Math 4460
2/6/23

Theorem (The division algorithm)

Let $a, b \in \mathbb{Z}$ with $b > 0$.
Then there exist unique integers q, r
where $a = qb + r$
and $0 \leq r < b$.

<u>proof:</u> Let $a, b \in \mathbb{Z}$ with $b > 0$.
Consider the set

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

<u>Ex:</u> $a = 10, b = 3$

$a - 2b = 10 - 2(3) = 4 \geq 0 \leftarrow 4 \in T$

$a - 3b = 10 - 3(3) = 1 \geq 0 \leftarrow 1 \in T$

$a - 4b = 10 - 4(3) = -2 \not\geq 0 \leftarrow -2 \notin T$

<u>Claim:</u> T is not empty

<u>proof of claim:</u>

case 1: Suppose $a=0$.

Then, if you set $x=0$, then

$$a-xb = 0-0b=0 \geq 0$$

So, $0 \in T$.

case 2: Suppose $a>0$.

$a>0$
$b>0$

Set $x=-1$, and get

$$a-xb = a-(-1)b = a+b > 0$$

So, $a+b \in T$

case 3: Suppose $a<0$.

Set $x=2a$ and get

$$a-xb = a-2ab = \underbrace{a}_{\boxed{a<0}}\underbrace{(1-2b)}_{} > 0$$

$b \geq 1$
$-2b \leq -2$
$1-2b \leq -1$
$1-2b < 0$

So,
$a-2ab \in T$

Thus, $T \neq \emptyset$

$\boxed{\text{Claim}}$

Since T is not empty and every element of T is non-negative, T must have a smallest element.

Let r be the smallest element of T.

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

Since r is in T we can write

$r = a - qb$ where $q \in \mathbb{Z}$

[I'm using q instead of x]

Thus, $\boxed{a = qb + r}$.

Is $0 \le r < b$?

We know $0 \le r$ because $r \in T$.

Why is $r < b$?

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

Suppose $r \geq b$.

Then, $\boxed{r - b \geq 0}$ and

$$\boxed{r - b = (a - bq) - b = \underbrace{a - (q+1)b}_{\text{of the form } a - xb}}$$

Then $r - b \in T$.

$\boxed{b > 0}$

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

This contradicts that r is the smallest element of T.

Thus, $r < b$.

So, $\boxed{a = qb + r \text{ and } 0 \le r < b.}$

What about uniqueness?

Suppose $a = qb + r$ and $a = q'b + r'$ where $0 \leq r < b$ and $0 \leq r' < b$ and $q, q', r, r' \in \mathbb{Z}$.

Let's show $q = q'$ and $r = r'$. $\leftarrow$ $\boxed{\text{Goal}}$

$\underbrace{\text{Without loss of generality}}$ assume $r' \leq r$.

means: same proof if $r \leq r'$

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

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

So,

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

Thus, b divides $r - r'$.

Recall $0 \le r' \le r < b$.

Subtract by r' to get

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

Thus,

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

But b divides $r - r'$!

Thus, $r - r' = 0$.

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

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

to get $0 = (q - q')b$.

So either $q - q' = 0$ or $b = 0$.

But $b > 0$.

So, $q - q' = 0$

Thus, $\boxed{q = q'}$

We've proved uniqueness.

$\boxed{\text{DIVISION ALG.}}$

Theorem: Let $a, b \in \mathbb{Z}$, not both zero. Then there exist integers x_0, y_0 where

$$\gcd(a,b) = a x_0 + b y_0$$

proof:
Let $a, b \in \mathbb{Z}$, not both equal to zero.

Define the following set

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

$$= \{ \underbrace{10a+12b}_{x=10,\, y=12},\ \underbrace{1\cdot a+0\cdot b}_{x=1,\, y=0},\ \underbrace{2a-10000b}_{x=2,\, b=-10000},\ \dots \}$$

Note that

$$a = a(1) + b(0)$$
$$-a = a(-1) + b(0)$$
$$b = a(0) + b(1)$$
$$-b = a(0) + b(-1)$$

are all in S.

Since $a, -a, b, -b \in S$ and a and b are not both zero, S must contain at least one positive integer.

Let d be the smallest positive integer in S.

Then, $d = ax_0 + by_0$ where $x_0, y_0 \in \mathbb{Z}$.

Now we show d is the gcd of a and b and we are done.

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

Let's show $d \mid a$.

By the division algorithm we can write $a = dq + r$ where $0 \le r < d$ where $q, r \in \mathbb{Z}$.

Let's show $r = 0$.

Note that

$$\left.\begin{aligned} r &= a - dq \\ &= a - (ax_0 + by_0)q \\ &= \underbrace{a(1 - x_0 q) + b(-y_0 q)}_{\text{form } ax+by} \end{aligned}\right\} \text{saying } r \text{ is in } S$$

So $\boxed{r \in S}$.

But also $\boxed{0 \le r < d}$.

Since d is the smallest positive integer in S, this forces $r = 0$.

Thus, $a = qd + r = qd$.

So, $d \mid a$.

Similarly you can show $d \mid b$.

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

positive

Why is d the greatest common divisor of a and b?

positive

Suppose d' is another common divisor of a and b.

We <u>must show</u> $d' \le d$.

Since $d' | a$ and $d' | b$ we know

$a = d'k$ and $b = d'l$
where $k, l \in \mathbb{Z}$.

Then,

$$d = ax_0 + by_0 = (d'k)x_0 + (d'l)y_0$$
$$= d'[kx_0 + ly_0]$$

So, d' divides d.

Since $d' | d$ and d and d' are both positive $d' \le d$.

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

DONE