I don't think I presented the proof of the unique prime factorisation theorem very well in the lectures, so I've written it out more clearly (hopefully) here.

Theorem 1 (Unique prime factorisation theorem)**.** *Any positive integer n can be expressed uniquely as a product of prime numbers.*

Proof. Existence: Strong induction on n: when $n = 1$, n can be expressed as an empty product of prime numbers.

Now suppose that every $m < n$ can be expressed as a product of prime numbers. Either n is prime, or it can be written as $n = ab$ where $a \geqslant 2$ and $b \geqslant 2$ are positive integers. In the first case, n can be written as the product of one prime – $n = n$. In the second case, since $a > 1$, $b < ab = n$, and similarly, $a < n$, so by our induction hypothesis, a and b can be expressed as products of prime numbers. Suppose $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b = q_1^{\beta_1} \cdots q_l^{\beta_l}$. Then n has a prime factorisation $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$.

Therefore, by strong induction, every positive integer can be expressed as a product of primes.

Uniqueness: For this we need the following lemma:

Lemma 1. *For any prime number p, and any positive integers a and b, if $p|ab$, then either $p|a$ or $p|b$.*

Proof. Suppose $p|ab$, but p does not divide a. We need to show that $p|b$. Since p is prime, its only positive factors are p and 1. Therefore, since (p, a) divides p, it must be 1 or p. However, (p, a) must also divide a, so it cannot be p. Therefore, it must be 1. Using Euclid's algorithm, we can find integers x and y such that $px + ay = 1$. Therefore, $pxb + aby = b$. However, p divides both pxb and aby, so it divides their sum, which is b. □

We can extend this to arbitrary products by induction:

Lemma 2. *For any prime number p, and any collection of positive integers $a_1, \ldots, a_n$ such that $p|a_1 \cdots a_n$, there is some i such that $p|a_i$.*

Proof. Induction on n. If $n = 0$, p won't divide the product, since the empty product is 1. If $n = 1$, then the result is trivial – it just says that if $p|a_1$, then $p|a_1$.

Now suppose the lemma holds for some value of n. We want to show that whenever $p|a_1 \cdots a_{n+1}$, we must have $p|a_i$ for some $1 \leqslant i \leqslant n + 1$. Using the previous lemma, we note that since $p|(a_1 \cdots a_n)a_{n+1}$, we must have either $p|a_1 \cdots a_n$, or $p|a_{n+1}$. In the first case, by our induction hypothesis, p must divide one of $a_1, \ldots, a_n$, so in either case, p must divide one of $a_1, \ldots, a_{n+1}$. □

Now we can prove uniqueness by strong induction on n. When $n = 1$, it is clear, because if there are any primes in the product, then it will be more than 1, so only the empty product of primes can equal 1.

Now suppose that for every $m < n$, the prime factorisation of m is unique up to order of multiplication, and suppose that we have two prime factorisations $n = p_1 \cdots p_k$ and $n = q_1 \cdots q_l$ (where some p_i and q_i may be repeated). By the above lemma, p_1 must divide one of $q_1, \ldots, q_l$, since it divides their product. However, since $q_1, \ldots, q_l$ are all prime, if $p_1 | q_i$, we must have $p_1 = q_i$ (since $p_1 \neq 1$). Now let $m = \frac{n}{p_1}$. We have $m = p_2 \cdots p_k$, and $m = q_1 \cdots q_{i-1} q_{i+1} \cdots q_l$. Since $p_1 > 1$, $m < n$, so by our induction hypothesis, the prime factorisation of m is unique. Therefore, $p_2, \ldots, p_k$ must be $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_l$ in some order. This means that the two factorisations of n must be the same up to the order of the factors. $\square$