Section 2. Unique Factorization

Note. In this section, we define prime numbers. We state and prove the Unique Factorization Theorem (Theorem 2.2; this is also called "The Fundamental Theorem of Arithmetic"). **In this section, we use lower-case italic letters to denote positive integers!** Much of the material in this section is also in my online notes for Mathematical Reasoning (MATH 3000) on Section 6.3. Divisibility: The Fundamental Theorem of Arithmetic.

Definition. An integer that is greater than 1 and has no positive divisors other than 1 and itself is a *prime* number. An integer that is greater than 1 but is not prime is a *composite* number.

Note. Notice that 1 is neither a prime nor a composite. In fact, 1 is a "unit." We *could* extend the ideas of prime and composite to negative integers, in which case -1 is also a unit (notice that -1 and 1 are the only integers with multiplicative inverses in $\mathbb{Z}$). However, Dudley only consider positive integers in this section. The ideas of prime and composites are explored in more detail in Introduction to Modern Algebra 2 (MATH 4137/5137); see my online notes for this class on Section IX.45. Unique Factorization Domains where primes are defined in the setting of integral domains (in particular, see Definition 45.5 and Corollary 45.18).

Note. No doubt you are familiar with prime numbers. The cover of the text book (the hard bound version published by W.H. Freeman in 1978) gives the (positive) prime numbers and unit for numbers up to 100 (I have actually always been puzzled as to why 1 is included...). As Dudley states: "The primes can thus be used to build, by multiplication, the entire system of positive integers. ...every positive integer can be written as a product of primes. Later we will prove the uniqueness of the representation." See page 11. The first two lemmas in this section deal with the *existence* of the representation of an integer as a product of primes.

Lemma 2.1. Every integer n, with $n > 1$, is divisible by a prime.

Lemma 2.2. Every integer n, with $n > 1$, can be written as a product of primes.

Note. Inductive proofs can also be given for Lemmas 2.1 and 2.2 (see Exercise 2.2, for example). The next result is a "celebrity of mathematics"! It appears in Euclid's *Elements of Geometry* in Book IX as Proposition 20. Euclid states it as "Prime numbers are more than any assigned multitude of prime numbers." A proof can be found in David Joyce's online version of Euclid's *Elements*. Links to several different versions are on the University of Tennessee-Martin's PrimePages on "Proofs that there are infinitely many primes". The website PrimePages has up-to-date information on prime number research (accessed 7/1/2021).

Theorem 2.1. Euclid's Theorem. There are infinitely many primes.

Note. Over the years, finding large prime numbers has been a challenge addressed by the increased computational power of computers. Dudley makes some quaint observations on page 12 where observes that the largest currently known prime is $2^{19,937} - 1$ which has over 6,000 digits; this was the state of things in 1978. According to Primepages' The Largest Known Primes—A Summary, the largest known prime is $2^{82,589,933} - 1$ which has 24,862,048 digits and was found in 2018 (accessed 7/1/2021).

Note. The next two lemmas relate to testing integers to see if they are composite.

Lemma 2.3. If n is composite, then it has a divisor d such that $1 < d \leq n^{1/2}$.

Lemma 2.4. If n is composite, then it has a *prime* divisor d such that $1 < d \leq n^{1/2}$.

Note. Lemma 2.4 is the basis for the "Sieve of Eratosthenes." The idea is to eliminate composite numbers by first removing multiples of 2 greater than 2, then removing multiples of 3 greater than 3, then removing multiples of 5 greater than 5, etc. If all multiples of primes less than or equal to n have been removed, then all numbers less than n^2 which remain must be prime. Wikipedia has a nice animated GIF of the Sieve of Eratosthenes which finds all prime numbers between 2 and 120 by eliminating multiples of 2, 3, 5, 7, and 11.

Note. Eratosthenes of Cyrene (275 BCE – 194 BCE) was born in modern-day Shabbat, Libya in North Africa. He served as the third librarian at the Alexandrian Library in Egypt starting around 240 BCE. In Eutocius commentary on Archimedes' *Sphere and Cylinder*, a letter written by Eratosthenes to Ptolemy III describes the history of the problem of duplicating the cube (that is, using a compass and straight-edge to construct a line segment of length $\sqrt[3]{2}$, given a line segment of length 1; this remained a famous unsolved problem until around 1800). Eratosthenes made several contributions to astronomy. He estimated the distance to the Sun and the Moon. He estimated the tilt of the Earth's axis with a high degree of accuracy. However, he is probably most famous for giving an accurate measurement of the circumference of the Earth in *On the Measurement of the Earth* (a work lost, but known from secondary references of the time; knowledge of ancient lost works is often based of references to the work such as in a commentary of the work). Of interest in this class is Eratosthenes contribution to number theory. The Sieve of Eratosthenes is described in *Introduction to Arithmetic* by Nicomachus; a version in English can be browsed online at the Hathi Trust Digital Library. This information, and the picture below, are from the Eratosthenes page on the MacTutor History of Mathematics Archive (accessed 7/1/2021).

Note. The next result, sometimes known as "Euclid's Lemma," makes the unique factorization of integers into products of primes possible. It appears in Euclid's *Elements of Geometry* as Proposition 30 of Book VII where it is stated as: "If two numbers, multiplied by one another make some number, and any prime number measures the product, then it also measures one of the original numbers." This statement and Euclid's proof can be found in David Joyce's Euclid's *Elements* page.

Lemma 2.5. Euclid's Lemma.
For p prime, if $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Note. We now extend Euclid's Lemma using Mathematical Induction.

Lemma 2.6. For p prime, if $p \mid (a_1 a_2 \cdots a_k)$ then $p \mid a_i$ for some $i = 1, 2, \ldots, k$.

Lemma 2.7. If $q_1, q_2, \ldots, q_n$ are primes and $p \mid q_1 q_2 \cdots q_n$ then $p = q_k$ for some $k = 1, 2, \ldots, n$.

Note. We can now state the main theorem of this section. Dudley refers to it as "The Unique Factorization Theorem" (thus the title of this section), but it is also commonly known as "The Fundamental Theorem of Arithmetic." A proof can also be found in Introduction to Modern Algebra 2 (MATH 4137/5137); see Corollary 45.18 in my online notes for this class on Section IX.45. Unique Factorization Domains.

Theorem 2.2. The Unique Factorization Theorem or **The Fundamental Theorem of Arithmetic.**

Any positive integer greater than 1 can be written as a product of primes in one and only one way.

Note. It follows from The Unique Factorization Theorem that each positive integer $n > 1$ can be written in exactly on way in the form $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where $e_i \geq 1$ and p_i is prime for $i = 1, 2, \ldots, k$, and $p_i \neq p_j$ for $i \neq j$.

Definition. For integer $n > 1$, the expression of n as in the form $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where $e_i \geq 1$ and p_i is prime for $i = 1, 2, \ldots, k$, and $p_i \neq p_j$ for $i \neq j$ is the *prime-power decomposition* of n.

Note. We can use the prime-power decomposition of two integers to easily find the greatest common divisor. Since the only divisor of a power of prime p (other than 1) is another prime power of p (less than or equal to the first), then the only common divisors involve powers of the same primes. That is, if the prime-power decomposition of m involves $p_i^{e_i}$ and the prime-power decomposition of n involves $p_i^{e_\ell}$ then a common divisor of m and n is $p_i^{\min\{e_i, e_\ell\}}$. For example, if $n = 120 = 2^3 \cdot 3 \cdot 5$ and $m = 252 = 2^2 \cdot 3^2 \cdot 7$ then we see that common divisors are 2^2 and 3, and these are the only power-or-a-prime common divisors. So the greatest common divisor is $(120, 252) = 2^2 \cdot 3 = 12$. Alternatively, we can express 120 and 252 as powers of common primes by using exponents of 0 to get: $120 = 2^3 \cdot 3^1 \cdots 5^1 \cdot 7^0$ and

$252 = 2^2 \cdot 3^2 \cdot 5^0 \cdots 7^1$. We then just pick off the powers of primes using the least exponents to get $(120, 252) = 2^2 \cdot 3^1 \cdot 5^0 \cdots 7^0 = 12$. This is the idea behind the next result, which we state without proof.

Theorem 2.3. If $e_i \geq 0$ and $f_i \geq 0$ for $i = 1, 2, \ldots, k$, and

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \text{ and } n = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k},$$

then $(m, n) = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$ where $g_i = \min\{e_i, f_i\}$ for $i = 1, 2, \ldots, k$.

Revised: 3/4/2022