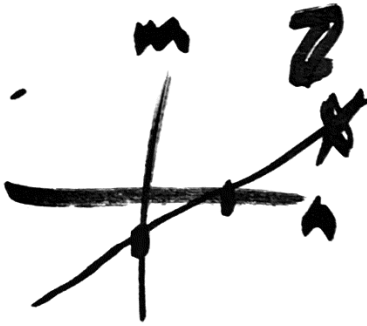
Last time: Look at $p < 100$, if $p \equiv 3 (4) \Rightarrow p \neq \square + \square$. if $p \equiv 1 (4)$, all are $p = \square + \square$. Back up to solving linear eqn's in $\mathbb{Z}$:

Ex: $17n - 25m = 4$. (over $\mathbb{R}$, line)

Attempt 1: $n=6, m=4$? $\underbrace{17 \cdot 6}_{102} - 25 \cdot 4 = 2$.



Obs: Double n & $m \Rightarrow$ double answer,

$\boxed{n=12, m=8} \Rightarrow \underbrace{17 \cdot 12}_{\text{even}} - \underbrace{25 \cdot 8}_{200} = 4$

Idea: Look at $17u - 25v = 0$! Why this other equation? Because if $17n_1 - 25m_1 = 4$ & $17n_2 - 25m_2 = 4$

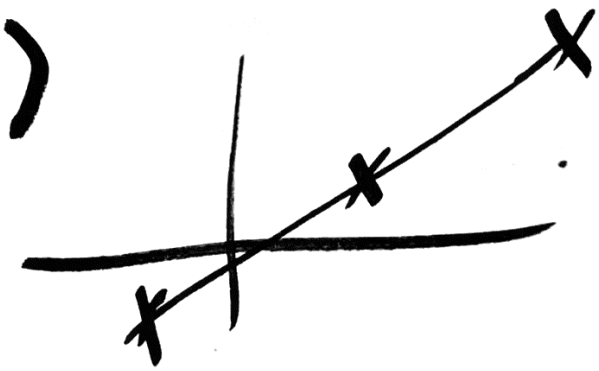
$$\Rightarrow 17\underbrace{(n_1 - n_2)}_{u} - 25\underbrace{(m_1 - m_2)}_{v} = 0.$$ How to solve $17u - 25v = 0$ in $\mathbb{Z}$?

Because 17 & 25 are coprime, all solutions are $\underbrace{(25k, 17k)}_{(u,v)}$ $\forall k \in \mathbb{Z}$.

$\hookrightarrow 17 \cdot 25k - 25 \cdot 17k = 0.$

So all solutions to $17n - 25m = 4$ are:

$(12 + 25k, 8 + 17k)$



$21n + 15m = 12$ Find all $n, m \in \mathbb{Z}$ solving.

Step 1: Find single solution: $(-3, 5)$

$21(-3) + 15(5) = 12$ ✓.

$(-3 + \underline{15}k, 5 - \underline{21}k)$ ← Not all solutions.

Step 2: $21u + 15v = 0 \iff 7u + 5v = 0 \iff (-5k, 7k)$

→ All sol'ns: $(-30 - 5k, 5 + 7k) \ni (2, -2)$.

→ Notice common factor of 3: $7n + 5m = 4$.

In general, try to solve $an + bm = c$?

Look at $S = \{an + bm \mid n, m \in \mathbb{Z}\} \subseteq \mathbb{Z}$.

Ex: What is $\{32n + 18m \mid n, m \in \mathbb{Z}\} = 2\mathbb{Z}$.

Note: 32 & 18 both even, $S \subseteq 2\mathbb{Z}$.

If $32n + 18m = 2$ has a solution, then $2\mathbb{Z} \subseteq S$.

$\Leftarrow$ $16n + 9m = 1$, $(n, m) = (4, -7)$

Now to solve $32n + 18m = 2k$, use $(n, m) = (4k, -7k)$.

Back to $S = \{an + bm \mid n, m \in \mathbb{Z}\}$

Thm: $S = d\mathbb{Z}$, where $d = \gcd(a, b)$.

Pf: **Claim 1:** $S \subseteq d\mathbb{Z}$. Because $\ell \mid a$ & $\ell \mid b$

$\Rightarrow \ell \mid an + bm$.

Claim 2: If $an + bm = d$ has a solution,

then $d\mathbb{Z} \subseteq S$. ($\Rightarrow S = d\mathbb{Z}$).

(4)

Last step: how to solve $an+bm=d$ where $d=\gcd(a,b)$? Euclidean algorithm.

$173, 215$.

$215 = 173 \cdot q_0 + r_0$ (or 42). $\in [0, 172]$.

$173 = 42 \cdot q_1 + r_1$ (or 4) ≤ 41.

$42 = 5 \cdot q_2 + r_2$ (or 2)

$5 = 2 \cdot q_3 + r_3$ (or 2) ← gcd.

$2 = 1 \cdot q_4 + r_4$ (or 2) $r_4 = 0$

$173n + 215m = 1$

$1 = 5 - 2 \cdot 2$

$= 5 - 2(42 - 5 \cdot 8)$

$= 17 \cdot 5 - 2 \cdot 42$

$= 17(173 - 4 \cdot 42) - 2 \cdot 42$.

1

$$1 = 17 \cdot 173 - 70 \cdot 42.$$
$$= 17 \cdot 173 - 70(215 - 173).$$
$$= 87 \cdot 173 - 70 \cdot 215.$$

Exercises: Solve in $\mathbb{Z}$: (all solutions)

① $187n + 221m = 68$

② $6188n + 4709m = 51$

③ $314n + 159m = -1$

$\uparrow$

3