GCD

Euclid's Algorithm

$n \quad m$

$(54, 24)$

$\downarrow$

$(24, 6)$

$\downarrow$

$(\boxed{6}, 0)$

$(n, m) \quad n \geq m$

$\downarrow$

$(m, n \text{ rem } m)$

$\gcd = 6$

$$
\begin{tikzcd}
(93,39) \arrow[d] & & \\
(39,15) \arrow[d] & & \\
(15,9) \arrow[r] & (9,6) \arrow[r] & (6,3) \arrow[d] \\
& & (3,0)
\end{tikzcd}
$$

T. Euclid's algorithm is correct ✓

Lemma $\underbrace{(n, m)}_{g} = \underbrace{(m, \overbrace{n \text{ rem } m}^{r})}_{g'}$ $m \neq 0$, $n \geq m$

Proof We are going to write a direct proof.

$g = (n,m)$ what does this mean?.

$g \mid n$, $g \mid m$, (for all) g_1, s.t $g_1 \mid n$ and $g_1 \mid m$, we have $g \geq g_1$

g divides n evenly

Universal quantification

$g' = (m, r)$ Remember $r = n$ rem m

$g' \mid m$, $g' \mid r$ $\forall g_1'$ s.t

$g_1' \mid m$ and $g_1' \mid r$

$g' \geq g_1'$

My goal is to show

$g = g'$

I will show $g \geq g'$ and $g' \geq g$

Let's Prove

$g \geq g'$, To apply inequality in gcd, I have to show $g' | n$ and $\underbrace{g' | m}$ ✓ $[g' = (\underset{\cdot}{m}, \underset{\cdot}{r})]$

I have to show $g' | n$.

$n = q \cdot \underline{m} + r \Rightarrow$

$g' | qm, g' | r \Rightarrow g' | n$ | $g \geq g'$

$g' \geq g$. $g \mid r$ and $g \mid r$

$r = n - qm$

$g \mid n$ and $g \mid m$.

$\Downarrow$

$g \mid qm$

So $g \mid r$ $g' \geq g$.

How to Prove Euclid's algo is correct from this lemma.

$$\boxed{(n, m)} \stackrel{=}{\longrightarrow} (m, r) \stackrel{=}{\longrightarrow} (r, m \text{ rem } r)$$

$$\downarrow \quad \parallel$$

$$(m \text{ rem } r,\ r \text{ rem } (m \text{ rem } r))$$

$$\vdots$$

$$\parallel$$

Rely on correctness here $\longrightarrow$ $\underline{(k, 0)}$

Proof by Induction

$1+2+\dots+n = \frac{n\cdot(n+1)}{2}$

What is the induction variable?
# of steps.

if # rem. steps $= 0$, i/p is $(k, 0)$
and algo. is correct.
o/w we have (n, m) where $m > 0$
and algo is correct due to lem

Why is Euclid's algo. fast?

Trivial $(n,m) \overset{n \geq m}{\sim} \min(n,m) = m$

For all (n,m), time taken is "Small".

Binary Search.

On i/p size n
Bin Search takes
$\sim \log(n)$ steps.

$$\underbrace{n \rightarrow n/2 \rightarrow n/4 \cdots 1}_{\sim \log_2(n)}$$

$$n \to 0.99n \to 0.99^2 n$$

$$\downarrow$$

$$\vdots$$

$$1$$

It's worse than BinSearch.

Independent of n.

$$\sim \log_{1/0.99} n = \frac{\log_2 n}{\log_2 1/0.99} = (\log_2 n) \cdot \frac{1}{\log_2 1/0.99}$$