The Fundamental Theorem of Arithmetic

The main objective of this section is to prove the following result, which justifies the expression ‘the primes are the building blocks of the integers’.

**Theorem**
(The Fundamental Theorem of Arithmetic)

Let $n \neq 0, 1$ be an integer. Then $n$ has a prime factorization of the form

$$n = \pm (p_1)^{a_1} \ldots (p_r)^{a_r} \quad i \geq 1,$$

where the $p_i$ are distinct prime numbers. Furthermore, up to the order of the $p_i$, this factorization is unique.

We remark that, however familiar this statement sounds, it is non-trivial. Suppose, for example, that instead of the integers, we work with only with the even integers. In this setting, the numbers 6, 10, 30, 50
are ‘primes’, in the sense that they cannot be decomposed into a product of smaller even numbers. Moreover, we have $300 = 10 \cdot 30 = 6 \cdot 50$, showing that the number 300 has two different ‘prime decompositions’ in the universe of even numbers.

To prove the FTA some preparation is required.

**Lemma** Let $a, b$ satisfy $(a, b) = 1$. If $a \mid bc$, then $a \mid c$.

**Proof:** By hypothesis, there exists $k$ such that $bc = ak$. We also have $(a, b) = 1 = ax + by$ for integers $x$ and $y$. Then $c = cax + cbx = a(cx) + (ak)y = a(cx + ky)$ so that $a \mid c$ as required.

**Remark** The condition $(a, b) = 1$ in the Lemma is necessary. Indeed, if $a = 6$, $b = 3$ and $c = 4$ we have
Corollary. Let $a_1, \ldots, a_n$, $p$ be integers with $p$ prime. If $p|a_1 \cdots a_n$ then $p|a_i$ for some $i$.

Proof. We will use induction on the number $n$ of integers $a_i$.

Let $n=1$. If $p|a_1$, then $p|a_i$ for $i=1$.

Induction Hypothesis: Assume that, for any $n$ integers $a_1, \ldots, a_n$, if $p|a_1 \cdots a_n$ then $p|a_i$ for some $i$.

We consider now $n+1$ integers $a_1 \cdots a_n a_{n+1}$. Suppose $p|a_1 \cdots a_n a_{n+1} = (a_1 \cdots a_n) \cdot a_{n+1}$. If $(p, a_1, \ldots, a_n) = 1$.

Then, by the Lemma, we have $p|a_{n+1}$. Suppose now $(p, a_1, \ldots, a_n) \neq 1$. Since $p$ is prime, we have $p|a_1 \cdots a_n$ and, by the induction hypothesis, we have $p|a_i$ for some $i=1, \ldots, n$ as desired.

Proof of FTA. The proof is divided into two parts. Namely, we first prove that a prime factorization exists and then we show this factorization is unique.
For $n < 1$ the result follows from the factorization of $-n$. Let $n > 1$ be an integer.

**Existence.**

If $n$ is prime, then taking $p_1 = n$ and $a_1 = 1$ gives the desired factorization.

Suppose $n$ is composite. For contradiction, suppose $n$ is the smallest integer without a prime decomposition.

We have

$$n = a \cdot b \text{ with } 1 < a, \ b < n,$$

and, by minimality of $n$, we have $a = p_1 \ldots p_k$ and $b = q_1 \ldots q_t$ where the $p_i$ and $q_j$ are primes. (Here we allow repetition of primes in these factorizations.) Thus

$$n = a \cdot b = p_1 \ldots p_k \cdot q_1 \ldots q_t,$$

is a prime factorization for $n$, a contradiction.

**Uniqueness.**
Suppose \( n = p_1 \ldots p_s = q_1 \ldots q_t \) are two prime decompositions of \( n \). After cancelling common factors and relabeling the remaining primes, we obtain

\[
p_1 \ldots p_s' = q_1 \ldots q_t' \quad \text{with} \quad 0 \leq s' \leq s, \quad 0 \leq t' \leq t.
\]

We will now show by contradiction that \( s' = t' = 0 \). This means that the previous equality is \( 1=1 \); that is, the initial decompositions of \( n \) are the same up to ordering of the prime factors. Indeed, suppose there is at least one prime on the left side, that is \( s' \geq 1 \) and \( p_1 \neq 1 \). Then, \( t' \geq 1 \) and \( p_i \neq q_j \) for all \( i, j \) since common primes were cancelled out. Moreover, since \( p_1 \) divides the product on the right hand side, by the Corollary, we have \( p_1 | q_j \) for some \( j \). Since \( q_j \) is prime, we must have \( p_1 = q_j \), contradicting the fact that \( p_i \neq q_j \) for all \( i, j \). Thus \( s' = t' = 0 \).

**Example**

\[
756 = 2 \cdot 378 = 2 \cdot 2 \cdot 189 = 2 \cdot 2 \cdot 3 \cdot 63 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 3 \cdot 3 = 2^2 \cdot 3^3 \cdot 7.
\]
Proposition 8. Let $n \in \mathbb{Z} > 0$ have prime factorization $n = p_1^{a_1} \cdots p_n^{a_n}$. Suppose that $d \mid n$. Then, the prime factorization of $d$ is of the form

$$d = p_1^{b_1} \cdots p_n^{b_n} \text{ with } 0 \leq b_i \leq a_i.$$ 

Proof. Let $n > 0$ and $d \mid n$. We have $n = dk$ for some integer $k$. Clearly, any prime divisor of $d$ is a prime divisor of $n$, so $d = p_1^{b_1} \cdots p_n^{b_n}$ with $b_i \geq 0$. Without loss of generality suppose that $b_1 > a_1$. Then, $b_1 - a_1 \geq 1$ and

$$n = dk \iff p_1^{a_1} \cdots p_n^{a_n} = (p_1^{b_1} \cdots p_n^{b_n})k \iff p_2^{a_2} \cdots p_n^{a_n} = p_1^{b_1-a_1+1} p_2^{n_2} \cdots p_n^{n_k k},$$

showing that $p_1$ divides the left hand side, which is impossible because the $p_i \neq p_1$ for all $i \geq 2$. Thus, $b_1 \leq a_1$, as desired.