The Fundamental Theorem of Arithmetic

Ryan C. Daileda

Trinity University

Number Theory

Introduction

Today we will finally prove the *Fundamental Theorem of Arithmetic*: every natural number $n \geq 2$ can be written uniquely as a product of prime numbers.

We will first define the term "prime," then deduce two important properties of prime numbers.

We will use mathematical induction to prove the existence of prime factorizations, and Euclid's lemma to prove their uniqueness.

Prime Numbers

Definition

A natural number $p \geq 2$ is called *prime* if its only (positive) divisors are 1 and p.

Examples.

- 2 is the smallest (and only even) prime number.
- The first few primes numbers are $2, 3, 5, 7, 11, 13, 17, 19, \ldots$.
- 6 is *not* prime since $2|6$ and $2 \neq 1, 6$.
- The unit 1 is *not* prime since $1 < 2$.

Definition

A natural number $n \geq 2$ is called *composite* if it is not prime.

Negating the definition of "prime" we find that

$$n \text{ is composite} \quad \Leftrightarrow \quad n = ab \text{ with } a, b \geq 2.$$

Examples.

- Since $15 = 3 \cdot 5$, 15 is composite.
- Since $143 = 11 \cdot 13$, 143 is composite.

The prime numbers are the "atoms" of multiplicative arithmetic: they cannot be (multiplicatively) decomposed in any nontrivial way.

In ring-theoretic parlance, the primes in $\mathbb{Z}$ are "irreducible."

If we apply Euclid's lemma, we find that primes enjoy another important property.

Lemma 1

Let $p \in \mathbb{N}$ be a prime number and let $a, b \in \mathbb{Z}$ be arbitrary. If $p|ab$, then $p|a$ or $p|b$.

Remark. Ring-theoretically this result says that prime numbers are truly "prime."

Before we prove Lemma 1 we make the following observation.

If p is prime and $a \in \mathbb{Z}$,then

$$(p, a) = \begin{cases} p & \text{if } p|a, \\ 1 & \text{otherwise,} \end{cases}$$

since the only (positive) divisors of p are 1 and p.

Proof of Lemma 1. Suppose $p|ab$. If $p|a$, we're done.

So we may assume $p \nmid a$, in which case $(p, a) = 1$, by the observation.

Since $p|ab$ and $(p, a) = 1$, Euclid's lemma implies that $p|b$. □.

The atomic nature of primes immediately yields the first half of the Fundamental Theorem.

Lemma 2

Let $n \in \mathbb{N}$. If $n \geq 2$, then n is either prime or a product of prime numbers.

Remarks.

- We frequently regard a single prime p as the "product" of the single factor p.
- We can then restate the lemma with the conclusion "n is a product of prime numbers."

Proof of Lemma 2. We proceed by strong induction on n.

Since $n = 2$ is prime, this establishes our base case.

Now let $n > 2$ and suppose we have proven that every natural number $2 \leq k < n$ is a product of prime numbers.

If n is prime, we are finished. Otherwise, $n = ab$ with $2 \leq a, b < n$.

By the inductive hypothesis, a and b are products of prime numbers.

It follows that $n = ab$ is also a product of primes.

This completes the induction and finishes the proof. □

Remarks.

- The proof we have given is non-constructive: it establishes existence, but does not give an algorithm for determining prime factorizations.

- The difficulty of finding prime factorizations is what makes many modern cryptographic protocols (such as RSA) secure.

We are now ready to state and prove our main result.

Theorem 1

Let $n \in \mathbb{N}$, $n \geq 2$. Then, up to the order of the factors, n can be expressed as the product of prime numbers in exactly one way.

Proof. Let $n \in \mathbb{N}$ with $n \geq 2$. According to Lemma 2, we can write

$$n = p_1 p_2 \cdots p_r$$

for some $r \in \mathbb{N}$ and prime numbers p_i. Suppose we can also write

$$n = q_1 q_2 \cdots q_s$$

with $s \in \mathbb{N}$ and q_i prime.

Since $p_1 p_2 \cdots p_r = n = q_1 q_2 \cdots q_s$,

$$q_1 | p_1 p_2 \cdots p_r.$$

Since q_1 is prime, Lemma 1 implies that $q_1 | p_j$ for some j.

But p_j is prime, so its only divisors are 1 and p_j. Since $q_1 \neq 1$, it must be that

$$q_1 = p_j.$$

If we reorder the p_i we can assume that $j = 1$. We therefore have

$$q_1 q_2 \cdots q_s = p_1 p_2 \cdots p_r = q_1 p_2 \cdots p_r.$$

Cancelling q_1 from both sides we are left with

$$q_2 \cdots q_s = p_2 \cdots p_r.$$

Repeating this argument, we can (after possibly reordering) successively cancel $q_2 = p_2, q_3 = p_3, \ldots$.

If $r > s$ we would be left with

$$1 = p_{s+1} \cdots p_r,$$

which is impossible since $p_i > 1$ for all i. We have a similar problem if $r < s$.

So we must have $r = s$ and $p_i = q_i$ for all i (after reordering). □

As a consequence of the FTA we prove:

Theorem 2 (Euclid)

There are infinitely many prime numbers.

Proof. We argue by contradiction.Assume there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_r.$$

Let $n = p_1 p_2 \cdots p_r + 1 \in \mathbb{N}$.

According to the FTA, n is a product of prime numbers. In particular, it is divisible by some p_j.

It follows that

$$p_j | n - p_1 p_2 \cdots p_r = 1,$$

which implies $p_j = 1$, a contradiction. □

Remarks

- Given $n \geq 2$, it can be convenient to group any repeated primes in its factorization, and write

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

with p_i *distinct* primes and $a_i \geq 1$ for all i. This is the *canonical form of* n, and is unique by the FTA.

- Euler showed that the infinitude of primes also follows from the FTA and the divergence of the harmonic series

$$\sum_{n=1}^{\infty} \frac{1}{n},$$

thereby initiating the field of *analytic number theory*.

- The distribution of the prime numbers has fascinated number theorists for centuries. Let

$$\pi(x) = \#\{p \,|\, p \leq x \text{ and } p \text{ is prime}\},$$

  the number of primes up to x.

- First conjectured by Legendre, Gauss, Dirichlet and others, the Prime Number Theorem (PNT) asserts that $\pi(x)$ satisfies the asymptotic relationship

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

- Using ideas of Riemann, the PNT was first proven independently in 1896 by Hadamard and de la Vallée Poussin.

Applications

Using the FTA we can establish the following fact.

Theorem 3

Let $a \in \mathbb{N}$, $a \geq 2$. If a is not a perfect square, then $\sqrt{a}$ is irrational.

We will require the following lemma.

Lemma 3

Let $a \in \mathbb{N}$, $a \geq 2$. Write a in its canonical form:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

with each p_i distinct and $a_i \geq 1$. Then a is a perfect square if and only if every a_i is even.

Proof. If $a = b^2$, write b in canonical form:

$$b = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r},$$

with each p_i distinct and $c_r \geq 1$. Then

$$a = b^2 = p_1^{2c_1} p_2^{2c_2} \cdots p_r^{2c_r}.$$

By the FTA this must be the canonical form of a, and clearly $2c_i$ is even for all i.

The reverse implication is an easy exercise. □

Theorem 3

Proof of Theorem 3. We argue by contradiction. Assume that a is *not* a perfect square and that

$$\sqrt{a} = \frac{s}{t}$$

with $s, t, \in \mathbb{N}$.

Clearing the denominator and squaring yields

$$t^2 a = s^2.$$

We now express a, s, t in their canonical forms. By allowing the exponents to be 0, if necessary, we may assume the primes occurring in all three are the same.

So we may write

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$
$$s = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r},$$
$$t = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r},$$

with each p_i distinct and every exponent nonnegative.

Because a is not a perfect square, a_j must be odd for some j, by Lemma 3.

The equation $t^2 a = s^2$ implies

$$p_1^{a_1+2t_1} p_2^{a_2+2t_2} \cdots p_r^{a_r+2t_r} = p_1^{2s_1} p_2^{2s_2} \cdots p_r^{2s_r}.$$

Uniqueness in the FTA implies that $a_i + 2t_i = 2s_i$ for all i.

That is,

$$a_i = 2s_i - 2t_i = 2(s_i - t_i) \quad \Rightarrow \quad a_i \text{ is even}$$

for all i.

This contradicts the fact that a_j is odd, and completes the proof. □

Remarks.

- Although $\sqrt{a}$ is irrational, it is still *algebraic*: it is the root of the polynomial $X^2 - a$, which has rational coefficients.

- The systematic study of algebraic numbers falls under the purview of *algebraic number theory*.