Euclidean Algorithm

Theorem: Let a, b be two positive number and r be its remainder, if a is divided by b then.

$(a, b) = (b, r)$

~~Proof~~: Let $d = (a, b)$ and $d' = (b, r)$

To Prove: $d = d'$

① $d \mid d'$

② $d' \mid d$.

Proof:

① $d \mid d'$

$d = (a, b)$

By division algorithm:

$a = bq + r$ (for some q)

As $d = (a, b)$

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

$d \mid a$ and $d \mid bq$.

$d \mid a - bq$ (linear combination)

$d \mid r$.

As $d \mid r$ and $d \mid b$.

$d \mid (b, r)$

$d \mid d'$

② $d' \mid d$.

As $d' = (b, r)$

$d' \mid b$ and $d' \mid r$.

$d' \mid bq$ and $d' \mid r$.

$d' \mid bq + r$.

$d' \mid a$

As $d' \mid a$ and $d' \mid b \Leftrightarrow d' \mid (a, b)$

$d' \mid d$

$\therefore d = d'$