m & n.

Then $a-(a-b) = md' - nd'$
$a-(a-b) = (m-n)d' \Rightarrow b = (m-n)d'$

Thus $d' \mid b$ & ~~$d' \mid (a-b)$~~ $d' \mid a$, Since d' is the common divisor ~~$d' \leq d$~~ of a and b

$d' \leq d$ — ②

From ① & ②, we get

$d = d'$

Hence proved.

Linear Combination

It is the sum of multiples of a and b, that is sum of the form $ma + nb$, where m & n are integers.

Ex: i) $2 \cdot 3 + 5 \cdot 7$ is a linear combination of 3 & 7

ii) $1 \cdot 3 + 4 \cdot 7$ is a linear combination of 3 & 7.

Theorm (Euler theorm)

The gcd of positive integers a & b is a linear combination of a and b.

$[d = (a, b), \quad d = ma + nb]$

Proof:

Let S be set of all positive linear combinations of a & b; $S = \{ma + nb \mid ma + nb > 0, m, n \in \mathbb{Z}\}$

To show: S is non empty, ie S has a least element.

Since $a > 0$, $a = 1 \cdot a + 0 \cdot b \in S$

So, S is non empty.

By well ordering principle, S has a least positive element d.

To show: $d = (a, b)$

Since $d \in S$, $d = ma + nb$ for some int m & n

(1) First we show that $d \mid a$ & $d \mid b$;

By the division algorithm, there exist integers q & r such that $a = dq + r$ where $0 \le r < d$

Substituting for d

$$a = dq + r$$

$$r = a - dq$$

$$= a - (\alpha a + \beta b) q$$

$$= (1 - \alpha q) a + (-\beta q) b$$

This shows r is a linear combination of a & b.

If $r > 0$, then $r \in S$.

Since $r < d$, r is less than the smallest element in S. (which is contradiction)

So, $r = 0$, thus $a = dq$ [$\because r = 0$ is substituted in $a = dq + r$)

$\Rightarrow d \mid a$

lly, $d \mid b$

$\therefore$ d is common divisor of a & b.

2 To show : $d' \le d$

By a theorm,

Let a, b, c, m & n be any int, Then

1. If $a \mid b$ & $b \mid c$, then $a \mid c$ (transitive property)
2. If $a \mid b$ & $a \mid c$, then $a \mid (\alpha b + \beta c)$
3. If $a \mid b$, then $a \mid b$

By the above theorm we say $d' \mid d$.

So $d' \le d$

By 1 & 2, we get

$$d = (a, b)$$

Hence proved.