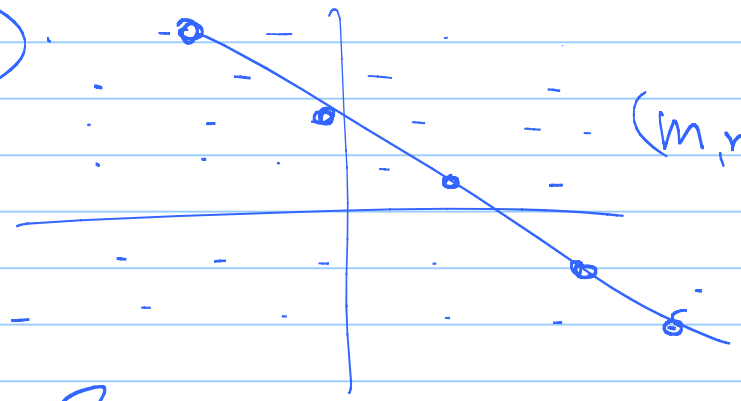
MA-222

Note Title 10-08-2021

Lec-6

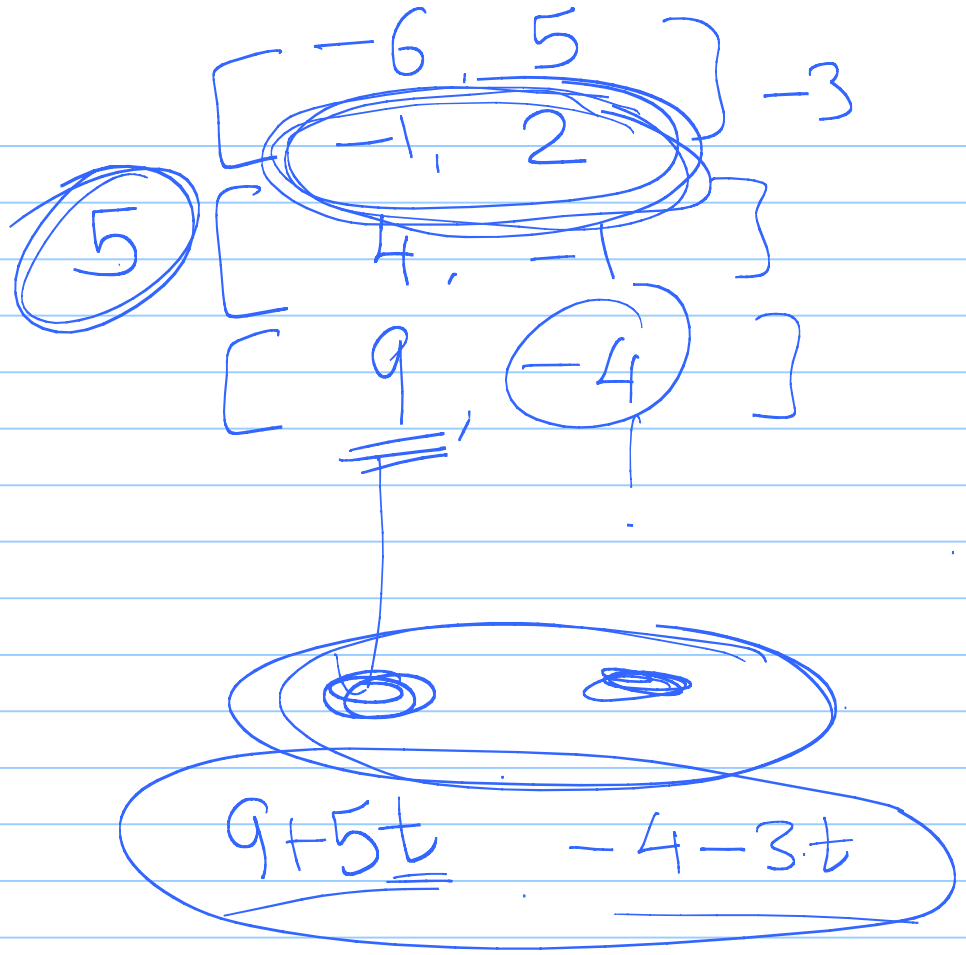
$l : 3x + 5y = 7$



$(m,n) \in \mathbb{R}^2$

$m, n \in \mathbb{Z}$

$l \cap \mathbb{Z}^2 = \phi$ or has infinitely many pts.



$3x+5y=7$

$9x+9y=7$

$ax+by=c$

If $\gcd(a,b) \nmid c$ then no soln.

Bezout's Lemma:

Extended Euclidean Algo.

$a, b \in \mathbb{N}$, then $\exists\, r, s \in \mathbb{Z}$ s.t.

$d = \gcd(a,b) = ar + bs$.

Pf

$d \mid a$. $d \mid b$. $\Rightarrow$ $d \mid ax + by$ for all $x, y \in \mathbb{Z}$.

$S = \{ ax + by \mid x, y \in \mathbb{Z} \;\&\; ax + by > 0 \} \subseteq \mathbb{N}$.

$\Rightarrow S \neq \emptyset$.

By WOP ∃ a least elt., say

$e = ax_0 + by_0$.

Claim: $d = e$.

Clearly $d \mid e$.

Subclaim: $e \mid a$ & $e \mid b$.

Supp not. i.e. $e \nmid a$

Write $a = eq + r$ $\quad 0 \leq r < e$.

$r = a - eq$

$r = a - eq$

$= a - (ax_0 + by_0)q$

$= a(1 - x_0 q) + b(-y_0 q)$

Thus r is a lin. comb. of a & b. & $r > 0$

$\Rightarrow r \in S$.

But $r < e$, contra to the choice of e

Thus $e \mid a$. Similarly $e \mid b$.

$\exists$ $e \leq d$ & $d \mid e$

$\Rightarrow e = d$.

Recall $d = gcd(a, b)$

i) $d > 0$

ii) $d \mid a$, $d \mid b$.

iii) d is the largest common div.

i.e. any other common div. $\leq d$.

Given $a, b \in \mathbb{N}$ $\exists x, y \in \mathbb{Z}$ s.t. $ax + by = gcd(a, b)$

Thm: $ax+by=c$ has a soln iff $(a,b) \mid c$.

Pf: ($\Rightarrow$) $d = \gcd(a,b)$

$\Rightarrow d \mid a \quad d \mid b \Rightarrow d \mid (ax+by)$

$\Rightarrow d \mid c$.

($\Leftarrow$) Conversely suppose $d \mid c \rightarrow c = dr$

$d = \gcd(a,b) \Rightarrow \exists x_0, y_0 \in \mathbb{Z}$ s.t.

$d = ax_0 + by_0$. //

mult by γ $\quad d\gamma = (ax_0 + by_0)\gamma$.

$\Rightarrow \quad c = a(\gamma x_0) + b(\gamma y_0)$

Thus $(\gamma x_0, \gamma y_0)$ is a soln to $ax+by=c$.

Thm: In other words a soln to $ax+by=c$ is $x = x_0 \frac{c}{d}, \; y = y_0 \frac{c}{d}$

where $x_0, y_0 \in \mathbb{Z}$ are such that

$ax_0 + by_0 = d$ //

□

Thm: If $ax+by=c$ has a soln, say (x_0, y_0) then all other solns are of the form

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t \qquad t \in \mathbb{Z}$$

$d = \gcd(a, b)$

Thm: **Special case:** $d = 1$ i.e. $(a, b) = 1$.

Then $ax+by=c$ always has a soln & the soln is given by $x = rc + bt$, $y = sc - at$ $t \in \mathbb{Z}$

where $r, s \in \mathbb{Z}$ s.t $ar + bs = 1$.

Thm: If $ax+by=c$ has a soln then all soln's are given by

$$x = r\left(\frac{c}{d}\right) + \left(\frac{b}{d}\right)t, \quad y = s\left(\frac{c}{d}\right) + \left(\frac{-a}{d}\right)t$$

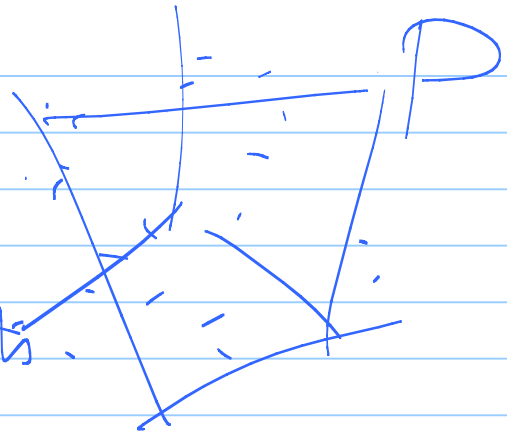
$t \in \mathbb{Z}$

$ax+bs = \gcd(a,b)$

$$16456x - 15779175\,00y = 24$$

$$ax+by+cz=d$$

$P \cap \mathbb{Z}^3 = \emptyset$ or has infinitely many pts.



Thm: $ax+by+cz=d$ has a soln $\iff$ $\gcd(a,b,c) \mid d$

Pf: Consider $S = \{ax+by \mid x, y \in \mathbb{Z}\}$

$d = \gcd(a,b)$. $d \in S$.

d divides every elt of S.

$ax+by+cz = d$ has a soln

iff $dw + cz = d$ has a soln.

iff $\gcd(d,c) \mid d$

iff $\gcd(a,b,c) \mid d$.

Thm: In gen. the

$a_1x_1 + \cdots + a_nx_n = b$ has a soln

iff $\gcd(a_1, \ldots, a_n) \mid b$.