Math 4460
2/22/23

TOPIC 3 – Fundamental theorem of arithmetic

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

<u>Theorem:</u> Suppose p is a 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 $p \mid a_i$ and $1 \leq i \leq n$.

<u>proof:</u> Let p be a prime.
[p is fixed through the proof.]

Let $S(n)$ be the following:

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

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

The base case is when $n=2$.

$S(2)$ says: "If $p \mid a_1 a_2$ where $a_1, a_2 \in \mathbb{Z}$, then $p \mid a_1$ or $p \mid a_2$"

We proved this previously in class,

So, $S(2)$ is true.

Now let $k \geq 2$ where $k \in \mathbb{Z}$.

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

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

Then, $p \mid (a_1 a_2 \cdots a_k) \cdot a_{k+1}$.
Since $S(2)$ is true then 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 by assumption,
there exists i where $p \mid a_i$.
So, $S(k+1)$ is true.

<u>case 2:</u> Suppose $p \mid a_{k+1}$.
Then $S(k+1)$ is true.

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

By the magical powers of induction $S(n)$ is true for all $n \geq 2$.

Induction

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.

$\boxed{\text{Ex:}}$ $n = 300$

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

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

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

these are the same factorizations except for the ordering of the primes

$3 \cdot 100$

$3 \cdot 2 \cdot 50$

$3 \cdot 2 \cdot 2 \cdot 25$

$3 \cdot 2 \cdot 2 \cdot 5 \cdot 5$

Scratchwork

Proof: Let $n \in \mathbb{Z}$, $n \geq 2$.

Previously, we proved that n can be factored as the 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 imply that

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

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 the above

Suppose n factored in two different ways.

$n = s \cdot s \cdot t \cdot u \cdot u \cdot w$ } the two

$n = s \cdot u \cdot y \cdot y \cdot z$ factorizations

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

Then,

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

Cancel common terms to get

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

$$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \qquad q_1 \cdot q_2 \cdot q_3$$

Equation (*) says that

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

Since p_1 is prime, by the previous theorem there exists i where $p_1 \mid q_i$ where $1 \le i \le m$.

Since p_1 and q_i are primes and $p_1 | q_i$ we know $p_1 = q_i$

Contradicting the above where we had $p_1 \neq q_i$

Thus, the factorization of n is unique up to reordering the prime factors. $\blacksquare$

HW 2

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

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

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

Note: $\frac{x}{d}$ is an integer because d divides x

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

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

So, $yz = y\left(\frac{x}{d}\right)k$.

Thus, $yz = x\left(\frac{y}{d}\right)k$.

Note: $y/d \in \mathbb{Z}$ because d divides y

And, $\left(\frac{y}{d}\right)k \in \mathbb{Z}$.

So, $x \mid yz$.

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

Then, $yz = x\ell$ where $\ell \in \mathbb{Z}$.

Divide by d to get

$$\left(\frac{x}{d}\right)\ell = \left(\frac{y}{d}\right)z.$$

Note: $\frac{x}{d}, \frac{y}{d}$ are both integers since $d \mid x$ and $d \mid y$

By a previous theorem, since $d = \gcd(x, y)$ we know that

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

By another previous theorem, since $\gcd\left(\frac{x}{d}, \frac{y}{d}\right) = 1$ and $\frac{x}{d} \mid \left(\frac{y}{d}\right) \cdot z$ we know that $\frac{x}{d} \mid z$.

$\blacksquare$