GCD Characterization Theorem GCD CT: If $d$ is positive common divisor of the integers $a$ and $b$, and $\exists\ x,y \in \mathbb{Z}$ s.t. $ax+by=d$, then $d=\gcd(a,b)$

ex. $a,b,c \in \mathbb{Z}$. Prove if $\gcd(a,b,c)=1$, then $\gcd(a,c), \gcd(b,c)=1$.

By the EEA, $\exists\ x,y \in \mathbb{Z}$ s.t. $ab(x)+c(y)=1$.

Since $1|a$ and $1|c$ and $a(bx)+c(y)=1$, by GCD CT.
where $bx, y \in \mathbb{Z}$

thus, $\gcd(a,c)=1$

Since $1|b$ and $1|c$ and $b(ax)+c(y)=1$
where $ax, y \in \mathbb{Z}$

ex. 2. State converse and prove/disprove. If $\gcd(a,c)=\gcd(b,c)=1$ then $\gcd(a,b,c)=1$

~~gcd(17, 59) = gcd(34~~ true. If $a,c$ are relatively prime if $b,c$ are relatively prime then $a,b,c$ are pairwise prime. $\therefore$ true.

Proof: If $\gcd(a,c)=1$ then by EEA there exist $x,y \in \mathbb{Z}$ s.t. $ax+cy=1$. Likewise, if $\gcd(b,c)=1$ then by EEA $\exists\ k,m \in \mathbb{Z}$ s.t. $bk+cm=1$. Multiplying these gives: $(ax+cy)(bk+cm)=1$

$axbk+axcm+cybk+c^2ym=1$

Since $1|ab$ and $1|c$ and $ab(\quad)+c(\quad)=1$, then by GCD CT $\gcd(a,b,c)=1$

$ab(xk)+c(axm+ybk+cym)=1$ where $xk, axm+ybk+cym \in \mathbb{Z}$

Observation: EEA is useful with gcd in the hypothesis, GCD CT is useful with GCD in the conclusion

Proposition: (GCD of One (GCD OO))

Let $a,b \in \mathbb{Z}$. Then $\gcd(a,b)=1$ iff $\exists x,y \in \mathbb{Z}$ with $ax+by=1$

Proof of GCD OO

1. ($\Rightarrow$) Suppose $GCD(a,b)=1$. Then by EEA $\exists x,y \in \mathbb{Z}$ s.t. $ax+by=d$ $=1$.

($\Leftarrow$) Suppose $\exists\, x,y \in \mathbb{Z}$ s.t. $ax+by=1$
Since $1|a$ and $1|b$, by GCDCT, $gcd(a,b)=1$. ■

Division by the GCD (DB GCD)

Let $a,b \in \mathbb{Z}$. If $gcd(a,b)=d$ and $d \neq 0$, then $gcd(\frac{a}{d}, \frac{b}{d}) = 1$

ex. Let $a=91$ and $b=70$. Then $gcd(a,b)=7$ and by DBGCD, $gcd(\frac{a}{d}, \frac{b}{d})$ $= gcd(\frac{91}{7}, \frac{70}{7}) = gcd(13,10)=1$

Pf: Suppose $gcd(a,b)=d \neq 0$. Then by EEA, $\exists x,y \in \mathbb{Z}$ s.t. $ax+by=d$.
Dividing by $d$ gives $\frac{a}{d}x + \frac{b}{d}y = 1$

By GCDOO, since $\frac{a}{d}(x) + \frac{b}{d}(y) = 1$, where $x,y \in \mathbb{Z}$
thus $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

Def'n: Coprime : Two integers a and c are coprime if $gcd(a,c)=1$

Proposition: Coprimeness and Divisibility (CAD)

If $a,b,c \in \mathbb{Z}$ and $c|ab$ and $gcd(a,c)=1$ then $c|b$.

ex. (CAD). Let $a=14$, $b=30$, $c=15$. Then $c|ab$ since $15|420$ and $gcd(a,c)=1$ $= gcd(14,15)=1$. Thus by CAD, $c|b$ or $15|30$.

Proof of CAD: Suppose $gcd(a,c)=1$ and $c|ab$. Since $gcd(a,c)=1$ then by EEA $\exists x,y \in \mathbb{Z}$ s.t. $ax+cy=1$.
Multiplying by $b$ gives $abx+cby=b$
Since $c|ab$, $\exists\, k \in \mathbb{Z}$ s.t. $ab=ck$. Substituting into * gives

$$ckx + cby = b$$

$c(kx+by) = b$ where $(kx+by) \in \mathbb{Z}$ $\therefore c \mid b$ $\blacksquare$