The Fundamental Theorem of Arithmetic

Problem

#####Theorem (the Fundamental Theorem of Arithmetic)

Every integer greater than 1 can be expressed as a product of primes. Moreover, this product is unique up to reordering the factors.

This is a really important theorem—that's why it's called "fundamental"! It tells us two things: existence (there *is* a prime factorisation), and uniqueness (the prime factorisation is unique). Both parts are useful in all sorts of places.

The existence part is useful because it tells us that the primes are somehow the "building blocks" from which all integers are made, and this helps with lots of things.

The uniqueness part is useful because it allows us to do certain things that would otherwise not be possible. For example, if we know the prime factorisation of n, then we know the prime factorisation of n^2, safe in the knowledge that n^2 can't also have some other prime factorisation.

Note that the fundamental theorem of arithmetic is one good reason why it's convenient to define 1 not to be a prime. If it were prime, then we could include as many factors of 1 as we liked in the prime factorisation of a number to get lots of different (but not interestingly different) factorisations.

The statements below can be sorted into a proof of the Fundamental Theorem of Arithmetic. You might want to print them out and cut them up to rearrange them.

Say $n = p_1 \cdots p_k = q_1 \cdots q_l$, where $p_1, \dots, p_k, q_1, \dots, q_l$ are primes, not necessarily distinct.

Then we can cancel these primes from the products.

Uniqueness

So n is composite, say $n = ab$ with $1 < a, b < n$.

Since $q_1, \ldots, q_l$ are prime, we must have $p_1 = q_r$ for some r.

If the result is not true, then there must be a *minimal counterexample*.

Suppose that some number n has two prime factorisations.

Since a and b are smaller than n, they have prime factorisations.

We can continue in this way.

Then $p_1 \mid q_1 \cdots q_l$ and p_1 is prime, so $p_1 \mid q_1$ or $p_1 \mid q_2$ or … or $p_1 \mid q_l$.

So the products must in fact be the same.

So there is not a counterexample—the result is true.

Existence

So n is not prime.

That is, there is a smallest number that doesn't have a prime factorisation, say n.

But then n has a prime factorisation: the product of the prime factorisations of a and b.

Any prime has a prime factorisation.

Relevance

NA3 What are highest common factors and why do they matter?