1. EEA
2. Coprimes

GCD Char: If $d|a, d|b$ and $ax+by=d$ has an int sol^n, then $d=\gcd(a,b)$.

EEA: If $d=\gcd(a,b)$, then $ax+by=d$ has an int sol^n.

They're converses.

"Magic Box" Method: Finds gcd and (x,y) at the same time.

Example: $\gcd(4141, 3649)$

x_i	y_i	r_i
1	0	4141
0	1	3649
1	-1	492
-7	8	205
15	-17	82
-37	42	41
		0 stop

Maintain: $4141x_i + 3649y_i = r_i$

$\overset{row1}{4141} = 1 \cdot \overset{row2}{3649} + \boxed{492}$ row$_1$ − row$_2$

$3649 = 7 \cdot 492 + 205$ row$_2$ − 7 · R_3

$492 = 2 \cdot 205 + 82$ row$_3$ − 2 · R_4

$205 = 2 \cdot 82 + 41$ row$_4$ − 2 · R_5

$82 = 2 \cdot 41 + 0$

So $\gcd(4147, 3649) = 41$

$4141 \cdot (-37) + 3649 \cdot (42) = 41$

Coprimes

Definition: For $a, b \in \mathbb{Z}$, a,b are <u>coprime</u> if $\gcd(a,b)=1$.

15, 22 are coprime.

Proposition: (Coprimeness and divisibility, CAD): Let $a,b,c \in \mathbb{Z}$. If $c|ab$ and a,c are coprime, then $c|b$.

[$6 | 3 \cdot 2$ $\gcd(6,3) \neq 1$ $6 | 7 \cdot 6$ $\gcd(6,7) = 1$, so $6 | 6$]

Proof: Since $\gcd(a,c)=1$, there exist $x, y \in \mathbb{Z}$ such that $ax+cy=1$ by EEA. Multiply both sides by b to get $\underline{bax} + \underline{bcy} = b$. By assumption, $c | ab$, also $c | c$. By div. of int comb, $c | (bax + bcy)$. So $c | b$.

Corollary (Primes and Divisibility, PAD, Euclid's Lemma)

Let $a, b \in \mathbb{Z}$. If p is prime and $p | ab$, then $p | a$ or $p | b$.

Proof: If $p | a$, then we are done. Assume $p \nmid a$. Since the only positive divisors of p are 1 and p, and $p \nmid a$, $\gcd(p,a)=1$. By CAD, since $p | ab$ and $\gcd(p,a)=1$, $p | b$.

Proposition (Division by GCD, DB GCD): Let $a, b \in \mathbb{Z}$. If $d = \gcd(a,b)$ and $d > 0$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

[$a=12$ $b=15$. $d=3$. $\gcd\left(\frac{12}{3}, \frac{15}{3}\right) = \gcd(4,5) = 1$]

Proof: Since $d = \gcd(a,b)$, by EEA, there ~~exist~~ $x, y \in \mathbb{Z}$ such that $ax + by = d$. Since $d > 0$, we can divide both sides by d to get $\frac{a}{d}x + \frac{b}{d}y = 1$. Since $d | a$ and $d | b$, $\frac{a}{d}, \frac{b}{d}$ are integers. Since $1 | \frac{a}{d}$, $1 | \frac{b}{d}$ and $\frac{a}{d}x + \frac{b}{d}y = 1$ has an int sol^n, by GCD char, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.