Theorem from last time

Let $a, b, c \in \mathbb{Z}$, a and b not both zero

Let $d = \gcd(a, b)$

① $ax + by = c$ has integer solutions if and only if $d \mid c$

② If there are integer solutions and (x_0, y_0) is a particular solution, then all integer solutions to $ax + by = c$ are given by

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

where t can be any integer

Ex: Consider

$\boxed{c=17}$

$$578x + 153y = 17$$

$\boxed{d=17}$

We know

$$\gcd(578, 153) = 17$$

Since $d \mid c$ there is an integer solution and we found a particular solution previously using the Euclidean algorithm.

It was $x_0 = 4$, $y_0 = -15$.

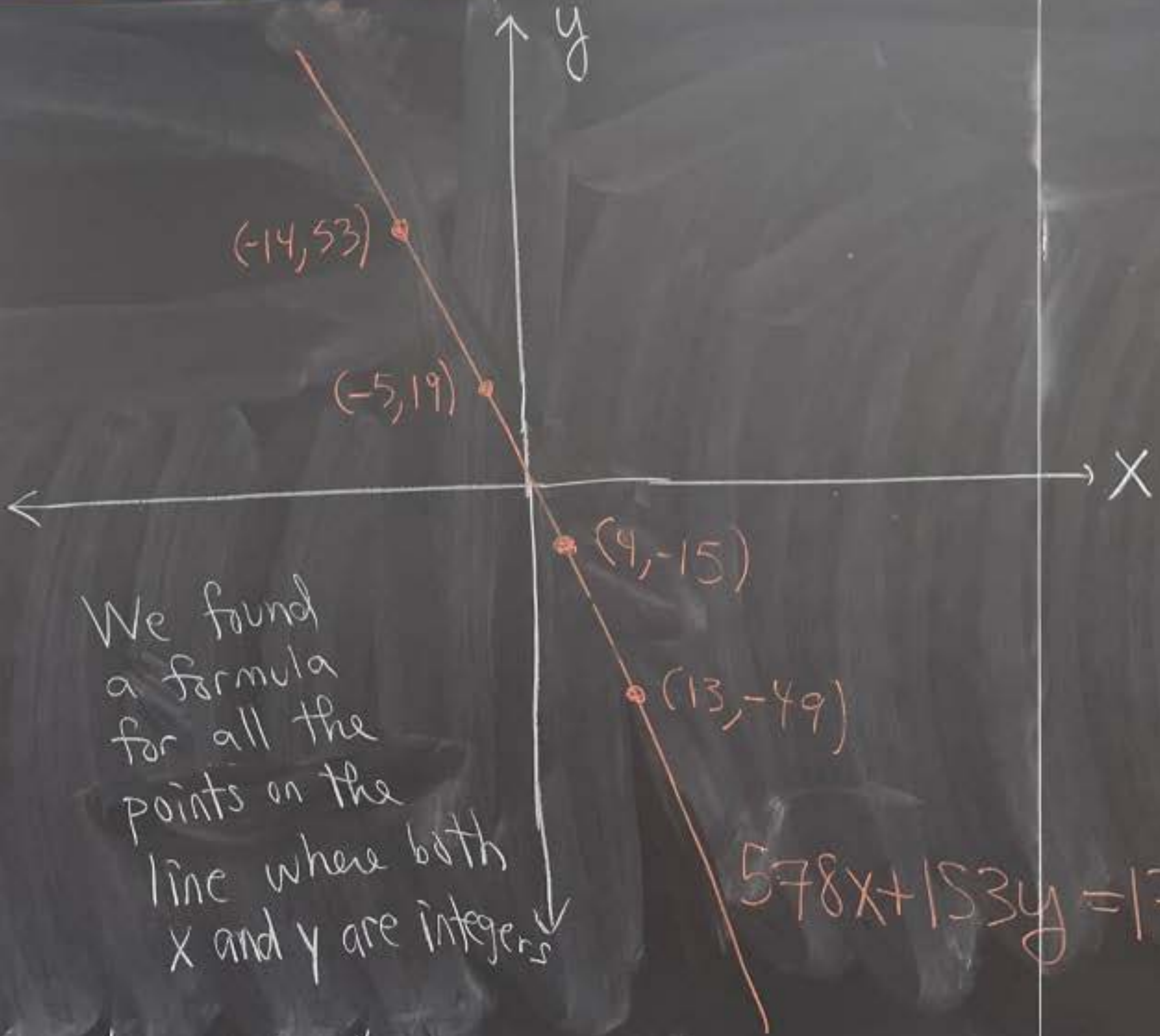
The formula from (2) gives all solutions to $578x + 153y = 17$.

They are

$$x = x_0 - t\left(\frac{b}{d}\right) = 4 - t\left(\frac{153}{17}\right) = 4 - 9t$$

$$y = y_0 + t\left(\frac{a}{d}\right) = -15 + t\left(\frac{578}{17}\right) = -15 + 34t$$

t	$x = 4 - 9t$	$y = -15 + 34t$
0	4	−15
1	−5	19
−1	13	−49
2	−14	53
−2	22	−83
⋮	⋮	⋮



We found a formula for all the points on the line where both x and y are integers

$$578x + 153y = 17$$

Proof of theorem

① Let $d = \gcd(a,b)$

($\Leftarrow$) Suppose $d \mid c$.

We proved previously that there exists $x_0, y_0 \in \mathbb{Z}$ where $ax_0 + by_0 = d$

(You use the Euclidean algorithm to find x_0, y_0)

Since $d \mid c$ we know $c = dk$ where $k \in \mathbb{Z}$.

Multiply $ax_0 + by_0 = d$ by k to get

$$a\underbrace{(kx_0)}_{x_1} + b\underbrace{(ky_0)}_{y_1} = \underbrace{dk}_{c}$$

Thus, $ax_1 + by_1 = c$

where $x_1 = kx_0$, $y_1 = ky_0$.

So, $ax + by = c$ has integer solutions.

($\Rightarrow$) Suppose $ax+by=c$ has integer solutions.

So we can find $x_0, y_0 \in \mathbb{Z}$ where $ax_0+by_0=c$.

Since $d=\gcd(a,b)$, we know $d|a$ and $d|b$.

So, $a=dk$ and $b=d\ell$ where $k,\ell \in \mathbb{Z}$.

Thus $ax_0+by_0=c$ becomes $dkx_0+d\ell y_0=c$.

So, $d[kx_0+\ell y_0]=c$

Thus, $d|c$.

② Suppose (x_0, y_0) is a particular solution, that is $\boxed{ax_0 + by_0 = c}$.

(i) Let's check if

$$x = x_0 - t\left(\frac{b}{d}\right)$$

$$y = y_0 + t\left(\frac{a}{d}\right)$$

that we still have a solution.

Substituting this into the equation gives

$$\begin{aligned} ax+by &= a\left[x_0 - t\left(\frac{b}{d}\right)\right] + b\left[y_0 + t\left(\frac{a}{d}\right)\right] \\ &= ax_0 - t\frac{ab}{d} + by_0 + t\frac{ab}{d} \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

It works!

Why does the formula give us <u>all</u> the integer solutions?
Let's show that now.

Suppose (x_0, y_0) is a particular solution, that is, $\boxed{ax_0 + by_0 = c}$

Suppose (x, y) is another solution, that is,

$$\boxed{ax + by = c}.$$

Subtracting the formulas gives

$$\boxed{a(x - x_0) + b(y - y_0) = 0}$$

Divide [redacted] by d and rearrange

$$\frac{a}{d}(x-x_0)=\frac{-b}{d}(y-y_0)$$

Multiply by -1 to get

$$\boxed{\frac{a}{d}(x_0-x)=\frac{b}{d}(y-y_0)} \quad (*)$$

Note $\frac{a}{d}$ and $\frac{b}{d}$ are integers because $d \mid a$ and $d \mid b$.

$(*)$ says that $\frac{a}{d} \mid \frac{b}{d}(y-y_0)$.

Since $d=\gcd(a,b)$ we know from a previous theorem that $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$.

Since $\frac{a}{d} \mid \frac{b}{d}(y-y_0)$ and $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$ we know $\frac{a}{d} \mid (y-y_0)$.

So, $y-y_0=t\left(\frac{a}{d}\right)$ where $t\in\mathbb{Z}$.

Thus, $y=y_0+t\left(\frac{a}{d}\right)$.

Plug $y = y_0 + t\left(\frac{a}{d}\right)$

back into (*) to get

$$\frac{a}{d}(x_0 - x) = \frac{b}{d}\left(y_0 + t\left(\frac{a}{d}\right) - y_0\right)$$

So,

$$\frac{a}{d}(x_0 - x) = \frac{b}{d} \cdot \frac{a}{d} \cdot t$$

Thus, $x_0 - x = \frac{b}{d}t$. So, $x = x_0 - \frac{b}{d}t$.

Thus, the formula gives all solutions.

$\boxtimes$