The Fundamental Theorem of Arithmetic

The fundamental theorem of arithmetic states that every natural number n is either a prime number, or else it can be decomposed into prime factors $n = p_1^{\alpha_1} * p_2^{\alpha_2} * \ldots * p_k^{\alpha_k}$ in one and essentially only one way, if we ignore the order of the prime factors. This theorem was known to the ancients; it is found in Euclid's *Elements*. It was very well-known and accepted as proven for more than two thousand years, even though Euclid's proof was incomplete. Carl Friedrich Gauss gave the first complete proof of this theorem in his *Disquisitiones Arithmetica*, first published in 1801.

Perhaps the reason nobody bothered to prove this theorem rigorously for so long is that it seems intuitively obvious. Or maybe it's because Euclid was held in such high regard by all the mathematicians who came after him. We lay the groundwork for a formal proof with a couple of definitions. A natural number m is said to be a *divisor* of n if and only if there exists some natural number q such that $qm = n$. A natural number p is said to be a *prime number* if and only if its only divisors are p itself, and unity. (1 is not generally regarded as a prime number; most authors take 2 to be the smallest prime.)

The proof that every natural number greater than unity is either prime, or the product of primes, is by induction on k. Clearly the theorem is true when $k = 2$, because 2 has no divisors besides 1 and 2; 2 is therefore a prime number. If $k + 1 > 2$, then either $k + 1$ is prime, or it is not prime. If it is prime, the theorem is true. If it is not prime, then it must have a divisor d that is less than $k + 1$. and the induction is complete.

Now we must show that the decomposition of n into prime factors is unique, except for the order of the factors. Suppose that we are given two purportedly different decompositions of n into prime factors, $n = p_1 * p_2 * p_3 * \ldots * p_k = q_1 * q_2 * q_3 * \ldots * q_j$. Since p_1 is a divisor of n, p_1 is also a divisor of $q_1 * q_2 * q_3 * \ldots * q_j$ (because the product of the $q_i = n$). But if p_1 divides $q_1 * q_2 * q_3 * \ldots * q_j$ it must divide at least one of the q_i; otherwise, by the division algorithm, $q_1 * q_2 * q_3 * \ldots * q_j / p_1$ would leave a non-zero remainder, contradicting the fact that p_1 divides n. So p_1 divides one of the q_i. Since we can shuffle the factors q into any order we like without changing the product, let's set $i = 1$, i.e., p_1 divides q_1. But the q_i are prime numbers by hypothesis, and have no divisors except themselves and unity. Since p_1 divides q_1, $p_1 = q_1$. Repeating this argument for $p_2, p_3, \ldots, p_k$ completes the proof.

An historical note: In 1843 Ernst Eduard Kummer, a German mathematician, devised what he thought to be a proof of Fermat's Last Theorem (that the equation $x^n + y^n = z^n$ has no solutions in integers if $n > 2$). He showed this "proof" to another mathematician, Peter Gustav Lejeune Dirichlet, who found an error: Kummer had assumed that the fundamental theorem of arithmetic held in certain algebraic fields of complex numbers, when in fact unity itself could be expressed as the product of factors (other than 1) in those complex algebraic number fields; in other words, there were no "prime numbers" in those fields of algebraic numbers, so the fundamental theorem of arithmetic did not hold in that context. Kummer was motivated to rescue his proof; he subsequently invented the notion of "ideals" in algebraic number theory, and so was able to prove Fermat's Last Theorem for all exponents n except those divisible by an "irregular" prime. The concept of an "ideal" is now central to algebraic number theory. But that's a topic for another day.