6. The Fundamental Theorem of Arithmetic

We saw from the last worksheet that every integer greater than one is a product of primes. We wish to show now that there is only one way to do that, apart from rearranging the factors. This fact is called *The Fundamental Theorem of Arithmetic.* Its importance in mathematics (and yes, applications!) cannot be understated. To prove this, we begin with the following lemma:

**Lemma 1.** Let $a, b, c$ be integers such that $a \mid bc$ and $\gcd(a, b) = 1$. Then $a \mid c$.

**Proof.** Since $\gcd(a, b) = 1$ then $1 = ax + by$ for some $x, y \in \mathbb{Z}$. Multiplying this equation by $c$, we have $c = axc + bcy$. Since $a \mid bc$, $bc = as$ for some $s \in \mathbb{Z}$. Then $c = axc + bcy = axc + asy = a(xc + sy)$. This shows that $a \mid c$. \hfill $\square$

**Exercise:** Let $b$ be an integer and $p$ a prime which doesn’t divide $b$. Prove that $\gcd(p, b) = 1$.

**Proposition 2.** Let $p$ be a prime and $a$ and $b$ integers such that $p \mid ab$. Then $p \mid a$ or $p \mid b$.

**Proof.** If $p \mid a$, we’re done. Suppose $p$ doesn’t divide $a$. By the Exercise, $\gcd(p, a) = 1$. Now by the Lemma, we see that $p \mid b$. \hfill $\square$

This result can be generalized as follows.

**Proposition 3.** Let $p$ be a prime and $a_1, \ldots, a_n$ be integers. Suppose $p \mid a_1a_2 \cdots a_n$. Then $p \mid a_i$ for some $i$.

**Proof.** Homework! \hfill $\square$

We can now state the *Fundamental Theorem of Arithmetic*:

**Theorem 4.** Every integer greater than one can be factored uniquely into primes. To be precise, suppose $n = p_1 \cdots p_k$ and $n = q_1 \cdots q_\ell$ are two prime factorizations for the integer $n$. Then, $k = \ell$ and, after reordering, $p_i = q_i$ for $i = 1, \ldots, k$.

**Proof.** Rather than give the formal proof (which uses induction on either $k$ or $\ell$), I will just demonstrate the proof in the case $k = 2$ and $\ell$ is arbitrary. So, in this case we have $n = p_1p_2 = q_1 \cdots q_\ell$. Since $p_2 \mid q_1q_2 \cdots q_\ell$, we have by Proposition 3 that $p_2 \mid q_i$ for some $i$. But since $q_i$ is prime, $p_2 = q_i$. Now, by rearranging the primes, we can assume $p_2 = q_\ell$. Substituting this into our equation, we have $p_1p_2 = q_1 \cdots q_{\ell-1}p_2$. Canceling $p_2$ from both sides, we get $p_1 = q_1 \cdots q_{\ell-1}$. Since $p_1$ is prime, there can’t be more than one prime on the right-hand side. That is, $p_1 = q_1$ and $\ell - 1 = 1$. Thus, $\ell = 2$, $p_1 = q_1$ and $p_2 = q_2$. \hfill $\square$

By grouping like primes together using exponents, and by ordering the primes in ascending order, we can write any integer greater than one in one and only one way in the form $p_1^{m_1} \cdots p_k^{m_k}$ where $p_1 < p_2 < \cdots < p_k$ are primes and $m_i \geq 1$ for all $i$. For example, $100 = 2^2 \cdot 5^2$ and $126 = 2^1 \cdot 3^2 \cdot 7^1$.

The Fundamental Theorem of Arithmetic has many applications. For instance, it can be used to show the irrationality of certain numbers.

**Example:** Let’s show that $\sqrt{2}$ is irrational. Suppose, by way of contradiction, that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ for some integers $a$ and $b$. Multiplying both sides by $b$ and then squaring
both sides, we have $2b^2 = a^2$. Now, consider the number of 2’s in the prime factorization of $a^2$. If 2 occurs $m$ times in the prime factorization of $a$, then 2 occurs $2m$ times in the prime factorization of $a^2$. Similarly, if 2 occurs $n$ times in the prime factorization of $b$, then 2 occurs $2n$ times in the prime factorization of $b^2$, which means 2 occurs $2n + 1$ times in the prime factorization of $2b^2$. But $2n + 1$ is odd and $2m$ is even, contradicting the Fundamental Theorem of Arithmetic.

**Exercise:** Prove that $\sqrt[3]{9}$ is irrational.

**Homework:**

1. Prove Proposition 3 using Proposition 2 and induction.

2. Suppose $n > 1$ is composite. Prove that $n$ is divisible by some prime $p$ with $p \leq \sqrt{n}$.
   (Hint: Use proof by contradiction.)