Section 3.3: GCDs I

Thm: Let $a, b, n \in \mathbb{Z}$. Then $(a,b) = (a+nb, b)$

Ex: $(1000, 248) = (1000-248, 248)$

$= (752, 248)$

$= (504, 248)$

$= (256, 248)$

$= (8, 248)$

$= \cdots = (8, 0) = 8$

Pf: Goal: Show (a,b) and $(a+nb, b)$ have the same divisors

Suppose $d \mid (a,b)$

Then $d \mid a$ and $d \mid b$

$\rightarrow d \mid a+nb$
$\rightarrow d \mid b$
$\rightarrow d \mid (a+nb, b)$

(1) Every divisor of (a,b) is a divisor of $(a+nb, b)$

Now suppose $f \mid (a+nb, b)$

So $f \mid b$, $f \mid a+nb$

Since $f \mid a+nb$, $\exists g$: $fg = a+nb$

Since $f \mid b$: $\exists h$: $fh = b$

$a = fg - nb = fg - nfh = f(g - nh)$

$\left.\begin{array}{l} \to f \mid a \\ f \mid b \end{array}\right\} \to f \mid (a, b)$

(2) Every divison of $(a+nb, b)$ is a divison of (a, b)

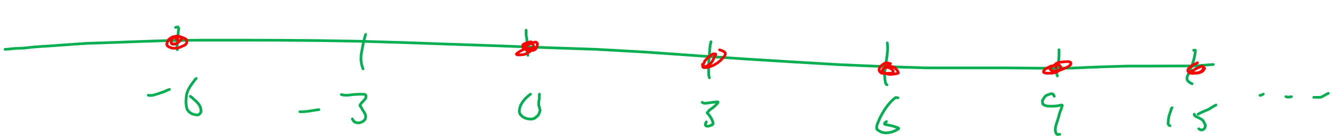
By (1) and (2) (a, b) and $(a+nb, b)$ have the same divisors; since both are positive, theyre the same number.

Before: if $d \mid a$, $d \mid b$, then $d \mid ma+nb$

So $(a, b) \mid ma + nb$

Ex: $a = 9$, $b = 15$

$(9, 15) = 3$ and $3 \mid 9n + 15m$



Note: $n=-3$, $m=2$: $9(-3)+15(2)=3$

$$9(-3)+15(2) \mid (9,15)$$

Goal: Show that $(a,b)=am+bn$ for some m and n is possible

Thm: If $a,b \in \mathbb{N}$, not both 0, then $\exists\, m,n \in \mathbb{Z}$ s.t. $am+bn=(a,b)$

Pf: Let $S=\{am+bn>0 \cdot m,n \in \mathbb{Z}\}$

$S \subseteq \mathbb{N}$ because all elts. of S are nonnegative ✓

$S \neq \emptyset$ because $a,b \geq 0$, one is nonzero (say $a \neq 0$), so $a \cdot 1 + b \cdot 0 \in S$

Therefore, S has a least element, say $d = ma + nb$

Goal: Show $d = (a, b)$

Subgoal: show $d \mid a$

swap a, b

Write $a = dq + r$ for $0 \le r < d$

$r = a - dq = a - (ma + nb)q$

$= (1 - mq)a - (nq)b$

So r is a lin. comb. of a, b

Since $0 \le r < d$ and r is a lin. comb. of a, b and d is the least pos. lin. comb. of a, b, r must be 0.

$a = dq \rightarrow d \mid a$

By symmetry, $d \mid b$

So $d \mid (a, b)$

Also $(a, b) \mid ma + nb = d$

Therefore $(a, b) = d = ma + nb$

Ex: Show that for $k \in \mathbb{Z}_{\geq 0}$

$3k + 2$ and $5k + 3$ are relatively

prime ($\gcd = 1$)

Soln 1: $(5k+3, 3k+2)$

$= (5k+3-(3k+2), 3k+2)$

$= (2k+1, 3k+2)$

$= (2k+1, 3k+2-(2k+1))$

$= (2k+1, k+1)$

$$= (2k+1-(k+1),\ k+1)$$

$$= (k,\ k+1)$$

$$= (k,\ k+1-k) = (k, 1) = 1$$

Soln 2:

$$\begin{array}{r} 5(3k+2) \\ -\ 3(5k+3) \\ \hline 1 \end{array}$$

Note $2 = 10(3k+2) - 6(5k+3)$

but $2 \neq (3k+2,\ 5k+3)$