Fundamental Theorem of Arithmetic

First Step (Prop 10.1 pg 186)

Recall that, if a and b are natural numbers, there are integers k and l so that

$$\gcd(a,b) = ak + bl.$$

Proposition: Suppose that $n \geq 2$ and that $a_1, \ldots, a_n$ are n integers. Let p be a prime number. If $p|(a_1 \cdot a_2 \cdots a_n)$ then p divides at least one of the a_i.

Proof:

If $a_1 \cdots a_n = pk$ for some k then one of $a_i = pk'$ for some k'! e.g: $7 \mid 21 \cdot 16 \Rightarrow 7 \mid 21$.

Proof by induction. We must show that if $p|a_1 a_2$ then $p|a_1$ or $p|a_2$.

Note: $\gcd(p, a_1)$ has 2 possibilities. Either $\gcd(p,a_1) = p$ or $\gcd(p,a_1) = 1$. If it's p, then $p|a_1$ so we are done. If $\gcd(p,a_1) = 1$ we can find k, l so that

$$\gcd(a_1,p) = 1 = pk + a_1 l.$$

$$\therefore \quad a_2 = pa_2 k + a_1 a_2 l$$

Since $p | a_1 a_2$, $a_1 a_2 = pS$

$$a_2 = pa_2 k + pSl = p(a_2 k + Sl)$$

so $p|a_2$.

Now suppose that, if $p|a_1 \cdots a_n$, then $p|a_i$ for some i.

We must show that if $p | a_1 \cdots a_n a_{n+1}$ then $p|a_i$ for some i.

But $p|(a_1 \cdots a_n)a_{n+1}$ so by the case $n=2$ either $p|a_{n+1}$ or $p|(a_1 \cdots a_n)$. By inductive hypothesis, $p|a_i$ for some i. This finishes proof.

Second Step (Theorem 10.1, page 192)

Proposition: Any integer $n > 1$ has a unique prime factorization, meaning it can be written as a product of prime numbers, and any two such products differ only up to the order of the factors.

Step 1: Every ~~integer~~ natural number has a prime factorization (strong induction).

Proof: $n = 2$ is prime so it has a prime factorization.

Suppose all integers from $2, \ldots, n$ have prime factorizations.

Consider $n+1$. Either $n+1$ is prime, so it has a prime factorization, or $n+1 = ab$ where $2 \le a, b \le n$.

By strong induction $a = p_1 \cdots p_r$ and $b = q_1 \cdots q_s$ where p_i, q_j are primes.

$\therefore n+1 = p_1 \cdots p_r \cdot q_1 \cdots q_s$ is too.

Step 2: The prime factorization is unique (minimal counterexample).

Assume that there is some integer which has 2 different prime factorizations. Pick the smallest such integer n.

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

all p_i, q_j are prime.

Now $p_1 | n$ so $p_1 | q_1 \cdots q_s$.

Therefore there is some q_j, $1 \le j \le s$, so that $p_1 | q_j$ so $p_1 = q_j$.

omitted q_j

$$n_1 = n/p_1 = p_2 \cdots p_r = q_1 \cdots q_{j-1} q_{j+1} \cdots q_s$$

$n_1 < n$ so it has a unique factorization.

$$q_1, q_2, \cdots q_{j-1}, q_{j+1}, \cdots q_s \longleftrightarrow p_2, \cdots p_r.$$

$$n_1 = p_2 \cdots p_r$$

$$n = p_1 p_2 \cdots p_r = \underset{p_1}{q_j} \underbrace{(q_1 \cdots q_{j-1} q_{j+1}, \cdots q_s)}^{p_2 \cdots p_r}$$

This a contradiction of assumption that n is the minimal natural number that doesn't have a unique factorization. Conclude: all natural numbers have a unique factorization