

Theorem: (GCD And Linear Combination) Let $a, b \in \mathbb{Z}$, not both zero. Then there exist two integers s, t such that

$$\rightarrow (a:b) = sa + tb$$

Proof:

Preview from Notesale.co.uk
Page 6 of 10

$$r_{l-2} = k_l r_{l-1} + r_l \Rightarrow r_l = r_{l-2} - k_l r_{l-1}$$

$$\begin{aligned} r_{l-3} &= k_{l-1} r_{l-2} + \underline{r_{l-1}} \Rightarrow r_l = r_{l-2} - k_l (r_{l-3} - k_{l-1} r_{l-2}) \\ &= (1 + k_l k_{l-1}) r_{l-2} - k_l r_{l-3} \end{aligned}$$