Math 3450
2/20/24

Ex: $a = 5$
$b = 17$

$$3 \leftarrow \boxed{q}$$
$$5\,\overline{)\,17}$$
$$\underline{-15}$$
$$2 \leftarrow \boxed{r}$$

$$\underbrace{17 = 5(3) + 2}_{b = aq + r}$$

$$0 \leq r < a$$

Theorem (Division Algorithm)
Let $a, b \in \mathbb{Z}$ with $a > 0$.
Then there exists unique integers q and r where

$$b = aq + r \text{ and } 0 \leq r < a$$

proof:

(existence)

Let $S = \{ b - ax \mid x \in \mathbb{Z} \text{ and } b - ax \geq 0 \}$

Ex: $a = 5, b = 17$

$S = \{ 17 - 5x \mid x \in \mathbb{Z},\ 17 - 5x \geq 0 \}$

$= \{ 2, 7, 12, 17, 22, \ldots \}$

Smallest element of S

x	$17-5x$
$\vdots$	$\vdots$
5	-8
4	-3
3	2
2	7
1	12
0	17
-1	22
$\vdots$	$\vdots$

$$\boxed{S = \left\{ b - ax \;\middle|\; \begin{array}{l} x \in \mathbb{Z} \\ b - ax \geq 0 \end{array} \right\}}$$

Let's show $S \neq \emptyset$.

Case 1: Suppose $b \geq 0$.

Setting $x = -1$ we get

$$b - ax = b - a(-1) = b + a \geq 0$$

$$\boxed{\begin{array}{c} b \geq 0 \\ a > 0 \end{array}}$$

So, $b - a(-1) \in S$.

Case 2: Suppose $b < 0$.

Set $x = 2b$ and we get

$$b - ax = b - a(2b) = \underbrace{b}_{b<0}\underbrace{(1-2a)}_{\begin{array}{l} a \geq 1 \\ -2a \leq -2 \\ 1-2a \leq -1 \\ 1-2a < 0 \end{array}} > 0$$

Thus, $b - a(2b) \in S$.

$$\boxed{S = \{b - ax \mid x \in \mathbb{Z},\ b - ax \geq 0\}}$$

So, by case 1 and case 2, $S \neq \emptyset$.

Since S is non-empty and it consists of non-negative integers, S must have a smallest element.

Let r be the smallest element of S.

Thus there exists $q \in \mathbb{Z}$ with $r = b - aq$ and $r = b - aq \geq 0$.

[I switched x to q here.]

So, $\boxed{b = aq + r}$.

We have $0 \leq r$.

We must show that $r < a$.

Suppose instead that $a \leq r$.

Then $0 \leq r - a$.

Also, $r - a = (b - aq) - a$

$$= \underbrace{b - a(q+1)}_{\text{has the form } b-ax} \in S$$

But $r - a < r$ and r is the smallest element of S.

Thus, it can't be that $r - a \in S$.

It's a contradiction.

Hence, $r < a$.

So, $b = aq + r$ with $0 \le r < a$.

Uniqueness Suppose

$b = aq + r$ with $0 \le r < a$, and

$b = aq' + r'$ with $0 \le r' < a$,

where $q, q', r, r' \in \mathbb{Z}$.

We will show $q = q'$ and $r = r'$

Let's show that $r = r'$.

Without loss of generality, assume $r' \geq r$

Means same proof will work if $r \geq r'$

Then, $\boxed{r' - r \geq 0}$.

Since $b = aq + r = aq' + r'$ we get

$$\boxed{a(q - q') = r' - r}.$$

Let $k = q - q'$.

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

Then from the eqn above since $a > 0$ and $r' - r \geq 0$ we know $k \geq 0$.

Let's show $k = 0$.

Suppose $k > 0$.

If so, then

$$r' - r = ak \underset{\boxed{k \geq 1}}{\geq} a(1) = a.$$

Then, $a \leq r' - r.$

However we also have that

$$0 \leq r' - r \underset{\boxed{r' < a}}{<} a - r \underset{\boxed{0 \leq r}}{\leq} a$$

So, $r' - r < a$

CONTRADICTION

This is nonsense!

So, $k \not> 0$.

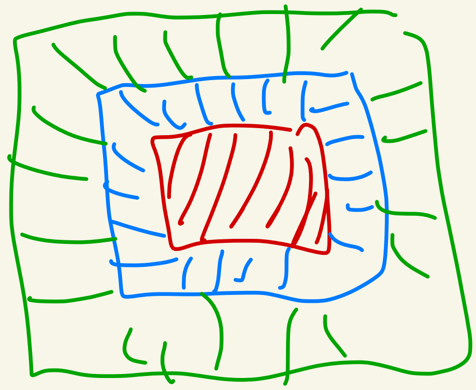
We must have $k = 0$.

Thus, $0 = k = q - q'$.

So, $q = q'$.

Also, $0 = a\underbrace{k}_{0} = r' - r$

So, $r = r'$.



Calculating modulo n using the division algorithm

Let $n \geq 2$.

Let $x \in \mathbb{Z}$.

Divide n into x to get

$$x = nq + r$$

where $q, r \in \mathbb{Z}$ and $0 \leq r < n$.

Then, $nq = x - r$

So, $n \mid (x-r)$.

So, $x \equiv r \pmod{n}$

Hence, $\overline{x} = \overline{r}$ in $\mathbb{Z}_n$

Ex: Let $n = 4$.

Let $x = 10,562$.

$$\begin{array}{r} 2640 \\ 4\overline{)\,10,562} \\ -8 \\ \hline 25 \\ -24 \\ \hline 16 \\ -16 \\ \hline 02 \\ -0 \\ \hline 2 \end{array}$$

$$\underbrace{10,562}_{x} = \underbrace{4}_{n}(2640) + \underbrace{2}_{r}$$

So,

$$10,562 \equiv 2 \pmod{4}$$

Ex: $n = 6$

$x = 220$

$$\begin{array}{r} 36 \\ 6\,\overline{)\,220} \\ -18 \\ \hline 40 \\ -36 \\ \hline 4 \end{array}$$

$$\underbrace{220}_{x} = \underbrace{6}_{n}(36) + \underbrace{4}_{r}$$

So, $220 \equiv 4 \pmod{6}$