Topic 3 –

Fundamental Theorem of Arithmetic

Previously in Math 4460:
$a, b, p \in \mathbb{Z}$, p prime
If $p \mid ab$, then $p \mid a$ or $p \mid b$

$n=2$ case (below)

<u>Theorem:</u> Suppose that p is prime and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ with $n \geq 2$.
If $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i with $1 \leq i \leq n$

<u>proof:</u> Let p be a prime. [p is fixed for the proof]
Let $S(n)$ be the statement:

$\boxed{\text{"If } p \mid a_1 a_2 \cdots a_n \text{ where } a_1, a_2, \ldots, a_n \in \mathbb{Z}, \text{ then } p \mid a_i \text{ for some } i \text{ with } 1 \leq i \leq n\text{"}}$

We will induct on $S(n)$ where $n \geq 2$.

We already proved $S(2)$ is true in a previous class

[Ie, if $p \mid a_1 a_2$, then $p \mid a_1$ or $p \mid a_2$] ← $S(2)$

So we've proved the base case.

Let $k \in \mathbb{Z}$, $k \geq 2$.
Assume $S(k)$ is true.

induction hypothesis

We want to show $S(k+1)$ is true.

Suppose $p \mid \underbrace{a_1 a_2 \cdots a_k}_{(a_1 a_2 \cdots a_k)} \cdot \underbrace{a_{k+1}}_{(a_{k+1})}$, where $a_i \in \mathbb{Z}$ for $1 \leq i \leq k+1$

Since $S(2)$ is true, either
$p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$

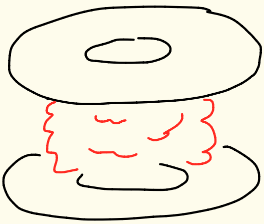
case 1: If $p \mid a_1 a_2 \cdots a_k$, then since $S(k)$ is true, $p \mid a_i$ where $1 \leq i \leq k$

case 2: Otherwise $p \mid a_{k+1}$

Therefore, $p \mid a_i$ for some $1 \leq i \leq k+1$.

Thus, $S(k+1)$ is true.

So, by induction, $S(n)$ is true for all $n \geq 2$. $\blacksquare$



Theorem: (Fundamental Theorem of Arithmetic)

Let $n \in \mathbb{Z}$ with $n \geq 2$.
Then n factors into a product of one or more primes.
Moreover, the factorization is unique apart from the ordering of the prime factors.

Ex: $n = 300$

$$300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$$
$$= 3 \cdot 5 \cdot 2 \cdot 5 \cdot 2$$

same except for the ordering of the prime factors

<u>proof:</u> Let $n \in \mathbb{Z}$, $n \geq 2$.

We proved in a previous class that n factors into a product of one or more primes.

We now prove the uniqueness of such a factoring.

Suppose n factors into two different prime factorizations.

By dividing off the common factors this would give us

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m \quad (*)$$

where $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_m$ are all primes and $p_i \neq q_j$ for all i, j.

Explanation of above:

Suppose

$$n = s \cdot s \cdot t \cdot u \cdot u \cdot w = s \cdot u \cdot y \cdot y \cdot z$$

where s, t, u, w, s, y, z are primes.

Then cancel common factors and get

$$n = s \cdot t \cdot u \cdot w = y \cdot y \cdot z$$

$$\quad\; p_1 \;\; p_2 \;\; p_3 \;\; p_4 = q_1 \;\; q_2 \;\; q_3$$

Equation (*) tells us that
$p_1 \mid q_1 q_2 \cdots q_m$.

The previous theorem tells us that
$p_1 \mid q_j$ for some $1 \leq j \leq m$.

We had a theorem that tells us that since p_1 and q_j are prime and $p_1 \mid q_j$, we must have $p_1 = q_j$ [1/25 pg. 7]

This contradicts the previous page where we said $p_i \neq q_j$ for all i, j.

Therefore, when we factor n into primes, the factorization is unique up to the ordering of the prime factors. $\blacksquare$

Theorem: Let $a, b \in \mathbb{Z}$ with $a, b \geq 1$. Suppose that $\gcd(a,b) = 1$ and $ab = c^n$ where $c, n \in \mathbb{Z}$, $c \geq 1$, $n \geq 1$. Then there exist $d, e \in \mathbb{Z}$, with $d \geq 1$, $e \geq 1$ and $a = d^n$ and $b = e^n$.

proof: Suppose $\gcd(a,b) = 1$ and $c^n = ab$.

If $a = 1$, then set $d = 1$ and $e = c$.
If $b = 1$, then set $d = a$ and $e = 1$.
So for the remainder of the proof suppose $a \geq 2$, $b \geq 2$.

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

Thus, we have that

$$\boxed{\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \\ \text{and} \quad b &= p_{r+1}^{a_{r+1}} p_{r+2}^{a_{r+2}} \cdots p_{r+s}^{a_{r+s}} \end{aligned}}$$

where $p_1, p_2, \ldots, p_{r+s}$ are distinct primes and $a_1, a_2, \ldots, a_{r+s}$ are positive integers with $r \geq 1$, $s \geq 1$.

Ex:

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

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

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

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

Suppose that

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

is the prime decomposition of c where $q_1, \ldots, q_k$ are distinct primes and $b_i \geq 1$.

Since $ab = c^n$ we get that

$$\underbrace{p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} p_{r+1}^{a_{r+1}} \cdots p_{r+s}^{a_{r+s}}}_{ab} = \underbrace{q_1^{nb_1} q_2^{nb_2} \cdots q_k^{nb_k}}_{c^n}$$

By the fundamental theorem of arithmetic the left factorization and right factorization of the above equation are the same.

Thus, $r+s = k$, and the primes q_j are the same as the primes p_j (except for the ordering possibly) and the corresponding exponents are the same.

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

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

And thus

$$a_j = n b_j \quad \text{for} \quad 1 \le j \le r+s.$$

So,

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

$$= (\underbrace{p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}}_{d})^n$$

and

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

$$= (\underbrace{p^{b_{r+1}} p_{r+2}^{b_{r+2}} \cdots p_{r+s}^{b_{r+s}}}_{e})^n$$

Set $d = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$

and $e = p_{r+1}^{b_{r+1}} \cdots p_{r+s}^{b_{r+s}}$ $\blacksquare$

HW 3

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

Ex: $a = 25$, $b = 10$

$$\frac{a}{b} = \frac{25}{10} = \frac{5}{2} = \frac{x}{y}$$

$$\gcd(x,y) = \gcd(5,2) = 1$$

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

Then, $x = \frac{a}{d}$ and $y = \frac{b}{d}$.

We know that $x, y \in \mathbb{Z}$ because $d \mid a$ and $d \mid b$.

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

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

① (d) Let p be prime.
Prove that $\sqrt{p}$ is irrational.

<u>proof:</u> We will prove this by contradiction.

Suppose $\sqrt{p}$ is a rational number.
By part (a), we can write

$$\sqrt{p} = \frac{x}{y} \quad \text{where } x, y \in \mathbb{Z}$$

and $y \neq 0$ and $\boxed{\gcd(x,y) = 1}$.

Squaring both sides gives

$$p = \frac{x^2}{y^2},$$

Or, $\boxed{p y^2 = x^2}$ $(*)$

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

Because p is prime and $p \mid xx$ ☆☆☆

we know $\boxed{p \mid x}$

Thus, $x = p\ell$ where $\ell \in \mathbb{Z}$.

Plug $x = p\ell$ into $(*)$ to get

$$\underbrace{p y^2 = \underbrace{(p\ell)^2}_{x^2}}_{(*)} = p^2 \ell^2$$

☆☆☆ <u>Using</u>
p prime
If $p \mid ab$,
then
$p \mid a$
or
$p \mid b$.

Cancelling gives $y^2 = p\ell^2$.

So, $p \mid y^2$.

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

we know $\boxed{p \mid y}$.

Since $p \mid x$ and $p \mid y$, p is a common divisor of x and y.

But then $\gcd(x,y) \geq p$.

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

Thus, $\sqrt{p}$ is irrational. $\blacksquare$