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.

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

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 $a = dq + r$)

$\Rightarrow d | a$

lly, $d | b$

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

By the above theorm we say $d' | d$.

So $d' \le d$

By (1) & (2), we get

$$d = (a, b)$$

Hence proved.