


Math 4460
2/19/25

_____ 

Proof of theorem from Monday

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

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

①

(\Rightarrow) Suppose there exist
integers x and y where

$$ax + by = c.$$

Our goal is to show that $d \mid c$.

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

Thus, $a = dk$ and $b = dl$
where $k, l \in \mathbb{Z}$.

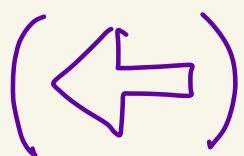
Plug these into $ax + by = c$

to get $dkx + dly = c$.

$$\text{So, } d[kx + ly] = c$$

this is an integer

Therefore, $d|c$.



Now assume that $d|c$.

Our goal is to find $x, y \in \mathbb{Z}$
where $ax + by = c$.

Since $d|c$ we know $c = dm$
where $m \in \mathbb{Z}$.

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

$$ax_0 + by_0 = d$$

for some $x_0, y_0 \in \mathbb{Z}$.

use
Euclidean
algorithm

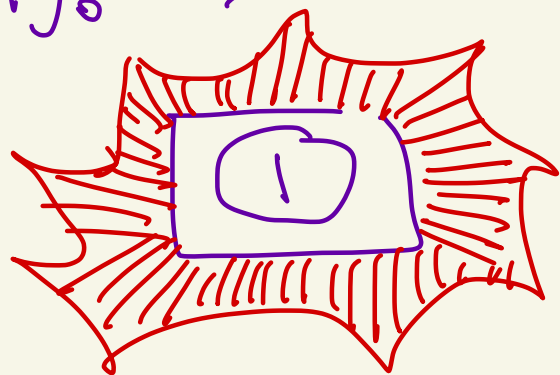
Multiply by m to get

$$a(mx_0) + b(my_0) = dm$$

This gives

$$ax + by = c$$

Where $x = mx_0, y = my_0$



② Suppose $ax + by = c$ has integer solutions. Let's find a formula for all of them.

Let (x_0, y_0) be a particular solution, that is suppose $ax_0 + by_0 = c$ where $x_0, y_0 \in \mathbb{Z}$

Our goal is to show that every solution is of the form

$$\left. \begin{aligned} x &= x_0 - t \left(\frac{b}{d} \right) \\ y &= y_0 + t \left(\frac{a}{d} \right) \end{aligned} \right\} (*)$$

where $t \in \mathbb{Z}$

Let's first check that (*) gives a solution by plugging it in. We get:

$$ax + by$$

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

$$= ax_0 - t \left(\frac{ab}{d} \right) + by_0 + t \left(\frac{ab}{d} \right)$$

$$= ax_0 + by_0$$

$$= c$$

But why does (*) give us all the solutions?

We are assuming $ax_0 + by_0 = c$.

Suppose we have another solution $ax + by = c$.

Subtract to get

$$a(x - x_0) + b(y - y_0) = 0$$

Thus,

$$b(y - y_0) = -a(x - x_0)$$

So,

$$b(y - y_0) = a(x_0 - x)$$

Thus,

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

$$\frac{b}{d}, \frac{a}{d} \in \mathbb{Z} \quad \text{because } d|a, d|b \\ d = \gcd(a, b)$$

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

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

From another previous theorem

since $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ and

$\frac{a}{d} \mid \frac{b}{d}(y-y_0)$ we know

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

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

where $t \in \mathbb{Z}$.

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

Plug $y - y_0 = t\left(\frac{a}{d}\right)$ into $(**)$
to get:

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

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

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

So every solution of $ax + by = c$
is of the form $(*)$. □(2)

③ Follows from
1 and 2.

QED =

EX: (HW 2 #4(f))

Solve

$$39x + 17y = 22$$

Let

$$d = \gcd(39, 17).$$

Euclidean algorithm time

$$39 = 2 \cdot 17 + 5$$

$$17 = 3 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

$$\gcd(39, 17) = 1$$

Use above to solve $39x_0 + 17y_0 = 1$

Rewrite above with remainders on left side.

$$5 = 1 \cdot 39 - 2 \cdot 17$$

$$2 = 1 \cdot 17 - 3 \cdot 5$$

$$1 = 1 \cdot 5 - 2 \cdot 2$$

← start here

We get

$$1 = 1 \cdot 5 - 2 \cdot 2$$

$$= 1 \cdot (1 \cdot 39 - 2 \cdot 17) - 2 \cdot (1 \cdot 17 - 3 \cdot 5)$$

$$= 1 \cdot 39 - 4 \cdot 17 + 6 \cdot 5$$

$$= 1 \cdot 39 - 4 \cdot 17 + 6 \cdot (1 \cdot 39 - 2 \cdot 17)$$

$$= 7 \cdot 39 - 16 \cdot 17$$

Thus,

$$1 = 39(7) + 17(-16)$$

Multiply by 22 to get:

$$22 = 39(154) + 17(-352)$$

Thus

$$39x_0 + 17y_0 = 22$$

$$\text{where } x_0 = 154, y_0 = -352$$

Every solution to

$$39x + 17y = 22$$

is of the form

$$x = x_0 - t\left(\frac{b}{d}\right) = 154 - t\left(\frac{17}{1}\right)$$

$$y = y_0 + t\left(\frac{a}{d}\right) = -352 + t\left(\frac{39}{1}\right)$$

That is, any solution is of the form

$$x = 154 - 17t$$

$$y = -352 + 39t$$

Where t is any integer