Important Proof (Thm 3.1.17) ☆ This proof is the basis of the ⇒Euclidian Algorithm⇐

$$a = qb + r \Rightarrow \gcd(a,b) = \gcd(b,r)$$

all $\in \mathbb{Z}$

Let $d = \gcd(a,b)$ WTS $d = \gcd(b,r)$

Main Idea: We know #1✓ and #2✓ hold for $d = \gcd(a,b)$. Using that, we WTS #1✓ and #2✓ hold for $d = \gcd(b,r)$.

✱ Proof of #1✓: WTS $d \mid b$ and $d \mid r$

$d = \gcd(a,b)$

$\Rightarrow [\, d \mid a \wedge d \mid b \,]$ using #1✓ from $d = \gcd(a,b)$

$\Rightarrow a = sd \wedge b = td$

$a = qb + r$

$\Rightarrow r = a - qb$

$\Rightarrow r = sd - q(td)$

$\Rightarrow r = (s - qt)d$

$\Rightarrow d \mid r$

✱ Proof of #2✓: WTS $(d' \mid b \wedge d' \mid r) \Rightarrow (d' \mid d)$

Assume $d' \mid b \wedge d' \mid r$

$\Rightarrow b = ud' \wedge r = vd'$

$a = qb + r$

$\Rightarrow a = q(ud') + (vd')$

$\Rightarrow a = (qu + v)d'$

$\Rightarrow d' \mid a$

Now we know $d' \mid b \wedge d' \mid a$

$d = \gcd(a,b)$, so $[\,(d' \mid b \wedge d' a) \Rightarrow (d' \mid d)\,]$ using #2✓ from $d = \gcd(a,b)$

So $d' \mid d$

Thus $d = \gcd(b,r)$ ■