Fundamental Theorem of Arithmetic and Divisibility Review Mini Lecture

Here we will provide a proof of the Fundamental Theorem of Arithmetic (about prime factorizations). Before we get to that, please permit me to review and summarize some divisibility facts.

Definition We say b *divides* a and write $b|a$ when there exists an integer k such that $a = bk$.
We also defined $\gcd(a, b)$ to be the largest divisor of both a and b.

Basic Theorems

1. ***Theorem*** (The Division Algorithm)
   For all $a, b \in \mathbb{N}$, there exists $q, r \in \mathbb{N}$ such that $a = bq + r$ and $0 \leq r < b$.

   For the proof we used the well ordering principle to find r, then we gave a proof my contradiction to show $r < b$. See your notes. Note in particular that if $r = 0$, then b divides a.

2. ***Theorem*** For all $a, b, c \in \mathbb{Z}$, $\gcd(a, b) = \gcd(a - bc, b)$.

   For the proof, we showed that any common divisor of a and b is also a common divisor of $a - bc$ and b (and vice versa). This theorem is key as it shows why the Euclidean algorithm works to compute the greatest common divisor.

3. ***Theorem*** (The Euclidean Algorithm) Let $a, b \in \mathbb{N}$ with $a \geq b > 0$ and define $r_0 = a$, $r_1 = b$ and $r_i = q_{i+1}r_{i+1} + r_{i+2}$, where $0 \leq r_{i+2} < r_{i+1}$.
   If $r_n \neq 0$ and $r_{n+1} = 0$ for some n, then $\gcd(a, b) = r_n$.

   For the proof we used the previous theorem over and over again.

4. ***Theorem*** (Bezout's Lemma or the Linear Diophantine Equation Theorem) For all $a, b \in \mathbb{Z}$, not both zero, there exists $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $\gcd(a, b)$ divides c.

   For the reverse direction we proved this using induction to explain why we could back solve through the Euclidean algorithm to find a solution to $ax_1 + by_1 = d$ where $d = \gcd(a, b)$, then we multiplied x_1, y_1, and d by the correct multiple to get c. For the forward direction, we used the fact that $d = \gcd(a, b)$ is a common factor of a and b and substituted into the equation $ax + by = c$ to find that d divides c.

   STRATEGY: Whenever a $\gcd(a, b)$ appears in a theorem, you can immediately say the following in your proof: *Let* $d = \gcd(a, b)$. *By the LDE Theorem, there exists* $x, y \in \mathbb{Z}$ *such that* $ax + by = d$. This can be quite useful as we illustrated in examples.

   Here are several basic consequences that can be proved with the theorems above (you should know how to prove all of these):

   - ***Theorem*** If $c|a$ and $c|b$, then $c|(a + b)$.
   - ***Theorem*** If $\gcd(a, b) = 1$ and $a|bq$, then $a|q$. (This is important!)
   - ***Theorem*** If p is a prime and $p|ab$, then $p|a$ or $p|b$. (This follows from the theorem above).
   - ***Theorem*** If p is a prime and $p|a_1a_2 \cdots a_n$, then p divides at least one of $a_1, a_2, \ldots,$ or a_n. (This follows by induction and the theorem above).

Now for the proving of the fundamental theorem of arithmetic.

Theorem (The Fundamental Theorem of Arithmetic)
For all $n \in \mathbb{N}$, $n > 1$, n can be *uniquely* written as a product of primes (up to ordering).
Another way to say this is, for all $n \in \mathbb{N}$, $n > 1$, n can be written in the form $n = \prod_{i=1}^{r} p_i = p_1 p_2 \cdots p_r$ for some unique set of primes $p_1, p_2, \ldots, p_r$.
Examples: $12 = 2 \cdot 2 \cdot 3$, $75 = 3 \cdot 5 \cdot 5$, $90 = 2 \cdot 3 \cdot 3 \cdot 5$, $13 = 13$, $15 = 3 \cdot 5$.

Proof: We must show two things. First that such a factorization into primes *exists*, then we must show the factorization is *unique*.

We will use a contradiction proof and the well-ordering principle to prove existence. Assume there exists $n \in \mathbb{N}$, $n > 1$ that have CANNOT be written as a product of primes. By the well-ordering principle, there is a natural number, call it $n_0 > 1$, that cannot be written as a product or primes.

The number n_0 cannot be a prime number because otherwise it would be it's own prime factorization and we're assuming n_0 can't be factored into primes. Hence, n_0 is composite. That means that n_0 has some divisor a strictly between 1 and n_0. Hence $n_0 = ab$ for some integers a and b where $1 < a < n_0$ (and therefore $1 < b < n_0$). Since n_0 is the smallest example that cannot be factored into primes and a and b are smaller, a and b must have prime factorizations. Thus, we can write $a = p_1 p_2 \cdots p_u$ and $b = q_1 q_2 \cdots q_v$ for some primes p_i and q_j. But that means that $n_0 = ab = p_1 p_2 \cdots p_u q_1 q_2 \cdots q_v$ is a product of primes which is a contradiction. Therefore our original assumption is wrong. Hence, all integers $n \in \mathbb{N}$, $n > 1$ CAN be written as a product of primes.

Now we show uniqueness. Let $n \in \mathbb{N}$, $n > 1$ and assume $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$ are two prime factorizations of n. We will show that these factorizations must be the same. Since both of these factorizations are equal to n we have $p_1 p_2 \cdots p_r = n = q_1 q_2 \cdots q_s$. Assume that the factorizations are different. After canceling all the common factors from both sides, some sets of different primes will remain on each side (or else the factorizations would be the same), say: $p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$. If p is one of the primes on the left-hand side, then by definition of divisibility p divides $q_{j_1} q_{j_2} \cdots q_{j_v}$. Since p is a prime, using the theorem from above, p must divide at least one of prime, call it q, from $q_{j_1}, q_{j_2}, \cdots$, or q_{j_v}. But if p is a prime and q is a prime and p divides q, then $p = q$ (because nothing divides a prime besides one and itself). But this contradicts the fact that the primes on each side were different. Thus, all the factors on each side must be the same. $\square$

Here is an alternate proof of existence using Strong Induction (I only show you this so that you have another example of strong induction and how it can be used).

Theorem For all $n \in \mathbb{N}$, $n > 1$, there exists a primes factorization of n.
Proof: We use strong induction on n.
BASE STEP: The number $n = 2$ is a prime, so it is it's own prime factorization.
INDUCTIVE STEP: Assume $i = 2, \cdots, k$ all have prime factorizations for some $k \geq 2$.
If $k + 1$ is a prime, then it is it's own prime factorization (and we would be done).
If $k + 1$ is not a prime, then $k + 1$ has some divisor a strictly between 1 and $k + 1$. Hence $k + 1 = ab$ for some integers a and b where $1 < a < k + 1$ (and therefore $1 < b < k + 1$). By the strong inductive hypothesis (twice), a and b must have prime factorizations. Thus, we can write $a = p_1 p_2 \cdots p_u$ and $b = q_1 q_2 \cdots q_v$ for some primes p_i and q_j. And by substitution, $k + 1 = ab = p_1 p_2 \cdots p_u q_1 q_2 \cdots q_v$ is a prime factorization of $k + 1$.
Hence, in all cases, $k + 1$ can be factored into primes.
Thus, by the principle of strong induction, a prime factorization exists for all integers $n > 1$. $\square$