1. GCD Characterization
2. Extended Eudidean Algebra

$d = \gcd(a,b)$

① $d \mid a$

② $d \mid b$

③ If $c \mid a$ and $c \mid b$, then $c \leq d$.

Proposition (GCD Characterization): For $a, b \in \mathbb{Z}$ not both 0, if d is a positive divisor of a, b and $ax+by=d$ has an integer for (x,y), then $d = \gcd(a,b)$.

ex. $a=12$ $b=15$

$12x+15y=\square$ If this has int solution, is $\square$ the gcd? Only if $\square \mid 12$ and $\square \mid 15$.

$12x+15y=12$ $(1,0)$ is a sol^n, but $12 \neq \gcd$

$3 \mid 12$, $3 \mid 15$, $(-1,1)$ is an int solution

$\gcd(12,15)=3$.

$12x+15y=1$ $1 \neq \gcd$, conc is false $\Rightarrow$ hyp. is false.

$1 \mid 12$, $1 \mid 15$, so no sol^n.

Proof: By assumption, $d \mid a$ and $d \mid b$. Let $c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$. Suppose (x_0, y_0) is an int solution to $ax+by=d$.

By div. of int. comb, $c \mid (ax_0 + by_0)$, so $c \mid d$. using bounds by div, $|c| \leq |d| = d$, since $d > 0$, so $c \leq d$, and $d = \gcd(a,b)$

The integers (x, y) serves as a certificate that d is the gcd of a, b. To verify $d = \gcd(a,b)$:

$d \mid a$ ✓ $\quad d \mid b$ ✓ $\quad ax + by = d$ ✓

Extended Euclidean Algorithm (EEA)

Find x, y such that $ax + by = \gcd(a,b)$

Example: $\gcd(744, 264)$
$= \gcd(264, 216)$
$= \gcd(216, 48)$
$= \gcd(48, 24)$
$= 24$

$744 = 2 \cdot 264 + 216$ ①
$264 = 1 \cdot 216 + 48$ ②
$216 = 4 \cdot 48 + 24$ ③

Back substitution ...

$24 = 216 - 4 \cdot 48$ ③
$= 216 - 4(264 - 1 \cdot 216)$
$= 5 \cdot 216 - 4 \cdot 264$ ②
$= 5(744 - 2 \cdot 264) - 4 \cdot 264$
$= 5 \cdot 744 - 14 \cdot 264$ ①

Proposition (EEA): Let a, b $\mathbb{Z}$, If $d = \gcd(a,b)$, then $ax+by=d$ has an int solution.

(Only prove for $a, b \in \mathbb{N}$)

Let $E(a,b)$ be the # of steps in the EA when finding $\gcd(a,b)$.

Proof: Induction on $E(a,b)$.

If $a=b$, then $\gcd(a,b)=a$. So $a\cdot 1+b\cdot 0=a$.

without loss of generality, assume $a>b$.

Base Case: If $E(a,b)=1$, then $b|a$, and $\gcd(a,b)=b$. So $a\cdot 0+b\cdot 1=b$.

Ind. Hyp.: Assume result holds when $E(a,b)=k$ for some $k \in \mathbb{N}$.

Ind. Step: Suppose $E(a,b)=k+1$

In the first step of E.A, we find $a=qb+r$, and $\gcd(a,b)=\gcd(b,r)$ We need k steps to find $\gcd(b,r)$, so $E(b,r)=k$. By ind. hyp, there exists $x_0, y_0 \in \mathbb{Z}$ such that $bx_0+ry_0=\gcd(b,r)=\gcd(a,b)=d$.

Replace $r=a-qb$, $d=bx_0+(a-qb)y_0=ay_0+b(x_0-qy_0)$.

So $ax+by=d$ has an int solution. (y_0, x_0-qy_0)