FUNDAMENTAL THEOREM OF ARITHMETIC

SECOLINSKY

The Fundamental Theorem of Arithmetic is important when beginning to study number theory and so deserves rigorous development. The proof of the FTA is accessible and requires a simple lemma about prime divisibility.

Lemma 1. *Let p be prime and $a_1, ..., a_n \in \mathbb{Z}$. Then $p|a_1 \cdots a_n \Rightarrow p|a_1 \vee \cdots \vee p|a_n$.*

Proof. Consider the set $S \subset \mathbb{Z}_+$ of all positive integers n for which the lemma holds true. Obviously $1 \in S$. The fact that $2 \in S$ is known as Euclid's lemma. It will not be expounded but instead be left as an exercise. So do assume that $2 \in S$ and that $n \in S$. It then follows that $p|(a_1 \cdots a_n)a_{n+1}$ implies $p|a_1 \vee \cdots \vee p|a_{n+1}$. Thus $n+1 \in S$. Therefore $S = \mathbb{Z}_+$. □

So the lemma says that for a prime which divides a product of integers, we have that such a prime will divide at least one of the factors. Now to use this result.

Theorem 1 (FTA)**.** $(\forall n \in \mathbb{Z}_+)(n > 1 \Rightarrow n$ *is prime or a unique product of primes*$)$.

Proof. Let $S = \{x \in \mathbb{Z}_+ \backslash \{1\} : x$ is prime or a product of primes$\}$. We'll first show that for all integers $n > 1$, $n \in S$. Obviously $2 \in S$ since 2 is prime. Using the Strong Induction Principle, assume $2, ..., n-1 \in S$. If n is prime, then $n \in S$.

Otherwise, n is composite and so we let $n = ab$ where $1 < a < n$ and $1 < b < n$. Now a and b can be expressed as a product of primes and thus n too. Hence $n \in S$. Therefore $S = \{x \in \mathbb{Z}_+ : x \geq 2\}$.

Now we'll need to show that for all composite numbers $n \in S$, n can be expressed uniquely as a product of primes. It'll be shown by contradiction. Assume to the contrary that $p_1 \cdots p_r = q_1 \cdots q_s$ where all common factors of n have been cancelled out so that $p_i \neq q_j$ for any i, j. Since $p_1|q_1 \cdots q_s$ and p_1 is prime, $p_1|q_j$ for some $1 \leq j \leq s$. But q_j is prime too so that it must be that $p_1 = q_j$, a contradiction. □

The FTA is used in the proofs of many statements about divisibility. To see it in use, we first define the concepts of greatest common divisor and least common multiple for two integers. Let $a, b \in \mathbb{Z}$, $D = \{d \in \mathbb{Z}_+ : d|a \wedge d|b\}$, and $M = \{m \in \mathbb{Z}_+ : a|m \wedge b|m\}$. Then d^* is the greatest common divisor of a, b means that

$$[d^* \in D \wedge \forall d \in D, d|d^*]$$

and will be denoted as (a, b). To say that m^* is the least commom multiple of a and b means that

$$[m^* \in M \wedge \forall m \in M, m^*|m]$$

and is denoted as $[a, b]$.

Using the FTA, appreciate the simplicity of prooving the following statements:

Statement 1. *Let $a, b \in \mathbb{Z}_+$. Then $ab = [ab](a, b)$.*

Statement 2. *Let $a, b, c \in \mathbb{Z}_+$. Then $(a, bc) = 1 \Leftrightarrow (a, b) = (a, c) = 1$*

The FTA shows us that primes are the building blocks of the natural numbers. What more can be said? Well, there are infinitely many primes. The proof of the infinitude of primes uses the following lemma.

Lemma 2. *Let $p_1, \dots, p_n$ be primes. Then for all $i \in \{1, \dots, n\}$,*

$$p_i \nmid (\prod_{j=1}^{n} p_j) + 1$$

Proof. Assume to the contrary that $p_m | p_1 \cdots p_n + 1$ for some $m \in \{1, \dots, n\}$. So $p_m | (p_1 \cdots p_n + 1) - (p_1 \cdots p_n) = 1$. Because p_m is prime, $p_m > 1$. So $p_m | 1$ and $p_m > 1$, a contradiction. Thus $(\prod_{j=1}^{n} p_j) + 1$ isn't divisible by any prime p_m. □

We are now ready to prove the following:

Theorem 2. *There are infinitely many primes*

Proof. Asssume to the contrary that there are finitely many primes $p_1, \dots, p_n$ and consider $N = p_1 \cdots p_n + 1$. Note that because $N > p_i$ for any prime, N can't be prime and thus it must be a product of primes. So let $N = p_1^{k_1} \cdots p_n^{k_n}$ where $k_i \in \overline{\mathbb{Z}}_+$. But $p_i \nmid p_1 \cdots p_n + 1 = N = p_1^{k_1} \cdots p_n^{k_n}$, a contradiction. □