The Fundamental Theorem of Arithmetic

4.1 The Theorem of Ages

From the earliest grades, teachers of mathematics try to enlighten their students to the basic principles of arithmetic. Every natural number, we are told, can be factored as a product of *primes*. The primes themselves, we are told, are distinguished by the property that they cannot be factored as a product of strictly smaller natural numbers. The Fundamental Theorem of Arithmetic asserts something very special about the factorization of natural numbers into prime factors. It asserts that the factorization is essentially unique, which is to say that if we ignore the order of the prime factors, then there is one and only one way to accomplish the factorization.

The Fundamental Theorem of Arithmetic is widely taken for granted. Evidence suggests that it was known to all cultural groups, at all stages of civilization, as far back as recorded history permits us to probe. It enjoys the distinction of being the oldest and most cosmopolitan of all fundamental principles in mathematics. It has been called the Theorem of Ages.

4.2 Elements of Arithmetic

To begin, we must establish exactly what is meant by the phrase "b is a factor of a" or, equivalently, "b is a divisor of a". By definition, we say that $b \in \mathbb{Z}$ is a divisor of $a \in \mathbb{Z}$ iff there exists $c \in \mathbb{Z}$ such that $a = bc$. If b is a divisor (or factor) of a, then we denote this relation symbolically as $b \mid a$. It is customary to read the symbolic string "$b \mid a$" as "b divides a". Equivalently, it is also legitimate to say that "a is divisible by b".

Let a, b and c be integers. The following basic properties of the divisibility relation are easily verified:

(a) If $c \mid b$ and $b \mid a$, then $c \mid a$.

(b) If $c \mid a$ and $c \mid b$, then $c \mid ax + by$ for all $x, y \in \mathbb{Z}$.

(c) If $x \in \mathbb{Z}$ and $x \mid 1$, then $x = \pm 1$.

Occasionally, we may want to talk about the set of all positive divisors of an integer $a \in \mathbb{Z}$. For this purpose, we introduce the notation $\text{div}(a) = \{b \in \mathbb{N} \mid b \text{ is a positive divisor of } a\}$. For instance, the set of all positive divisors of $a = 6$ is $\text{div}(6) = \{1, 2, 3, 6\}$.

Scattered among the set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$, there are special numbers called *primes*, which are distinguished by the property that they cannot be factored as a product of strictly smaller natural numbers. By definition, a natural number $p \geq 2$ is prime iff whenever $p = ab$, where $a, b \in \mathbb{N}$, then either $a = 1$ and $b = p$ or $a = p$ and $b = 1$. In terms of the above symbolism, a natural number p is prime iff $\text{div}(p) = \{1, p\}$. It may seem fairly obvious that every natural $n \geq 2$ must possesses at least one prime factor, but without witnessing a rigorous proof, no self-respecting student of mathematics should take this for granted.

Theorem 4.1: Every natural number $n \geq 2$ has at least one prime divisor.

Proof: If n is prime, then there is nothing to prove. Otherwise, if n is not prime, then it must possess at least one non-trivial divisor d such that $1 < d < n$. Let d_0 be the smallest non-trivial divisor of n. If d_0 is prime, then the proof is complete. Otherwise, If d_0 is not prime, then d_0 must possess a divisor d_1 such that $1 < d_1 < d_0$. But, if so, then d_1 must also be a non-trivial divisor of n. But since $d_1 < d_0$, this contradicts our assumption that d_0 is the smallest non-trivial divisor of n. Thus d_0 must be prime, and the proof is complete. ■

Does the set of primes $\{2, 3, 5, 7, 11, 13, \ldots\}$ go on forever, or do we eventually encounter a largest prime $p_{\max}$ beyond which no more primes can be found? The first proof in recorded history of the fact that the set of primes is infinite is due to Euclid of Alexandria (circa 365-275 B.C.). It is one of the most famous proofs in the history of mathematics.

Theorem 4.2: (Euclid) The set of primes is infinite.

Proof: Suppose that $p_{\max}$ is the largest prime in the world. We will show that this supposition leads to a contradiction. Consider the natural number q obtained by multiplying together all the primes in the world, from smallest to the largest and adding 1 to the product. That is

$$q = 2 \times 3 \times 5 \times 7 \times 11 \times \cdots \times p_{\max} + 1.$$

Now plainly $q > p_{\max}$. Since $p_{\max}$ is the largest prime, q itself cannot be prime. Thus, by Theorem 4.1, q possesses at least one prime factor, say p. Since $q - 1$ is the product of all primes in the world, it follows that $p \mid q - 1$. Now $p \mid q$ and $p \mid q - 1$ implies that $p \mid 1$, which is a contradiction. Therefore there can be no largest prime. ■

The primes $\{2, 3, 5, 7, 11, 13, \ldots\}$ are scattered among the natural numbers in a very irregular way. Any attempt to generate them by means of a simple formula or to try to fit them to a recognizable pattern is bound to fail. However, an efficient algorithm does exist for generating the list of all primes up to a given natural number n. The algorithm is named after Eratosthenes of Cyrene (276-194 B.C.), as he is the first person in recorded history to have explicitly described it in his writings. The *sieve of Eratosthenes* (described below) is a consequence of the following very simple theorem.

Theorem 4.3: Let $n \geq 2$. If n is not prime, then n possesses a prime divisor $p \leq \sqrt{n}$.

Proof: Since n is not prime, it must possess a prime divisor, say p, such that $1 < p < n$. If $p \leq \sqrt{n}$, then there is nothing further to show. Otherwise, suppose $p > \sqrt{n}$. Let $n_1 = n/p$. Then plainly $n_1 \mid n$ and $1 < n_1 < \sqrt{n}$. Let p_1 be any prime divisor of n_1. Then p_1 is also a divisor of n and $p_1 < \sqrt{n}$. ■

To generate a list of all primes up to given natural number n, proceed as follows. First, you may assume that you have already managed to generate a list of all primes up to $\sqrt{n}$. To extend the list all the way up to n, proceed down the list $1, 2, 3, 4, \ldots, n$, crossing out all multiples of 2 (except 2 itself), then crossing out all multiples of 3 (except 3 itself), then crossing out all multiples of 5 (except 5 itself), and so on. Continue in this fashion until you have crossed out all the multiples of the largest prime $p \leq \sqrt{n}$. At this point, by Theorem 4.3, you have crossed out all the non-prime (composite) numbers in the list $1, 2, 3, 4, \ldots, n$, leaving only the primes.

Every respectable discussion of arithmetic must, at some point, turn to the idea of the "greatest common divisor" of two integers. Given $a, b \in \mathbb{Z}$, the greatest common divisor of a and b, denoted by $\gcd(a, b)$, is defined as the largest member of the set $\text{div}(a) \cap \text{div}(b)$. That is

$$\gcd(a, b) = \max\left(\text{div}(a) \cap \text{div}(b)\right).$$

If $\gcd(a, b) = 1$, then we say that a and b are *relatively prime.*

Ex: By definition, $\gcd(40, 90) = \max\left(\text{div}(40) \cap \text{div}(90)\right)$. By direct calculation, we have
$\text{div}(40) = \{1, 2, 4, 5, 8, 10, 20, 40\}$
$\text{div}(90) = \{1, 2, 3, 5, 6, 9, 10, 15, 18, 30, 45, 90\}$
$\text{div}(40) \cap \text{div}(90) = \{1, 2, 5, 10\}$
Therefore $\gcd(40, 90) = \max\{1, 2, 5, 10\} = 10$.

Ex: By definition, $\gcd(40, 91) = \max\left(\text{div}(40) \cap \text{div}(91)\right)$. By direct calculation, we have
$\text{div}(40) = \{1, 2, 4, 5, 8, 10, 20, 40\}$
$\text{div}(91) = \{1, 7, 13, 91\}$
$\text{div}(40) \cap \text{div}(90) = \{1\}$
Therefore $\gcd(40, 91) = \max\{1\} = 1$. Thus, 40 and 91 are relatively prime.

The above examples serve to illustrate how to calculate $\gcd(a, b)$ directly from the definition. This method is extremely inefficient, as it forces us to find complete factorizations for each of the integers a and b, a process which, from a computational standpoint, happens to be very costly. A far more efficient technique is that known as the *Euclidean algorithm.* The Euclidean algorithm is aptly named after Euclid of Alexandria, the first individual in recorded history to have documented it, and quite possibly the first to have discovered it. Given two integers $a > b > 0$, to calculate $\gcd(a, b)$ by the Euclidean algorithm, we proceed as follows:

Step 1: $a = q_1 b + r_1 \ \ (0 \leq r_1 < b)$

Step 2: $b = q_2 r_1 + r_2 \ \ (0 \leq r_2 < r_1)$

Step 3: $r_1 = q_3 r_2 + r_3 \ \ (0 \leq r_3 < r_2)$

Step 4: $r_2 = q_4 r_3 + r_4 \ \ (0 \leq r_4 < r_3)$

$\vdots$

Step n: $r_{n-2} = q_n r_{n-1} + r_n \ \ (0 \leq r_n < r_{n-1})$

Step $n+1$: $r_{n-1} = q_{n+1} r_n + r_{n+1} \ \ (r_{n+1} = 0)$.

In each of the above steps, say step k, what we are doing is dividing the remainder (r_{k-2}) obtained two steps earlier by the remainder (r_{k-1}) obtained one step earlier, to obtain a new remainder (r_k). The successive quotients are denoted q_1, q_2, q_3, and so on. Since successive remainders are non-negative and decreasing, that is $b > r_1 > r_2 > r_3 > \cdots > r_k \geq 0$, the process must eventually terminate at a remainder of 0. The last non-zero remainder r_n is equal to $\gcd(a, b)$. To see why, suppose d is a divisor of r_n. By tracing the Euclidean algorithm in reverse, we deduce that d must be a divisor of both a and b, hence of $\gcd(a, b)$. Conversely, if d is any divisor of $\gcd(a, b)$, then, by tracing the Euclidean algorithm in forward order, we deduce that d is a divisor of r_n. Thus $\text{div}(\gcd(a, b)) = \text{div}(r_n)$, which implies $\gcd(a, b) = r_n$.

Ex: To calculate $\gcd(91, 40)$ by the Euclidean algorithm, we proceed as follows:

$91 = 2 \times 40 + 11$

$40 = 3 \times 11 + 7$

$11 = 1 \times 7 + 4$

$7 = 1 \times 4 + 3$

$4 = 1 \times 3 + 1$

$3 = 3 \times 1 + 0$

Therefore $\gcd(91, 40) = 1$.

From the Euclidean algorithm, we can infer the following fundamental result, whose importance in elementary number theory is second only to the Fundamental Theorem of Arithmetic:

Theorem 4.4: Let $a, b \in \mathbb{Z}$ and suppose $\gcd(a, b) = d$. Then there exist integers x and y such that $ax + by = d$.

Proof: Without loss of generality, we may assume that a and b are positive, for, if not, the signs of a and b can be adjusted by absorbing them into the coefficients x and y. By the Euclidean algorithm, we have $d = r_n$, where r_n is the last non-zero remainder in the algorithm. Now, using the the n-th step in the algorithm we can express d as a linear combination of r_{n-1} and r_{n-2}. Similarly, using the $(n-1)$-th step of the algorithm, we can express express r_{n-1} as a linear combination of r_{n-2} and r_{n-3}, so that d becomes a linear combination of r_{n-2} and r_{n-3}. Similarly, using the $(n-2)$-th step of the algorithm, we can express r_{n-2} as a linear combination of r_{n-3} and r_{n-4}, so that d becomes a linear combination of r_{n-3} and r_{n-4}. Continuing in the same manner, we see that, at every step of the algorithm, d can be expressed as a linear combination of r_k and r_{k-1}. Ultimately, back at step 1, we have $d = ax + by$. ■

Corollary 4.5: Two integers a and b are relatively prime ($\gcd(a, b) = 1$) if and only if there exist integers x and y such that $ax + by = 1$.

Proof: If $\gcd(a, b) = 1$, then, by Theoren 4.4, $\gcd(a, b) = ax + by = 1$. Conversely, suppose $ax + by = 1$. If $\gcd(a, b) = d$, then $d \mid a$ and $d \mid b$, so $d \mid ax + by = 1$, which implies $d = 1$.

Ex: Since $\gcd(40, 91) = 1$, there exist integer coefficients x and y such that $40x + 91y = 1$. To find them, we proceed, as in the proof of Theorem 4.4, by unraveling the Euclidean algorithm in reverse. To make it easier to distinguish the remainders in each step, we adorn them by dressing them in square brackets:

$[4] = 1 \times [3] + [1] \;\Rightarrow\; [1] = -[3] + [4]$

$[7] = 1 \times [4] + [3] \;\Rightarrow\; [3] = -[4] + [7] \;\Rightarrow\; [1] = 2[4] - [7]$

$[11] = 1 \times [7] + [4] \;\Rightarrow\; [4] = -[7] + [11] \;\Rightarrow\; [1] = -3[7] + 2[11]$

$[40] = 3 \times [11] + [7] \;\Rightarrow\; [7] = -3[11] + [40] \;\Rightarrow\; [1] = 11[11] - 3[40]$

$[91] = 2 \times [40] + [11] \;\Rightarrow\; [11] = -2[40] + [91] \;\Rightarrow\; [1] = -25[40] + 11[91]$

Therefore $40(-25) + 91(11) = 1$. That is $x = -25$ and $y = 11$.

Corollary 4.6: If $\gcd(a,b)=1$ then $\gcd(a^2,b^2)=1$.

Proof: By Theorem 4.4, we can find $x,y\in\mathbb{Z}$ such that $ax+by=1$. Raising both to the 3-rd power, we get $x^3a^3+3x^2a^2yb+3xay^2b^2+y^3b^3=1$, which is equivalent to $a^2x_1+b^2y_1=1$, where $x_1=x^3a+3x^2yb$ and $y_1=3xay^2+y^3b$. Thus, by Corollary 4.5, $\gcd(a^2,b^2)=1$. ■

To the mathematicians of antiquity, especially Pythagoras and his followers (circa 550 B.C.), it came as a great shock to discover that some numbers are not rational (cannot be expressed as the ratio of two whole numbers). Numbers that are not rational are called *irrational*. Using Corollary 4.6, we can show that $\sqrt{p}$ is irrational for every prime p.

Theorem 4.7: If p is prime, then $\sqrt{p}$ is irrational.

Proof: Suppose $\sqrt{p}$ is rational. We will show that this supposition leads to a contradiction. If $\sqrt{p}$ is rational, then it can be expressed as a fraction in lowest terms, say $\sqrt{p}=a/b$ where $\gcd(a,b)=1$. By Corollary 4.6, we have $\gcd(a^2,b^2)=1$ and we are assured that integers x_1 and y_1 exist such that $a^2x_1+b^2y_1=1$. The relation $\sqrt{p}=a/b$ implies $a^2=b^2p$, so that $b^2px_1+b^2y_1=1$. Therefore $b^2\mid 1$, which implies $b^2=1$. Thus $p=a^2$, which contradicts the assumption that p is prime. ■

Using Theorem 4.4, we can derive an alternate characterization of what it means for a natural number n to be prime. This alternate characterization of primality plays an essential role in the proof of the Fundamental Theorem of Arithmetic.

Theorem 4.8: A natural number n is prime if and only if n possesses Property P: whenever $n\mid ab$, where $a,b\in\mathbb{N}$, then $n\mid a$ or $n\mid b$.

Proof: If n is not prime (i.e. composite), then $n=ab$ for some natural numbers a and b, where $1<a<n$ and $1<b<n$. So $n\nmid a$ and $n\nmid b$. In particular, this means that if n is not prime, then n does not possess Property P. Conversely, suppose n is prime and $n\mid ab$. Then $ab=nk$ for some $k\in\mathbb{Z}$. If $n\nmid a$, then $\gcd(n,a)=1$. Thus, by Theorem 4.4, there exist integers x and y such that $nx+ay=1$. So $nbx+aby=b$, which implies that $nbx+nky=b$, which implies that $n\mid b$. Thus, if n is prime, then n possesses Property P. ■

Corollary 4.9: If p is prime and $p\mid a_1a_2a_3\cdots a_m$, then $p\mid a_j$ for some $1\le j\le m$.

Proof: We proceed by induction on m. By Theorem 4.8, the claim is valid for $m=2$. Suppose the claim is valid for $m=k$. If $p\mid a_1a_2a_3\cdots a_ka_{k+1}$, then $p\mid a_{k+1}$ or $p\mid a_1a_2a_3\cdots a_k$. That is, $p\mid a_{k+1}$ or $p\mid a_j$ for some $1\le j\le k$. ■

Corollary 4.10: If p is prime and $p\mid a^m$, where $m\ge 1$, then $p\mid a$.

Proof: Apply Corollary 4.9 with $a=a_1=a_2=\cdots=a_m$. ■

Corollary 4.11: If p and q are primes and $p\mid q^m$, where $m\ge 1$, then $p=q$.

Proof: By Corollary 4.10, $p\mid q$. However, since $\operatorname{div}(q)=\{1,q\}$, it follows that $p=q$. ■

4.3 The Fundamental Theorem of Arithmetic

Suppose we are given natural number n and suppose we are able to factor it as a product of primes, say $n = p_1 p_2 p_3 \cdots$. In general, there are many ways to write the product, depending on how we choose to order the factors and depending on how we choose to arrange the factors in terms of prime powers. For instance, $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 3 \cdot 5 \cdot 2 \cdot 3 \cdot 2 \cdot 2 = 3^2 \cdot 5^1 \cdot 2^3$. The preferred form of factorization is in terms of prime powers, where the distinct primes in the factorization are arranged in increasing order from left to right. That is

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} \quad \text{where} \quad p_1 < p_2 < p_3 < \cdots$$

A factorization like the above is called a *product of prime powers in standard arrangement.* For instance, if $n = 360$ is expressed as a product of prime powers in standard arrangement, we get $360 = 2^3 \cdot 3^2 \cdot 5^1$.

Theorem 4.12: (The Fundamental Theorem of Arithmetic) Every natural number $n \geq 2$ can be expressed *in exactly one way* as a product of prime powers in standard arrangement.

Proof: First we must show that n can be factored as a product of primes. By Theorem 4.1, there exists a prime p_1 such that $n = p_1 n_1$, where $n > n_1 \geq 1$. Similarly, by Theorem 4.1, there exists a prime p_2 such that $n_1 = p_2 n_2$, where $n > n_1 > n_2 \geq 1$. Continuing in this manner, we see that n can be expressed as $n = p_1 p_2 p_3 \cdots p_k n_k$ where $n > n_1 > n_2 > \cdots > n_k \geq 1$. Since the sequence of numbers n_j are decreasing and positive, they must eventually terminate, at which point the factorization of n as a product of primes is complete. By regrouping the factors as prime powers in standard arrangement, we obtain $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$. Now, we still have to show that this representation is unique. Suppose an alternate representation of n as a product of prime powers in standard arrangement is possible, say $n = q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m}$. We will show that these two representations are, in fact, one and the same. By Corollaries 4.9-4.11, every prime p_i in the first factorization divides some prime power $q_j^{s_j}$ in the second factorization, so that $p_i = q_j$. Similarly, every prime q_i in the second factorization divides some prime power $p_j^{r_j}$ in the first factorization, so that $q_i = p_j$. Thus, the primes that appear in the first factorization are exactly the same as the primes that appear in the second factorization. As a result, we have

$$n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}.$$

At this point, we must still show that corresponding exponents are equal. Suppose, by way of contradiction, that $r_i < s_i$ for some i, $1 \leq i \leq k$. If we divide the first factorization by $p_i^{r_i}$, then the prime p_i no longer occurs in the factorization of $n/p_i^{r_i}$. On the other hand, if we divide the second factorization by $p_i^{r_i}$, then, since $r_i < s_i$, the prime p_i still occurs in the factorization of $n/p_i^{r_i}$ with non-zero exponent $s_i - r_i$. This implies that p_i divides one of the prime power factors $p_j^{r_j}$ in the first factorization where $p_i \neq p_j$, which, by Corollary 4.11, implies that $p_i = p_j$, a contradiction. Therefore, all corresponding exponents must be equal, and the proof of the theorem is complete. ■

Ex: Using the Fundamental Theorem of Arithmetic, we show that $\log_{72}(175)$ is irrational. By way of contradiction, suppose that $\log_{72}(175)$ is rational, say $\log_{72}(175) = m/n$ where m and n are positive whole numbers. Then $175 = 72^{m/n}$, which implies $175^n = 72^m$, so that $(5^2 \cdot 7)^n = (2^3 \cdot 3^2)^m$. Hence $5^{2n} \cdot 7^n = 2^{3m} \cdot 3^{2m}$, which violates the unique factorization principle of the Fundamental Theorem of Arithmetic.

4.4 Exercises

1. Decide if the claim is true or false.
   (a) $9 \mid 4203$.
   (b) $12 \mid 4$.
   (c) $7 \mid 0$.
   (d) $3 \mid -18$.
   (e) $-6 \in \text{div}(18)$.
   (f) $-3 \in \text{div}(-6)$.
   (g) $\text{div}(5) \cap \text{div}(7) = \varnothing$.
   (h) $\dfrac{\sqrt{98}}{3\sqrt{8}}$ is a rational number.
   (i) The smallest positive prime number is 1.
   (j) A prime number cannot be even.
2. Use the Euclidean algorithm to find $\gcd(a, b)$.
   (a) $a = 495$ and $b = 147$
   (b) $a = 729$ and $b = 512$
3. Use the Euclidean algorithm in reverse to find integers x and y such that $ax + by = \gcd(a, b)$.
   (a) $a = 495$ and $b = 147$
   (b) $a = 729$ and $b = 512$
4. Express n as a product of prime powers in standard arrangement.
   (a) $n = 337500$
   (b) $n = 11307375$
   (c) $n = 510510$
   (d) $n = 2^{16} - 1$
   (e) $n = 15!$
5. Prove or disprove the claim that every integer of the form $n^2 - n + 41$ is prime for all $n \geq 0$.
6. Show that $\log_{3850}(4760)$ is irrational.
7. Show that if $\gcd(a, b) = 1$ then $\gcd(a^3, b^3) = 1$.
8. Prove that $\sqrt[3]{p}$ is irrational for every prime p.
9. Show that $\gcd(3x + 8, 5x + 13) = 1$ for every integer x.
10. Find two non-zero integers x and y such that $\dfrac{x}{81} + \dfrac{y}{25} = 1$.