MATH 407
2/16/18

Greatest Common Divisors (GCD):

* $a, b \in \mathbb{Z}$, $|a|+|b| \neq 0$
  $d = \gcd(a,b)$, $d \in \mathbb{Z}^+$

  i) $d|a$, $d|b$
  ii) if $c|a$, $c|b$ then $c|d$

* $\gcd(0,0)$ is undefined

* $a \neq 0$, $\gcd(a,0) = |a|$

<u>Th. 1.1.6</u>: Let $a, b \in \mathbb{Z}$, $|a|+|b| \neq 0$

Look at $I = \{na + mb : n \in \mathbb{Z}, m \in \mathbb{Z}\}$ $(= \text{span}\{a,b\})$

Let d be the smallest positive element of I so $I = d\mathbb{Z}$
then $d = \gcd(a,b)$

<u>Pf.</u> i) $a \in I$ so $d|a$
$b \in I$ so $d|b$

ii) Let $c \in \mathbb{Z}$
$c|a$, $c|b$
Then $a = ck$ and $b = cl$ some $k, l \in \mathbb{Z}$
$d \in I$ so $d = na + mb$
some $n, m \in \mathbb{Z}$
$d = nck + mcl = (nk + ml)c$
$\therefore c|d$

* $d = \gcd(a,b)$ unique
If c is another divisor of a and b,
then i) $c | d$
d is a divisor of d
c is $\gcd(a,b)$
so $d | c \Rightarrow d = c$

* Let $V \subseteq \mathbb{Z}$ be a subspace (closed under linear combinations) then $V = d\mathbb{Z}$.
d is $\gcd(V)$

$V = \text{span}\{a_1, \dots, a_k\}$
$d = r_1 a_1 + \dots + r_k a_k$

$d = \gcd(a_1, \dots, a_k)$

* Calculation of $\gcd(a,b)$
(Suppose $a \geq b \geq 0$)

$a = bq + r, \quad 0 \leq r < b$
$d = \gcd(a,b) = \gcd(b,r) = d'$

<u>Pf.</u> $d' | r$, $d' | b$
$d' | bq + r = a$
$d' | d$

$a - bq = r$
$d | a$, $d | b$ so
$d | r$
Thus $d | b$, $d | r$
Thus $d | d'$
$\therefore d' = d$

$*\ a = bq_1 + r_1\ ,\ b = r_0$

If $r_1 = 0$:

$a = bq_1\ ,\ r_0 = b = \gcd(a,b)$

$(b,0) = b$

else: $r_1 \neq 0$

Write $b = r_0 = r_1 q_2 + r_2\ \ (r_2 < r_1 < r_0 = b)$

$(r_0, r_1) = (r_1, r_2) = (a,b)$

If $r_2 = 0$, $r_0 = r_1 q_2$

$(a,b) = (r_0, r_1) = (r_1, 0) = r_1$

else: $r_2 \neq 0$

suppose: $a = r_0 q_1 + r_1$

$r_0 = r_1 q_2 + r_2$

$\vdots$

$r_{k-1} = r_k q_{k+1} + r_{k+1}$

$r_0 > r_1 > r_2 > \dots > r_{k+1} \geq 0$

If $r_{k+1} = 0$, stop. $(a,b) = r_k$

else continue $r_{k+1} > 0$

Example: $(126, 35)$

$\Rightarrow 126 = 35 \cdot 3 + 21\ ,\ r_1 = 21$

$35 = 21 \cdot 1 + 14\ ,\ r_2 = 14$

$21 = 14 \cdot 1 + 7\ ,\ r_3 = 7$

$14 = 7 \cdot 2 + 0\ ,\ r_4 = 0$

$\therefore 7 = \gcd(126, 35)$ (the last non-zero remainder)

$7 = n \cdot 126 + m \cdot 35$

$r_1 = 21 = 1 \cdot 126 - 3 \cdot 35$

$r_2 = 14 = 1 \cdot 35 - 1 \cdot 21$

since $r_1 = 21 = 1 \cdot 126 - 3 \cdot 35$

$r_2 = 14 = 4 \cdot 35 - 1 \cdot 126$ (substituted)

$r_3 = 1 \cdot 21 - 1 \cdot 14$

since $r_2 = 4 \cdot 35 - 1 \cdot 126$

$r_3 = 2 \cdot 126 - 7 \cdot 35$ (substituted)

$a = 126,\ b = 35$

$1 \cdot 126 + 0 \cdot 35 = 126$

$0 \cdot 126 + 1 \cdot 35 = 35$

$$\begin{array}{c} \times 1 \\ \times 3 \\ \\ \end{array} \begin{bmatrix} 1 & 0 & \vdots & 126 \\ 0 & 1 & \vdots & 35 \\ a & b & & \end{bmatrix} \quad 1 \cdot a - 3b = 21, \quad 1 \cdot 126 - 3 \cdot 35 = 21$$

$$\times 1 \begin{bmatrix} 1 & -3 & \vdots & 21 \end{bmatrix} \quad -126 + 4 \cdot 35 = 14$$

$$\begin{bmatrix} -1 & 4 & \vdots & 14 \end{bmatrix} \quad 2(126) - 7 \cdot 35 = 7$$

$$\begin{bmatrix} 2 & -7 & \vdots & 7 \end{bmatrix}$$

* More example next time

HW due on 2/21 : Sec. 1.1