Hw 2

Tuesday, 24 September 2024 11:37 PM

$a = bq + r$

let $x = gcd(a,b)$

$\Rightarrow x \mid (a + b)$

$\Rightarrow x \mid (bq + r + b)$

$\Rightarrow x \mid (b(q+1) + r)$

$\Rightarrow x \mid r$ — ①

* q is integer

from equation $a = bq + r$

$\Rightarrow r < b < a$ — ②

From ① and ②

If exist $y = gcd(b,r) > x = gcd(a,b)$

$\Rightarrow y \mid (b + r)$

$\Rightarrow y \mid (b + a - bq)$

$\Rightarrow y \mid (b(1-q) + a)$

$\Rightarrow gcd(a,b) = y$

③

∴ From ③ we know if exist $gcd(b,r) = y$

and $y > x$, $y \mid (b(1-q) + a)$

$gcd(a,b)$ will become y, and

from ② we know $r < b < a$, so

if exist $gcd(b,r)$ will also

same as $gcd(a,b)$