Math 4460

2/27/23

<u>Theorem:</u> Let $a,b \in \mathbb{Z}$ with $a,b \geq 1$

Suppose $\gcd(a,b)=1$ and

$$ab = c^n$$

where $c,n \in \mathbb{Z}$ and $c,n \geq 1$.

Then there exist $d,e \in \mathbb{Z}$

with $d,e \geq 1$ where

$a = d^n$ and $b = e^n$.

<u>proof:</u> Suppose $\gcd(a,b)=1$

and $c^n = ab$.

If $a=1$, set $\overbrace{d=1}^{a=1^n}$ and $\overbrace{e=c}^{b=c^n}$.

If $b=1$, set $\underbrace{d=c}_{a=c^n}$ and $\underbrace{e=1}_{b=1^n}$.

So we can assume $a \geq 2$, $b \geq 2$.

Since $\gcd(a,b)=1$ we know the prime factors of a and b are distinct.

Thus we may may write

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

and $$b = p_{r+1}^{a_{r+1}} p_{r+2}^{a_{r+2}} \cdots p_{r+s}^{a_{r+s}}$$

Ex:

$a = 7^2 5^4 2^{10}$

$p_1^{a_1} p_2^{a_2} p_3^{a_3}$

$b = 13^2 \cdot 11^4$

$p_4^{a_4} p_5^{a_5}$

where $p_1, p_2, \ldots, p_r, p_{r+1}, \ldots, p_{r+s}$ are distinct primes and $a_1, \ldots, a_{r+s}$ are positive integers, $r \geq 1$, $s \geq 1$.

Suppose that

$$c = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}$$

is the prime factorization of c where $q_1, q_2, \ldots, q_k$ are distinct primes and $b_1, b_2, \ldots, b_k$ are positive integers.

Since $ab = c^n$ we get that

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} p_{r+1}^{a_{r+1}} p_{r+2}^{a_{r+2}} \cdots p_{r+s}^{a_{r+s}} \leftarrow ab$$

$$= q_1^{nb_1} q_2^{nb_2} \cdots q_k^{nb_k} \leftarrow c^n$$

By the fundamental theorem of arithmetic the left factorization and the right factorization are the same up to reordering the primes. Thus, $r+s=k$, and the primes q_j are the same as the primes p_i (except for the ordering possibly) and the corresponding exponents are the same.

Thus we may renumber/reorder the q's so that

$q_j = p_j$ for $1 \leq j \leq r+s$.

Then, $a_j = nb_j$ for $1 \le j \le r+s$.

Then,

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{nb_1} q_2^{nb_2} \cdots q_r^{nb_r}$$

$$= \underbrace{\left(q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r} \right)}_{d}{}^{n}$$

And

$$b = p_{r+1}^{a_{r+1}} p_{r+2}^{a_{r+2}} \cdots p_{r+s}^{a_{r+s}} = q_{r+1}^{nb_{r+1}} q_{r+2}^{nb_{r+2}} \cdots q_{r+s}^{nb_{r+s}}$$

$$= \underbrace{\left(q_{r+1}^{b_{r+1}} q_{r+s}^{b_{r+2}} \cdots q_{r+s}^{b_{r+s}} \right)}_{e}{}^{n}$$

Set

$d = q_1^{b_1} q_2^{b_2} \cdots q_r^{b_r}$ and $e = q_{r+1}^{b_{r+1}} q_{r+2}^{b_{r+2}} \cdots q_{r+s}^{b_{r+s}}$

and we get $a = d^n$, $b = e^n$ $\blacksquare$

HW 3

1(a) Given $a, b \in \mathbb{Z}$ with $b \neq 0$ there exist $x, y \in \mathbb{Z}$ with $y \neq 0$ where $\frac{a}{b} = \frac{x}{y}$ and $\gcd(x,y) = 1$.

<u>Ex:</u> $a = 25$, $b = 10$

$$\frac{a}{b} = \frac{25}{10} = \frac{5}{2} = \frac{x}{y} \quad \left.\begin{matrix} x = 5 \\ y = 2 \end{matrix}\right\}$$

$\gcd(5,2) = 1$

<u>proof:</u> Let $d = \gcd(a,b)$.

Set $x = \frac{a}{d}$ and $y = \frac{b}{d}$

By a previous theorem,

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

And

$$\frac{x}{y} = \frac{a/d}{b/d} = \frac{a}{b}.$$

$\blacksquare$

$\boxed{\text{HW 3}}$

1 (d) Let p be a prime. Prove that $\sqrt{p}$ is $\underbrace{\text{irrational.}}_{\text{not a rational number}}$

proof: Lets do a proof by contradiction.

Suppose $\sqrt{p}$ is rational.

By problem 1(a) this implies that $\boxed{\sqrt{p} = \frac{x}{y}}$ where $x, y \in \mathbb{Z}$, $y \neq 0$ and $\gcd(x,y) = 1$.

By squaring we get $p = \frac{x^2}{y^2}$ or $\boxed{py^2 = x^2}$ $(*)$

$(*)$ tells us that $p \mid x^2$.

Since p is prime and $p \mid x \cdot x$ we know that $p \mid x$.

We used:
p prime and $p \mid ab \to p \mid a$ or $p \mid b$

Thus, $x = pk$ where $k \in \mathbb{Z}$.

Plug this back into $(*)$ to get

$$p y^2 = (pk)^2$$

So, $y^2 = pk^2$.

Thus, $p \mid y^2$.

Since p is prime and $p \mid y \cdot y$

we know $p \mid y$.

Thus, $p \mid x$ and $p \mid y$.

So, $\gcd(x, y) \geq p \geq 2$

This contradicts $\gcd(x, y) = 1$.

Therefore $\sqrt{p}$ is irrational $\blacksquare$

TOPIC 4 - Integers modulo n

<u>Def:</u> Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $x, y \in \mathbb{Z}$.
We say that <u>x is congruent to y modulo n</u> if n divides $x-y$, and write
$$x \equiv y \pmod{n}.$$

If n does not divide $x-y$ then we write $x \not\equiv y \pmod{n}$.

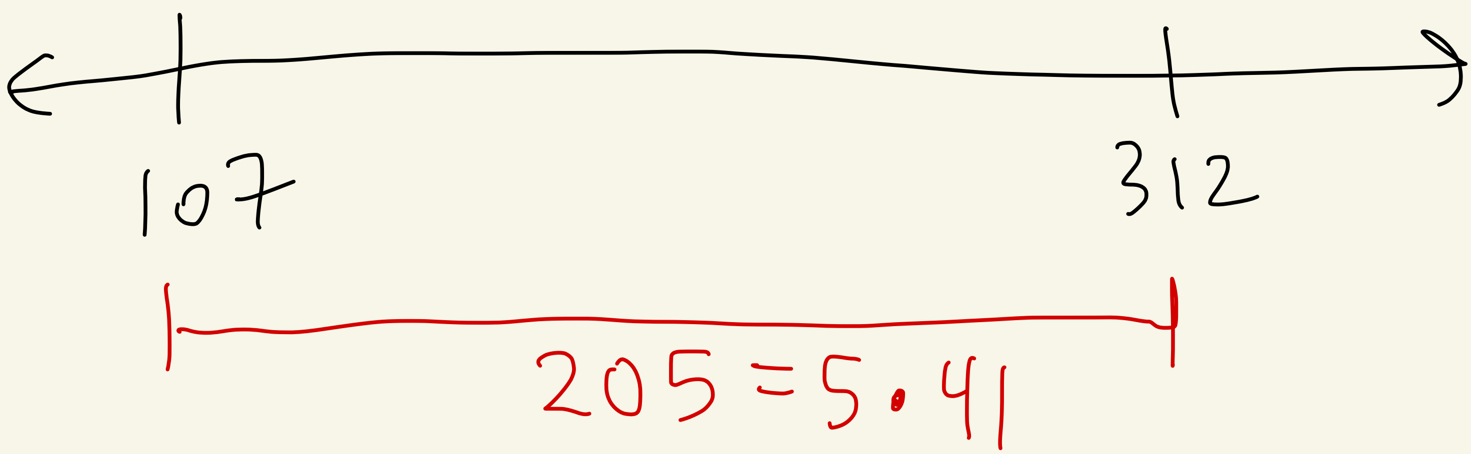
Ex: $n = 5$

$x = 312, \quad y = 107$

$x - y = 312 - 107 = 205 = 5 \cdot 41$

Thus, $5 \mid (312 - 107)$ and so

$$312 \equiv 107 \pmod{5}$$



They are a multiple of 5 apart from each other.

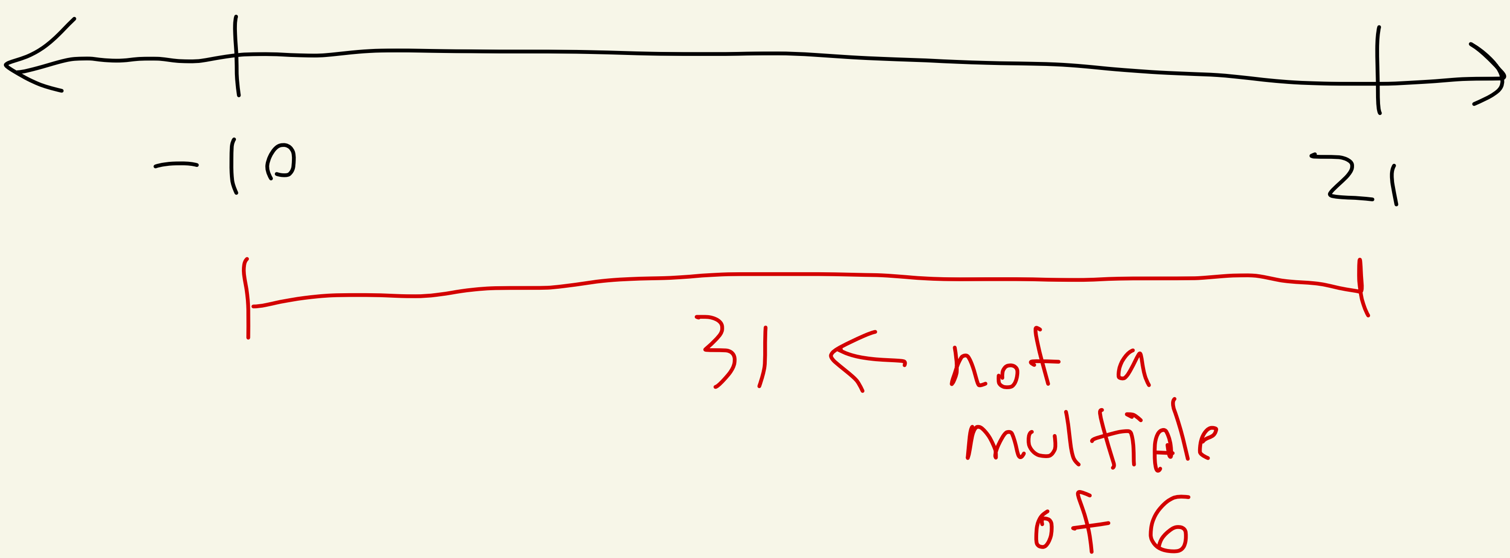
<u>Ex:</u> $n=6$

$x=-10 \quad y=21$

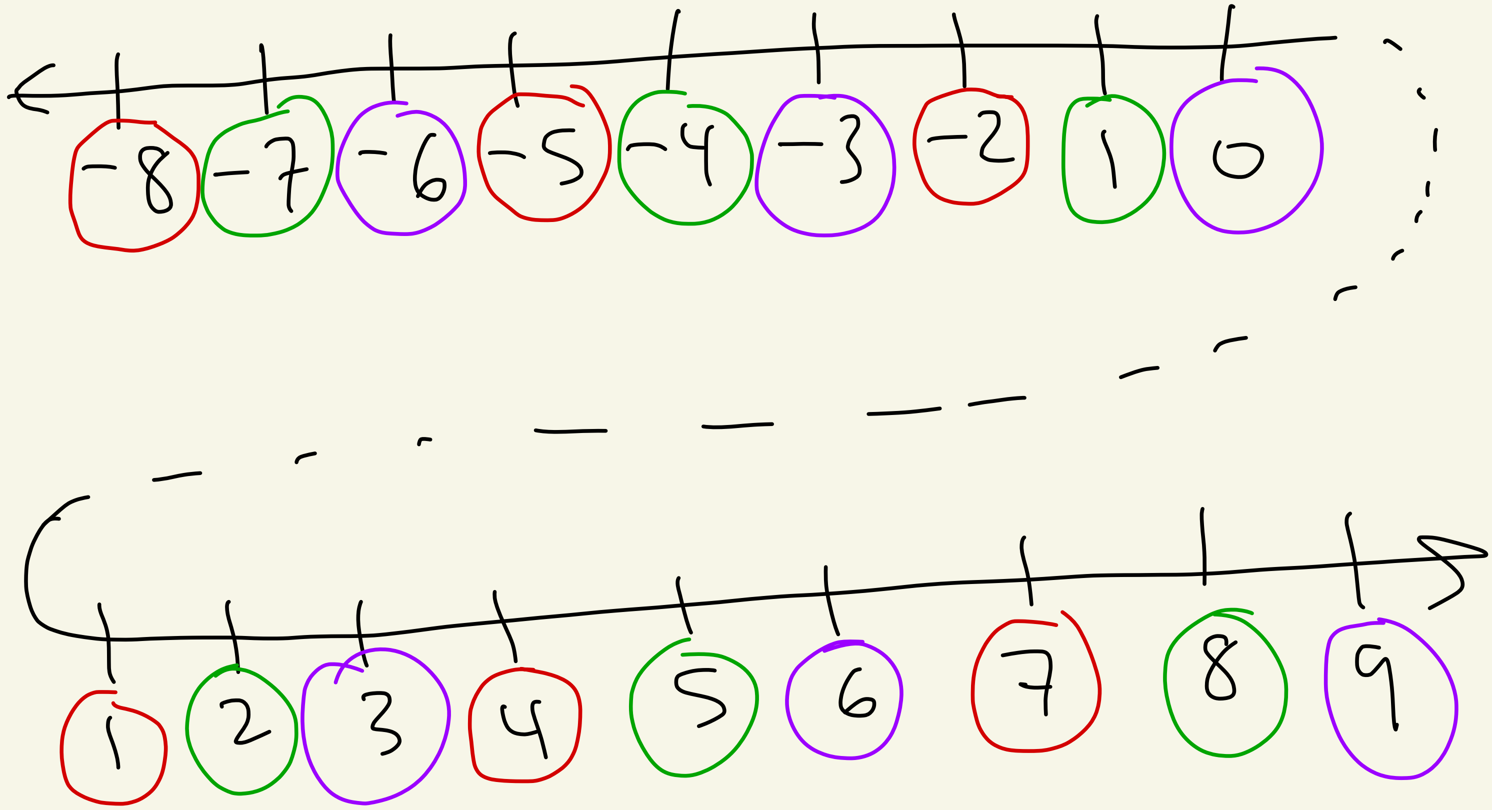
$x-y=-10-21=-31$

and $6 \nmid (-31)$.

So, $-10 \not\equiv 21 \pmod{6}$.



Ex: $n = 3$



$-8 \equiv -5 \pmod{3}$	$8 \equiv 2 \pmod{3}$	$9 \equiv 3 \pmod{6}$
$-2 \equiv -8 \pmod{3}$	$5 \equiv -4 \pmod{3}$	$-6 \equiv 6 \pmod{6}$
$1 \equiv -5 \pmod{3}$	$-7 \equiv 5 \pmod{3}$	$-6 \equiv 3 \pmod{6}$
$4 \equiv 7 \pmod{3}$	$\vdots$	$\vdots$
$\vdots$		