The Fundamental Theorem of Arithmetic.

The **Fundamental Theorem of Arithmetic** says that every integer > 1 can be factored uniquely into a product of powers of primes. I will prove this result in two steps: the existence part and the uniqueness part.

Theorem. Every integer > 1 can be factored into a product of powers of primes.

Proof. I will use Well-Ordering; this will be a proof by contradiction. Suppose that there is an integer > 1 which cannot be expressed as a product of powers of primes. By Well-Ordering, there is a *smallest* integer $n > 1$ which cannot be expressed as a product of powers of primes.

If n is prime, it is a product of powers of primes: itself! So n is not prime, and I can find integers a and b, where $1 < a, b < n$ and $n = ab$. Now a and b are less than n, and n was the smallest integer > 1 which cannot be expressed as a product of powers of primes. Hence, a and b *can* be expressed as a product of powers of primes. But since $n = ab$, the same is true for n. $\times$

Therefore, there is no integer > 1 which *cannot* be expressed as a product of powers of primes. So every integer > 1 *can* be expressed as a product of powers of primes. $\square$

In order to prove that the decomposition into primes is unique, I will prove a result which is important in its own right.

Lemma. Let p be a prime, and suppose $p \mid x_1 \cdots x_n$, where $x_i \in \mathbb{Z}$. Then $p \mid x_i$ for some i.

In other words, if a prime divides a product, it must divide one of the factors.

Proof. I'm going to prove this by induction. The result is trivial for $n = 1$; I will start the induction with $n = 2$.

Suppose, then, that $p \mid x_1 x_2$. I want to show p divides x_1 or p divides x_2. Suppose that $p \not| x_1$. I must show $p \mid x_2$.

I claim that $p \not| x_1$ means that p and x_1 are relatively prime. Why? Well, if $d > 0$ divides p and x_1, then d is either 1 or p, since p is prime. But $p \not| x_1$, so d can't be p. Hence, $d = 1$. In other words, the only positive common divisor of p and x_1 is 1. Therefore, $(p, x_1) = 1$ as I claimed.

The greatest common divisor of two numbers is a linear combination of the numbers, so

$$1 = ap + bx_1 \quad \text{for some } a, b \in \mathbb{Z}.$$

Multiply by x_2:

$$x_2 = apx_2 + bx_1x_2.$$

Now $p \mid apx_2$ and $p \mid bx_1x_2$ (because $p \mid x_1x_2$), so $p \mid x_2$. This was what I wanted to prove.

Now that I have the induction started, I will do the induction step. Suppose $n > 2$ — I have more than two x's — and suppose the result is true when I have fewer than n factors. Suppose $p \mid x_1 \cdots x_n$; I must show that p divides one of the x's.

Well, $p \mid (x_1 \cdots x_{n-1})x_n$; the right side is a product of two things $(x_1 \cdots x_{n-1})$ and x_n), so p must divide one of them, by induction. If $p \mid x_n$, I have p dividing one of the x's, and I'm done.

Otherwise, $p \mid x_1 \cdots x_{n-1}$. But the induction hypothesis says that the result holds for fewer than n factors, and I have $n - 1$ here. Therefore, p divides one of $x_1, \ldots, x_{n-1}$.

In either case, then, I've shown that p divides one of the x's. This completes the induction step, and the proof. $\square$

Theorem. Let $p_1, \ldots, p_m$ be distinct primes. Let $q_1, \ldots, q_n$ be distinct primes. Let $i_1, \ldots, i_m, j_1, \ldots, j_n$ be integers ≥ 1. Suppose

$$p_1^{i_1} \cdots p_m^{i_m} = q_1^{j_1} \cdots q_n^{j_n}.$$

Then $m = n$, and for each k, $1 \leq k \leq m$, there is an l, $1 \leq l \leq n$, such that $p_k^{i_k} = q_l^{j_l}$.

Proof. I will induct on the length of the smaller of the two decompositions. Suppose without loss of generality that $m \le n$ — that is, if there are more terms on one side, it is the right side.

In the case $m = 1$, I have

$$p^i = q_1^{j_1} \cdots q_n^{j_n}.$$

Now $p \mid q_1^{j_1} \cdots q_n^{j_n}$, so by the preceding Lemma p divides one of the prime powers on the right. Assume without loss of generality that $p \mid q_1^{j_1}$. Again by the preceding lemma, $p \mid q_1$. Since p and q_1 are prime, $p = q_1$.

If $i > j_1$, then I cancel $p^{j_1} = q_l^{j_1}$ off both sides to obtain

$$p^{i-j_1} = q_2^{j_2} \cdots q_n^{j_n}.$$

Now p divides the left side, but does not divide the right. $\times$

If $i < j_1$, then I cancel $p^i = q_1^i$ off both sides to obtain

$$1 = q_1^{j_1 - i} \cdots q_n^{j_n}.$$

Now q_1 divides the right side, but does not divide the left. $\times$

The only possibility, then, is that $i = j_1$. I cancel $p^i = q_1^{j_1}$ off both sides, leaving

$$1 = q_2^{j_2} \cdots q_n^{j_n}.$$

If there really are any q's on the right, then there is a prime dividing the right side but not the left. $\times$So there are no primes on the right side: q_l must have been the only prime on the right side to begin with. That means the original equation was $p^i = q_1^{j_1}$, with $p = q_1$ and $i = j_1$. This establishes the result for $m = 1$.

Now suppose $m > 1$, and suppose the result is true if the smaller number of terms is less than m. Suppose

$$p_1^{i_1} \cdots p_m^{i_m} = q_1^{j_1} \cdots q_n^{j_n}.$$

p_m divides the right side, so by the preceding Lemma it divides one of the prime powers on the right. Assume without loss of generality that $p_m \mid q_n^{j_n}$. Again by the preceding lemma, $p_m \mid q_n$, so $p_m = q_n$.

Arguing as in the case $m = 1$, I find that i_m must equal j_n. Cancel $p_m^{i_m} = q_n^{j_n}$ off both sides. The equation is now

$$p_1^{i_1} \cdots p_{m-1}^{i_{m-1}} = q_1^{j_1} \cdots q_{n-1}^{j_{n-1}}.$$

Now I have a decomposition with fewer than m terms on the left, so by the induction hypothesis, these two decompositions are the same. Since I already know that $p_m = q_n$ and $i_m = j_n$, the original decompositions are the same as well. □