Math 4460
2/24/25

Topic 3 – Fundamental Theorem of Arithmetic

Previously in Math 4460:

p prime

If $p \mid ab$, then $p \mid a$ or $p \mid b$

Theorem: Suppose p is prime and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, $n \geq 2$

If $p \mid a_1 a_2 \cdots a_n$, then there exists i where $p \mid a_i$ (here $1 \leq i \leq n$)

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

"If $p \mid a_1 a_2 \cdots a_n$ where $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, then there exists i where $p \mid a_i$ and $1 \leq i \leq n$"

We will induct on $n \geq 2$.
We've already proved the base case when $n = 2$:

"If $p \mid a_1 a_2$, then $p \mid a_1$ or $p \mid a_2$"

Let's induct!

Assume $S(k)$ is true for some $k \geq 2$.

Let's show $S(k+1)$ is true.

Suppose $p \mid a_1 a_2 \cdots a_k a_{k+1}$ where $a_1, a_2, \ldots, a_k, a_{k+1} \in \mathbb{Z}$.

Thus, $p \mid (a_1 a_2 \cdots a_k) a_{k+1}$

By $S(2)$ we get either $p \mid a_1 a_2 \cdots a_k$ or $p \mid a_{k+1}$.

<u>Case 1:</u> Suppose $p \mid a_1 a_2 \cdots a_k$.

Since $S(k)$ is true there

exists i where $p \mid a_i$ and $1 \le i \le k$

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

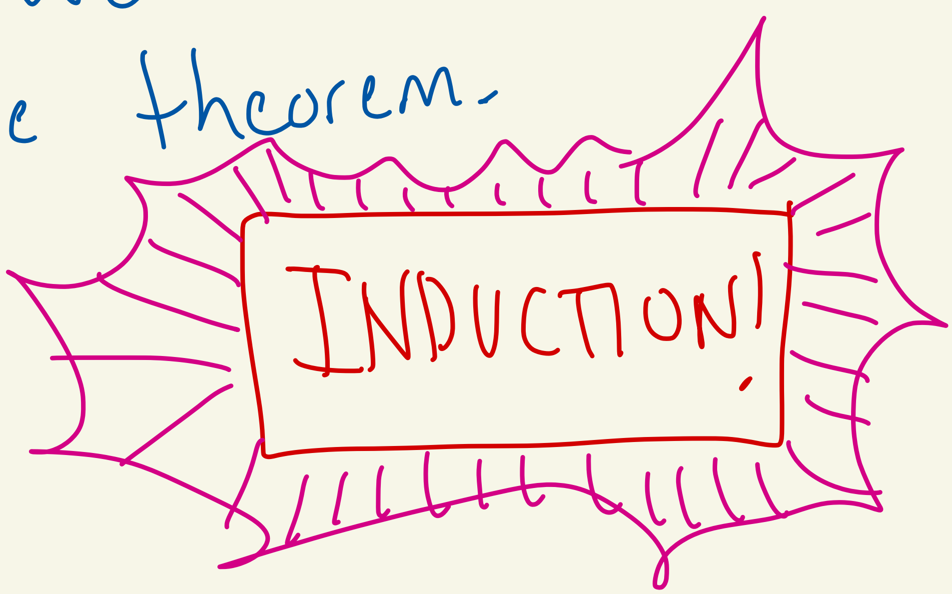
<u>Case 2:</u> Suppose $p \mid a_{k+1}$.

Then, set $i = k+1$.

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

In either case $S(k+1)$ is true.

By the magical powers of induction we have proven the theorem.



Theorem: (FTOA)

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: $n = 300$

$$\left.\begin{aligned} 300 &= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \\ &= 3 \cdot 5 \cdot 2 \cdot 5 \cdot 2 \\ &= 5 \cdot 5 \cdot 3 \cdot 2 \cdot 2 \end{aligned}\right\}$$

Same factorization

Just the ordering of the primes is different

PROOF:

Let $n \in \mathbb{Z}$ with $n \geq 2$.
Previously, we showed that n can be factored as the product of one or more primes.
We now prove the uniqueness of such a factoring.

Suppose, by way of contradiction, that n has two different prime factorizations
By dividing off the common factors this would imply that

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

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

Explanation of above

Suppose n factored in two ways.

$$\left.\begin{aligned} n &= s \cdot s \cdot t \cdot u \cdot u \cdot w \\ n &= s \cdot u \cdot y \cdot y \cdot z \end{aligned}\right\} \text{two factorizations}$$

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

Then,

$$\cancel{s} \cdot s \cdot t \cdot \cancel{u} \cdot u \cdot w = \cancel{s} \cdot \cancel{u} \cdot y \cdot y \cdot z$$

So,

$$\underbrace{s \cdot t \cdot u \cdot w}_{p_1 \cdot p_2 \cdot p_3 \cdot p_4} = \underbrace{y \cdot y \cdot z}_{q_1 q_2 q_3}$$

(Back to proof)

Equation (*) tells us that

$$p_1 \mid q_1 q_2 \cdots q_m$$

By the previous theorem

$$p_1 \mid q_j \text{ for some } 1 \le j \le m.$$

Since q_j is prime either

$$p_1 = 1 \text{ or } p_1 = q_j.$$

We can't have $p_1 = 1$ since p_1 is prime.

So, $p_1 = q_j$

This contradicts the above that said $p_1 \neq q_j$.

Thus, the factorization of n is unique.

$\boxed{\boxed{\boxed{\text{FTOA}}}}$

$\boxed{\text{HW 2}}$ 9

Let $x, y, z \in \mathbb{Z}$ with $x \neq 0$.

Prove: $x \mid yz$ iff $\frac{x}{\gcd(x,y)} \mid z$

$\boxed{\text{Proof:}}$

Let $d = \gcd(x,y)$.

($\Rightarrow$) Suppose $x \mid yz$.

Then, $yz = xk$ where $k \in \mathbb{Z}$.

Divide by d to get

$$\underbrace{\left(\frac{y}{d}\right)}\, z = \underbrace{\left(\frac{x}{d}\right)}\, k$$

$\frac{y}{d}, \frac{x}{d}$ are integers because $d \mid x$ & $d \mid y$

Recall that $\gcd\left(\frac{x}{d}, \frac{y}{d}\right) = 1$
when $d = \gcd(x,y)$.

We have that $\frac{x}{d} \mid \left(\frac{y}{d}\right) z$
and $\gcd\left(\frac{x}{d}, \frac{y}{d}\right) = 1$, so
by another theorem from
class we get that $\frac{x}{d} \mid z$.

If $c \mid ab$ and $\gcd(c,a) = 1$
then $c \mid b$

Done!

($\Leftarrow$) Suppose $\frac{x}{d} \mid z$.

Then, $z = \left(\frac{x}{d}\right) \ell$ where $\ell \in \mathbb{Z}$.

So, $dz = x\ell$.

Since $d = \gcd(x, y)$ we know $d \mid y$.

Thus, $y = dm$ where $m \in \mathbb{Z}$.

Multiply $dz = x\ell$ by m to get $\underbrace{(dm)}_{y} z = x(m\ell)$

So, $yz = x(m\ell)$

Then, $x \mid yz$.

$\blacksquare$