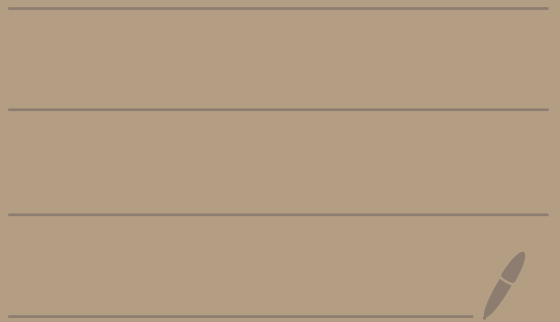


Math 4460

2/5/25



Theorem (Division algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$.

Then there exist unique integers q and r where

$$a = qb + r$$

$$\text{and } 0 \leq r < b$$

Proof:

First the existence part.

Define

$$T = \{ a - xb \mid x \in \mathbb{Z} \text{ and } a - xb \geq 0 \}$$

Ex: $a = 10, b = 3$

$$T = \{ 10 - 3x \mid x \in \mathbb{Z} \text{ and } 10 - 3x \geq 0 \}$$

$$a - 3b = 10 - 3 \cdot 3 = 1 \quad \leftarrow \boxed{x=3}$$

$$a - 2b = 10 - 2 \cdot 3 = 4 \quad \leftarrow \boxed{x=2}$$

So, $1 \in T$ and $4 \in T$

T is infinite

Idea: We will find the r we want inside of T .

Claim: T is not empty

pf of claim:

case 1: Suppose $a = 0$.

Then, if $x = 0$ we get

$$a - bx = 0 - b \cdot 0 = 0 \in T$$

case 2: Suppose $a > 0$.

Then set $x = -1$ and get

$$a - bx = \underbrace{a + b}_{> 0} \in T$$

Case 3: Suppose $a < 0$.

Set $x = 2a$ and get > 0

$$a - bx = a - 2ab = \underbrace{a}_{a < 0} \underbrace{(1 - 2b)}_{b \geq 1} \in T$$

$$a < 0$$

$$b \geq 1$$

$$-2b \leq -2$$

$$1 - 2b \leq -1$$

$$1 - 2b < 0$$

Summary of cases is: T is not empty

Claim

So, T is a non-empty set of non-negative numbers.

Thus, T must contain a smallest number, call that number r .

So, $r \leq t$ for all $t \in T$.

Since $r \in T$ we can write

$$r = a - bq$$

[I'm using q instead of x]

Thus, $a = bq + r$

Is $0 \leq r < b$?

We already know $r \geq 0$ since $r \in T$.

Let's rule out $b \leq r$.

Suppose $b \leq r$.

Then $0 \leq r - b$.

Also,

$$r - b = \underbrace{(a - bq)}_r - b$$

$$= a - b \underbrace{(q+1)}_x \in T$$

Thus, $r - b \in T$.

But then $0 \leq r - b < r$

$$\boxed{b > 0}$$

But r is the smallest element of T . We can't have

$$r - b \in T \text{ and } r - b < r.$$

Contradiction.

Thus, $0 \leq r < b$

Thus, there exist q, r with
 $a = bq + r$ and $0 \leq r < b$.

(uniqueness)

Suppose

$$a = bq + r \quad \text{and} \quad a = bq' + r'$$

where $0 \leq r < b$ and $0 \leq r' < b$.

Let's show this implies

$$\text{that } q = q' \text{ and } r = r'.$$

WLOG (without loss of generality)

assume $r' \leq r$.

Subtract $a = q'b + r'$ from $a = qb + r$
to get

$$0 = (q - q')b + (r - r')$$

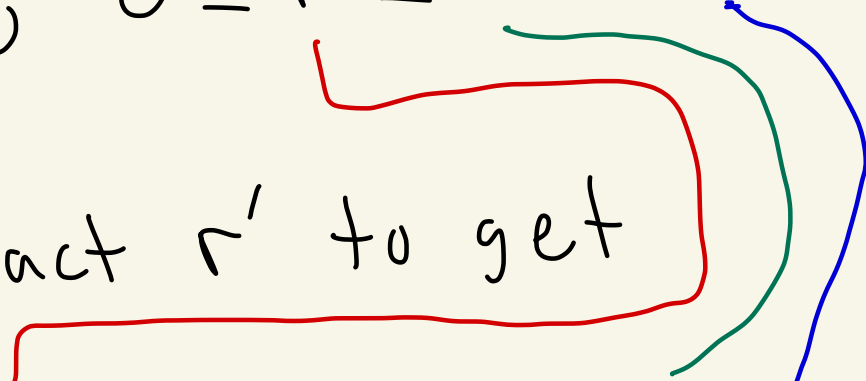
We get

$$(q' - q)b = (r - r')$$

So, $b \mid (r - r')$.

Also, $0 \leq r' \leq r < b$.

Subtract r' to get



$$0 \leq r - r' < b - r' \leq b$$

So, $b \mid (r - r')$ and $0 \leq r - r' < b$.

This can only happen if $r - r' = 0$

$$\text{So, } r = r'.$$

Plug $r - r' = 0$ into

$$0 = (q - q')b + (r - r')$$

to get

$$0 = (q - q') \underbrace{b}_{b > 0}$$

$$\text{So, } q - q' = 0.$$

$$\text{Thus, } q = q'.$$

END!

Theorem: Let $a, b \in \mathbb{Z}$,
not both zero. Then there
exist $x_0, y_0 \in \mathbb{Z}$ with
 $\gcd(a, b) = ax_0 + by_0$

proof: Define

$$S = \{ ax + by \mid x, y \in \mathbb{Z} \}$$
$$= \left\{ \underbrace{a \cdot 1 + b \cdot 0}_{x=1, y=0}, \underbrace{100a - 50b}_{x=100, y=-50}, \dots \right\}$$

Note that

$$a = a(1) + b(0) \in S$$

$$-a = a(-1) + b(0) \in S$$

$$b = a(0) + b(1) \in S$$

$$-b = a(0) + b(-1) \in S$$

So, $a, -a, b, -b \in S$.

Since a and b are not both zero this implies that S contains a positive integer.

So, S must contain a smallest positive integer, call it d .

Since $d \in S$ we have

$$d = ax_0 + by_0$$

where $x_0, y_0 \in \mathbb{Z}$.

Let's show that $d = \gcd(a, b)$
and we are done.

First let's show d is a
common divisor of a & b .

Let's show that $d|a$.

By the division algorithm
we get $q, r \in \mathbb{Z}$ where

$$a = dq + r$$

$$\text{and } 0 \leq r < d.$$

Note that

$$r = a - dq$$

$$= a - \underbrace{(ax_0 + by_0)}_d q$$

$$= a(1 - x_0q) + b(-y_0q)$$

is of form $ax + by$
where $x, y \in \mathbb{Z}$

So, $r \in S$.

But $0 \leq r < d$ and $r \in S$
and d is the smallest
positive element of S .

Thus, $r = 0$.

$$\text{So, } a = dq + r = dq$$

So, $d \mid a$.

Similarly you can show that $d \mid b$.

So, d is a common divisor
of a & b .

Why is d the greatest positive
common divisor of a & b ?

Suppose d' is another ^{positive} common
divisor of a and b .

That is, $d' \mid a$ and $d' \mid b$.

Let's show that $d' \leq d$.

Since $d' \mid a$ and $d' \mid b$

we get $a = d'k$ and $b = d'l$

where $k, l \in \mathbb{Z}$.

Then,

$$d = ax_0 + by_0$$

$$= d'kx_0 + d'ly_0$$

$$= d'[kx_0 + ly_0]$$

So, $d' \mid d$.

So, $d' \mid d$ and $d' > 0$ and $d > 0$
thus by a previous theorem
we get $d' \leq d$.

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

