GCD

Definition: Let $a, b \in \mathbb{Z}$, not both 0. The <u>greatest common divisor</u> of a, b denoted by $\gcd(a,b)$ is the integer d such that

① $d \mid a$ } "common divisor"
② $d \mid b$ }
③ For all $c \in \mathbb{Z}$, if $c \mid a$ and $c \mid b$, then $c \leq d$

Examples: $\gcd(35, 49) = 7$ 7135 7149 try all $\mathbb{Z}$
$\gcd(9141, 3647) = 41$ $\gcd(-35, -49) = 7$ $\gcd(0, a) = |a|$
$\gcd(0,0) = ?$ Define $\gcd(0,0) = 0$

Proposition (GCD with remainders): If $a, b, q, r \in \mathbb{Z}$ where $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$
"Euclidean Algorithm"

Strategy of proof: Let $d = \gcd(a,b)$. Prove $d = \gcd(b,r)$. Need
① $d \mid b$ ② $d \mid r$ ③ if $c \mid b$ and $c \mid r$, then $c \leq d$

Proof: Let $d = \gcd(a,b)$. By definition, $d \mid b$.
We know $r = a - qb$. Since $d \mid a$ and $d \mid b$, by div of int comb $d \mid (a - qb)$, so $d \mid r$.
Let $c \in \mathbb{Z}$ such that $c \mid b$ and $c \mid r$. Since $c \mid b$ and $c \mid r$, by div of int comb, $c \mid (qb + r)$ so $c \mid a$. Since c is a common divisor of a, b and $d = \gcd(a,b)$, $c \leq d$. So $d = \gcd(b,r)$, so $\gcd(a,b) = \gcd(b,r)$ □.

Running time of Euclidean Algorithm

Suppose (a_N, b_N) is the smallest pair of positive integers that terminates with N steps in E.C. Assume $a_N > b_N$.
$N = 1$ step $(a_1, b_1) = (2,1)$
$(a_N, b_N) \Rightarrow a_N = q b_N + r \Rightarrow \gcd(a_N, b_N) = \gcd(b_N, r)$
Minimize a_N: $q = 1$
(b_N, r) requires $N-1$ steps in E.C. $\Rightarrow$ Minimize $(b_N, r) = (a_{N-1}, b_{N-1})$

So $a_N = a_{N-1} + b_{N-1}$ (by induction)
$= a_{N-1} + a_{N-2}$

$a_0 = 1$
$a_1 = 2$
$a_2 = 3$
$a_3 = 5$
...

Worst cases for E.C are (f_{n+2}, f_{n+1})

$a_N = f_{N+2}$
$b_N = a_{N-1}$
$= f_{N+1}$

Input: (a,b), $a>b$. Suppose E.C. runs N steps. Then $a \geq f_{n+2}$, $b \geq f_{N+1}$

Fact: $f_{N+1} \geq \varphi^{N-1}$ where $\varphi = \frac{1+\sqrt{5}}{2}$

So $b \geq \varphi^{N-1}$

$\log b \geq \log \varphi^{N-1}$

$\geq (N-1)\log\varphi$ $\quad \log\varphi > \frac{1}{5}$

$> \frac{1}{5}(N-1)$

$5\log b > N-1$

$5(\log b + 1) > N$

$\therefore$ Running time $\leq 5(\#\text{ digits of } b)$

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 $d=\gcd(a,b)$

Proof: By assumption, $d|a$ and $d|b$. Let $c \in \mathbb{Z}$ such that $c|a$ and $c|b$. Suppose (x_0,y_0) is an int soln to $ax+by=d$. Then $ax_0+by_0=d$. By div of int comb, $c|ax_0+by_0$, so $c|d$. Using bounds by div, $|c| \leq |d| = d$ since $d>0$. So $c \leq d$, and $d=\gcd(a,b)$ □

The integers (x,y) serve as a certificate that d is the gcd of a,b.
To verify $d=\gcd(a,b)$: ① $d|a$ ② $d|b$ ③ $ax+by=d$

<u>Extended Euclidean Algorithm (EEA)</u>

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

Ex: Find x,y such that $744x+264y=\gcd(744,264)$

$\gcd(744,264)$ $\quad 744 = 2\cdot 264 + 216$ ①

$= \gcd(264,216)$ $\quad 264 = 1\cdot 216 + 48$ ②

$= \gcd(216,48)$ $\quad 216 = 4\cdot 48 + 24$ ③

$= \gcd(48,24)$

$= 24$

Back substitution

$24 = 216 - 4\cdot 48$

$= 216 - 4(264 - 1\cdot 216) = 5\cdot 216 - 4\cdot 264$

$= 5(744 - 2\cdot 264) - 4\cdot 264 = 5\cdot 744 - 14\cdot 264$

$x=5$ $\quad y=-14$

Proposition (EEA): Let $a,b \in \mathbb{Z}$. If $d=\gcd(a,b)$, then $ax+by=d$ has an integer 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 1st 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 soln (y_0, x_0-qy_0) □

Note: The GCD char and EEA are converses of each other.

"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 $\to R_1-R_2$
-7	8	205 $\to R_2-7R_3$
15	-17	82 $\to R_3-2R_4$
-37	42	41 $\to R_4-2R_5$
		0 $\to$ stop

Maintain: $4141x_i+3649y_i=r_i$

So $\gcd(4141,3649)=41$

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

Coprimes

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

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

Proof: Since $\gcd(a,c)=1$, there exists $x,y\in\mathbb{Z}$ such that $ax+cy=1$ by EEA. Multiply both sides by b to get $bax+bcy=b$. By assumption, $c|ab$ and $c|c$. 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 divisor 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): Let $a, b \in \mathbb{Z}$. If $d=\gcd(a,b)$ and $b>0$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right)=1$.

Proof: Since $d=\gcd(a,b)$, by EEA, there exists $x, y \in \mathbb{Z}$ 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 int solution, by GCD char, $\gcd\left(\frac{a}{d}, \frac{b}{d}\right)=1$ □

Division Algorithm

If a & b are integers and $b>0$, then there exists unique integers q and r such that

$$a=qb+r \text{ where } 0 \leq r < b$$