Last time: We ended with the following lemma. Note, p is always a prime.
Lemma: If $p \mid ab$ then $p \mid a$ or $p \mid b$.
Proof: Suppose that $p \mid ab$ and that $p \nmid a$. Then we want to show that $p \mid b$. If $p \nmid a$, then (as Miranda observed) we have $\gcd(p, a) = 1$: the only factors of p are 1 and p, and p is not a factor of a so the only common factor is 1. Konnor pointed out that Bézout's theorem yields $\exists x, y \in \mathbb{Z}$ such that $px + ay = 1$. Then multiplying by b, $pbx + abr = b$. Since $p \mid pbx$, and $p \mid aby$ since $p \mid ab$, we deduce that $p \mid pbx + aby$, whence $p \mid b$. □

Try this with $a = 10$, $b = 6$, and $p = 3$ to get a feel for the proof!

Corollary: If $p \mid a_1 a_2 \cdots a_n$, then $\exists i$ such that $p \mid a_i$.
Proof: By induction on n. The base case $n = 2$ follows from the Lemma above. For the inductive step, suppose the corollary holds for all $n < k$, then want to show that it holds for k (i.e. that if $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_i$ for some $i \le k$). Alex suggests breaking the product into $a_1 a_2 \cdots a_{k-1}$ and a_k. In other words,

$$\begin{aligned} p \mid a_1 a_2 \cdots a_k &\Rightarrow p \mid (a_1 a_2 \cdots a_{k-1})(a_k) \\ &\Rightarrow p \mid a_1 a_2 \cdots a_{k-1} \text{ or } p \mid a_k \end{aligned}$$

where the last implication is a consequence of our lemma. If $p \mid a_k$, we're done. But if $p \mid a_1 a_2 \cdots a_{k-1}$, then by induction $p \mid a_i$ for $i \le k - 1$, and we're done. □

Proof of the Fundamental Theorem of Arithmetic:
Recall the theorem asserts that any number can be expressed as a product of primes in an essentially unique way. Implicit in this assertion are two separate claims, which we prove one at a time.

Claim 1: Given $n \ge 2$, we can write $n = q_1 q_2 \cdots q_\ell$ where every q_i is prime.
Proof: By induction on n.
The base case $n = 2$: 2 is prime, and $2 = 2$. ✓

Now for the inductive step, suppose that claim 1 holds for all $n < k$, we need to show that it holds for k. Ben suggests the following cases: k is prime and k is composite.

Case 1: Suppose k is prime. Then $k = k$ and we win!

Case 2: Suppose k is composite. Then since k is composite, we can write $k = ab$ where $2 \le a, b < k$. By induction, since $2 \le a, b < k$, we can write each of these as a product of primes. Then k is the product of these products of primes, which means: k is a product of primes!

Claim 2: Given $n \ge 2$, the expression $n = q_1 q_2 \cdots q_\ell$ where the q_i's are all prime, is the unique

way to write n as a product of primes (up to re-ordering).
Proof: By induction on ℓ, the length of the shortest representation of n as a product of primes.
In the base case, $\ell = 1$, Max points out that this means that $n = q_1$, where q_i is prime, so n is prime and cannot be broken up further.

Now suppose that claim 2 holds for all $\ell < m$. We want to prove that if n can be written as a product of m prime factors, then this is the only way (up to re-ordering) to express n as a product of primes. Let

$$n = q_1 q_2 \cdots q_m$$

be a prime factorization of n.

Max-Thomas-Chris + Qiana + Miranda: Any prime factor of n must be one of the q_i.

Indeed, by our Corollary above, if $p \mid n$ then $p \mid q_i$ for some i. But q_i is prime, so its only factors are 1 and q_i. It follows that $p = q_i$.

Qiana's proof of uniqueness: Suppose $n = q_1 q_2 \cdots q_m = p_1 p_2 \cdots p_s$. We know that $s \geq m$ because m is the shortest length. Look at p_1, we know $p_1 \mid n$, so then by the corollary, $p_1 \mid q_1 q_2 \cdots q_m$, so $p_1 = q_i$ for some i. Without loss of generality, let's say $p_1 = q_1$. (We can ensure this by re-labeling the q_i's if necessary). Thus we find

$$\frac{n}{p_1} = q_2 q_3 \cdots q_m = p_2 p_3 \cdots p_s$$

Notice that the number $\frac{n}{p_1}$ has a prime factorization that uses fewer than m prime factors, namely $\frac{n}{p_1} = q_2 q_3 \cdots q_m$. Thus our induction hypothesis guarantees that this is the *unique* prime factorization of $\frac{n}{p_1}$; it immediately follows that $s = m$ and that (upon suitably relabeling the p_i's) we have $p_i = q_i$ for every i. We conclude that n has a unique prime factorization. □

Notation Note: By the FTA, any n can be written as $n = q_1 \cdots q_\ell$. Collecting the repeated primes together, we can express this in the form $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where $p_1 < p_2 < \cdots < p_k$ are distinct primes and $e_i \geq 1$ for every i.

Example: $60 = 2 \times 5 \times 3 \times 2 = 2^2 \times 3^1 \times 5^1$.

A different way to write prime factorizations is

$$n = \prod_p p^{\nu_p(n)},$$

where $\prod_p$ means a product over all primes p and $\nu_p(n)$ is a nonnegative integer for every prime p.

Example: $60 = 2^2 \times 3^1 \times 5^1 \times 7^0 \times 11^0 \cdots$, so then $\nu_2(60) = 2$, $\nu_3(60) = 1$, $\nu_5(60) = 1$, and $\nu_p(60) = 0$ for all $p \geq 7$.

We finished class with the following: Question: What can you say about $\nu_p(ab)$?

Konnor: $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

Proof: Write

$$a = \prod_p p^{\nu_p(a)} \qquad b = \prod_p p^{\nu_p(b)}.$$

Multiplying these prime factorizations we find

$$ab = \prod_p p^{\nu_p(a)+\nu_p(b)}.$$

On the other hand, we have

$$ab = \prod_p p^{\nu_p(ab)}.$$

By the FTA, the prime factorization is unique! This implies that

$$\nu_p(ab) = \nu_p(a) + \nu_p(b)$$

as Konnor claimed. □