Standard proof of FTA

We will prove that every integer has a unique prime factorization.

$$n = p_1 \cdot p_2 \ldots p_i$$

In this list of prime factors, a factor may be repeated. For example $12 = 2 \cdot 2 \cdot 3$.

This is our version of the standard proof of the theorem. A preliminary result that is needed for this version is called Euclid's lemma, which depends on yet another preliminary result.

Euclid's lemma

Every positive integer greater than 1 is either prime, or it is the product of two smaller natural numbers a and b.

But the same is true of a and b in turn. So every $n = ab$ is the product of the prime factors of a times the prime factors of b.

Suppose that a given prime p divides $n = ab$, i.e. $p|n$.

Then $p|a$ or $p|b$, or both.

proof of Euclid

The proof depends on Bézout's identity (or lemma), which we look at elsewhere. Bézout says that for $a, p \in \mathbb{N}$, there exist integers r and s

such that

$$ra + sp = d$$

where d is the greatest common divisor of a and p.

Of course, if p is prime, then

$$ra + sp = 1$$

Suppose that $p|n = ab$ but p does not divide a so that $\gcd(p, a) = 1$.

Then, we can find a linear combination of a and p in the integers such that:

$$ra + sp = 1$$

But then,

$$b(ra + sp) = b$$

$$rab + spb = b$$

Since $p|p$ and $p|ab$ (by hypothesis), $p|b$, as desired.

(If $p|m$ then $m = jp$ for some (integer) j, similarly if $p|n$ then $n = kp$ for some k so $m + n = (j + k)p$ which means that $p|m + n$).

example

Note that this is not necessarily true for non-primes. For example, $6 \cdot 10 = 60|4$ but neither $6|4$ nor $10|4$. This happens because 2 is a prime factor of both 6 and 10, generating a factor of 4 in the product.

another proof of Euclid, by contradiction

The proof is by contradiction. Suppose p is prime and and $p|ab$ but p divides neither a nor b.

Because a and p are co-prime, Bezout says that there exist integers x and y such that:

$$ax + py = 1$$

similarly (because b and p are co-prime) there exist X and Y such that:

$$bX + pY = 1$$

so

$$1 = (ax + py)(bX + pY)$$
$$1 = axbX + axpY + pybX + p^2yY$$
$$1 = ab(xX) + p(axY + ybX + pyY)$$

Since $p|ab$, p divides the right hand side, so p divides the left-hand side, that is, $p|1$. But this is absurd.

Therefore, p divides at least one of a and b.

proof of FTA by induction

Assume the lemma is true for all numbers between 1 and n. It is certainly true for $n < 31$, because we can check each case.

If n is prime there is nothing to prove and we move to $n + 1$.

If n is not prime, then there exist integers a and b (with $1 < a \leq b < n$) such that $n = a \cdot b$.

By the induction hypothesis, since $a < n$ and $b < n$, a has prime factors $p_1 \cdot p_2 \dots$ and b has prime factors $q_1 \cdot q_2 \dots$ so

$$n = ab = p_1 \cdot p_2 \dots q_1 \cdot q_2 \dots$$

This shows there exists a prime factorization of n.

uniqueness

To show that the prime factorization is unique, suppose that n is the smallest integer for which there exist two different factorizations:

$$n = p_1 \cdot p_2 \dots p_i$$

and

$$n = q_1 \cdot q_2 \dots q_j$$

Pick the first factor p_1. Since p_1 divides $n = q_1 q_2 \dots$, by Euclid's lemma, it must divide some particular q_j. Rearrange the q's to make that q the first one.

But since p_1 divides q_1 and both are prime, it follows that $p_1 = q_1$.

As wikipedia says now:

> This can be done for each of the m p_i's, showing that $m \leq n$ and every p_i is some q_j. Applying the same argument with the p's and q's reversed shows $n \leq m$ (hence $m = n$) and every q_j is a p_i.

$\square$