Proof of the Fundamental Theorem of Arithmetic

Discrete Mathematics 27100 Winter 2022

January 31, 2022

1 Bulding Blocks for the Fundamental Theorem of Arithmetic

We first review some facts we will need for proving the Fundamental Theorem of Arithmetic. The first fact is that every natural number $n > 1$ is divisible by at least one prime number. This follows from a lemma which we proved last lecture as a stepping stone for the proof that there are infinitely many prime numbers.

Lemma 1.1. *For all $n \in \mathbb{N}$, if $n > 1$ and $\forall p \in \mathbb{P} \cap [n-1](p \nmid n)$ then $n \in \mathbb{P}$. In other words, if $n > 1$ is not divisible by any prime less than n then n is prime.*

The second fact we need is that if p is a prime number and $n \in \mathbb{N}$ has a prime factorization in which p does not appear then $p \nmid n$. We prove this fact by using a key property of prime numbers, which is that if p is a prime number and $p \mid xy$ then $p \mid x$ or $p \mid y$

Lemma 1.2. *For all $x, y, z \in \mathbb{N}$, if $x \mid yz$ and $gcd(x, y) = 1$ then $x \mid z$.*

Proof. By Bézout's identity, $\exists a, b \in \mathbb{Z}(ax + by = gcd(x, y) = 1)$. Multiplying this equation by z, $z = azx + byz$. Since $x \mid x$ and $x \mid yz$, $x \mid azx + byz$ so $x \mid z$, as needed. □

Corollary 1.3 (Prime property)**.** *For all primes $p \in \mathbb{P}$ and all $xy \in \mathbb{N}$, if $p \mid xy$ then either $p \mid x$ or $p \mid y$*

Proof. There are two cases to consider. Either $p \mid x$ or $p \nmid x$. If $p \mid x$ then we are done. If $p \nmid x$ then $gcd(p, x) = 1$ because $Div(p) \cap \mathbb{N} = \{1, p\}$ and $p \notin Div(x)$. In this case, by Lemma 1.2, $p \mid y$, as needed. □

With this property of prime numbers, we can now prove this second fact.

Definition 1.4 (Delta function)**.** *For all $i, j \in \mathbb{N}$, we define $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$.*

Corollary 1.5. *If n has a prime factorization $n = \prod_{i=1}^{\infty} p_i^{c_i}$ (where $p_1, p_2, p_3, \ldots$ is the sequence of primes in ascending order) then for any j such that $c_j = 0$, $p_j \nmid n$*

Proof. We prove this by induction. For the base case, if $n = 1$ then for all $j \in \mathbb{N}$, $p_j \nmid n$. For the inductive step, assume that the result is true for all $n \leq k - 1$ and consider $n = k$. Since $n > 1$, $\exists j' \in \mathbb{N}(c_{j'} \geq 1)$. Now observe that $n = p_{j'}m$ where m has the prime factorization $\prod_{i=1}^{\infty} p_i^{c_i - \delta_{ij'}}$.

For any $j \in \mathbb{N}$ such that $c_j = 0$, $j \neq j'$ and $c_j - \delta_{jj'} = 0$. By the inductive hypothesis, $p_j \nmid m$. Since $p_j \nmid p_{j'}$, by Corollary 1.3, $p_j \nmid p_{j'}m = n$, as needed. □

2 Proof of the Fundamental Theorem of Arithmetic

Theorem 2.1 (The Fundamental Theorem of Arithmetic)**.** *Let $p_1, p_2, \ldots$ be the sequence of primes in ascending order. For all $n \in \mathbb{N}$ there exists a unique sequence $c_1, c_2, \ldots$ of non-negative integers such that*

1. $n = \prod_{i=1}^{\infty} p_i^{c_i}$
2. *Only finitely many of the c_i are nonzero.*

Proof. We first prove that every natural number n has a prime factorization. To prove this, we use strong induction.

For the base case, observe that $1 = \prod_{i=1}^{\infty} p_i^0$. For the inductive step, assume that for all $n \in \mathbb{N}$ such that $n \leq k-1$, n has a prime factorization and consider $n = k$. There are two cases to consider:

1. If n is prime then $n = p_j$ for some $j \in \mathbb{N}$ so $n = \prod_{i=1}^{\infty} p_i^{\delta_{ij}}$.
2. If p is not prime then by Lemma 1.1 there exists a $j \in \mathbb{N}$ such that $p_j \mid n$ and $p_j < n$. Since $p_j \mid n$, $n = mp_j$ for some $m \in \mathbb{N}$. By the inductive hypothesis, m has a prime factorization $m = \prod_{i=1}^{\infty} p_i^{c_i}$. Now $n = p_j m = \prod_{i=1}^{\infty} p_i^{c_i + \delta_{ij}}$ so n has a prime factorization, as needed.

To prove that the prime factorization of n is unique, we again use strong induction. For the base case, observe that if any $c_i > 0$ then $\prod_{i=1}^{\infty} p_i^{c_i} > 1$. Thus, $1 = \prod_{i=1}^{\infty} p_i^0$ is the unique prime factorization of 1.

For the inductive step, assume that every $n \leq k-1$ has a unique prime factorization and consider $n = k$. Let $n = \prod_{i=1}^{\infty} p_i^{c_i}$ and $n = \prod_{i=1}^{\infty} p_i^{c_i'}$ be two prime factorizations of n.

Choose a j such that $c_j \geq 1$ and observe that c_j' cannot be 0. To see this, assume $c_j' = 0$. If so, by Corollary 1.5, $p_j \nmid n$. However, since $c_j \geq 1$, $p_j \mid n$, which is a contradiction. Thus, $n = p_j m$ where m has the prime factorizations $m = \prod_{i=1}^{\infty} p_i^{c_i - \delta_{ij}}$ and $m = \prod_{i=1}^{\infty} p_i^{c_i' - \delta_{ij}}$. By the inductive hypothesis, m has a unique prime factorization, so $\forall i \in \mathbb{N}(c_i - \delta_{ij} = c_i' - \delta_{ij})$. This implies that $\forall i \in \mathbb{N}(c_i' = c_i)$ so n has a unique prime factorization, as needed. □

3 Advanced Note: Ring Without Unique Factorizations

While the fundamental theorem of arithmetic is intuitive, it should not be taken for granted. In fact, there are number systems (called rings) which are similar to the integers where factorizations into irreucible components may not be unique.

In particular, consider $\mathbb{Z}[\sqrt{5}i]$ where we adjoin the number $\sqrt{5}i$ to the integers. In other words, we consider all complex numbers of the form $\{a + b\sqrt{5}i : a, b \in \mathbb{Z}\}$.

Divisibility is defined in the same way as before:

Definition 3.1. *We say that $d \mid n$ in $\mathbb{Z}[\sqrt{5}i]$ if $\exists q \in \mathbb{Z}[\sqrt{5}i](qd = n)$*

For $\mathbb{Z}[\sqrt{5}i]$ (and other rings), the analogue to our definition of primes is irreducibility:

Definition 3.2 (Irreducibility)**.** *We say that $n \in \mathbb{Z}[\sqrt{5}i]$ is irreducible if there do not exist $x, y \in \mathbb{Z}[\sqrt{5}i]$ such that $xy = n$, $x \neq \pm 1$, and $y \neq \pm 1$.*

In $\mathbb{Z}[\sqrt{5}i]$, it can be shown that $1+\sqrt{5}i$, $1-\sqrt{5}i$, 2 and 3 are all irreducible in $\mathbb{Z}[\sqrt{5}i]$. Since $6 = 2 \cdot 3 = (1+\sqrt{5}i)(1-\sqrt{5}i)$, 6 does not have a unique factorization into irreducible components.

To define primes in $\mathbb{Z}[\sqrt{5}i]$ (and other rings), a stronger property of prime numbers is used.

Definition 3.3. *We say that $p \in \mathbb{Z}[\sqrt{5}i]$ is prime if for all $x, y \in \mathbb{Z}[\sqrt{5}i]$ such that $p \mid xy$, either $p \mid x$ or $p \mid y$.*

Remark 3.4. *Note that prime numbers are always irreducible but the converse is not always true. For example, in $\mathbb{Z}[\sqrt{5}i]$, $1+\sqrt{5}i$, $1-\sqrt{5}i$, 2 and 3 are all irreducible but they are not prime.*