6.3. Divisibility: The Fundamental Theorem of Arithmetic

Note. In this length section, we introduce the idea of divisibility and explore it in connection with prime numbers. We prove the Division Algorithm (in Theorem 6.17), discuss the Euclidean Algorithm for computing a greatest common divisor, and use these results to prove the Fundamental Theorem of Arithmetic (Theorem 6.29). Most of the material is also contained in my online notes for Elementary Number Theory (MATH 3120) on Section 1. Integers and Section 2. Unique Factorization.

Definition 6.13. Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that a *divides* b, or b is *divisible* by a, or a is a *divisor* or *factor* of b, or b is a *multiple* of a if $b = ac$ for some $c \in \mathbb{Z}$. The statement that a divides b is denoted $a \mid b$, and is negation is denotes $a \nmid b$. If $a \mid b$ and $|a| < |b|$ then a is a *proper divisor* of b.

Theorem 6.15. Let $a, b, c \in \mathbb{Z}$. Then

(a) If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$.

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

Note. Recall that a *prime number* is an integer $p > 1$ that has no integer factorization $p = ab$ in which both $a > 1$ and $b > 1$. In Section 2.10. Mathematical Induction

and Recursion we saw that every integer $n \geq 2$ is a product of primes numbers (see Theorem 2.71). The fact that there are infinitely many prime numbers is famously presented in Euclid's *Elements of Geometry* in Book IX as Proposition 20. A proof (similar to the one given below) is given in Elementary Number Theory (MATH 3120) in Theorem 2.1, "Euclid's Theorem," of Section 2. Unique Factorization. Some history of this result (and its connection to the Euclidean Algorithm) can be found in my online notes for Introduction to Modern Geometry-History (MATH 4157/5157) on Section 2.4. Books VII and IX. Number Theory.

Theorem 6.16. (Euclid, circa 300 BCE)
There are infinitely many prime numbers.

Definition. If integers n and $n+2$ are both prime, then n and $n+2$ are *twin primes*.

Note. Examples of twin prime pairs are $\{3,5\}$, $\{5,7\}$, $\{11,13\}\ldots$ Though is has been known that there are infinitely many prime numbers for over two millenia, it is not known whether or not there are infinitely many twin prime pairs. Another unsolved conjecture is Goldbach's Conjecture that speculates that every even integer greater than 2 can be expressed as a sum of two primes. This conjecture is named after German mathematician Christian Goldbach (March 18, 1690–November 20, 1764) who mentioned it in a letter to Swiss mathematician Leonhard Euler (April 15, 1707–September 18, 1783).

Note. In long division of integers, you are familiar with finding a quotient and remainder. As mentioned by Gerstein (page 290), when we divide 581 by 16 we get:

$$\begin{array}{rr} & 36 \longleftarrow \text{quotient} \\ \text{divisor} \longrightarrow 16\,\overline{)\,581} & \\ & \underline{48} \\ & 101 \\ & \underline{96} \\ & 5 \longleftarrow \text{remainder} \end{array}$$

We can write this either $\frac{581}{16} = 36 + \frac{5}{16}$ or $581 = 16 \cdot 36 + 5$. This idea is generalized in the Division Algorithm. This is addressed for quotients of positive integers in Elementary Number Theory (MATH 3120) in Section 1. Integers (see Theorem 1.2). The result holds for any quotient of integers, positive or negative (as long as we don't try to divide by 0). This more general form of the Division Algorithm is seen in Introduction to Modern Algebra (MATH 4127/5127) in Section I.6. Cyclic Groups (see Theorem 6.3). We now state and prove our version of the Division Algorithm which requires that we divide by a positive integer.

Theorem 6.17. Division Algorithm.

Let $a, b \in \mathbb{Z}$, with $b > 0$. Then there are integers q and r such that $a = bq + r$ and $0 \leq r < b$. Moreover, q and r are uniquely determined by these conditions. Here, q is the *quotient* and r is the *remainder*.

Definition 6.18. Let a and b be integers, not both 0. An integer $d \neq 0$ is a *common divisor* of a and b if $d \mid a$ and $d \mid b$. A common divisor d of a and b is a *greatest common divisor* if $d > 0$ and if every common divisor of a and b is also a divisor of d. The greatest common divisor of a and b is denoted (a, b).

Note. The next result shows that a greatest common divisor exists between any two integers (not both 0) and is unique. We can therefore speak of "the" greatest common divisor.

Theorem 6.20. If a and b are integers, not both 0, then a and b have a unique greatest common divisor.

Note. In the proof of Theorem 6.20, we see that the greatest common divisor of a and b is a linear combination of a and b. We promote this result to the level of a corollary.

Corollary 6.21. Let $d = (a, b)$. Then there are integers x and y such that $d = ax + by$.

Note. When claiming the existence of some mathematical object, we can establish this existence by actually constructing the object. This is not what we did in the proof of Theorem 6.20, but instead indirectly showed the existence. You might

be familiar with this idea in the setting of Calculus 1 where you might show the existence of a zero of the function $f(x) = x^3 + x - 5$ using the Intermediate Value Theorem (the function is negative at $x = 0$, positive at $x = 2$, and a continuous function, so $f(x) = 0$ for some x between 0 and 2); you could also show the existence of a zero by actually finding the zero, but I doubt that you know how to do that (I don't!). In Linear Algebra, you might show that a square matrix has an inverse by showing that its determinant is nonzero; you could also actually find the inverse. From Theorem 6.20, we know of the existence of a greatest common divisor but we do not have a process to find the "gcd." We now turn our attention to finding the greatest common divisor, (a, b), of two nonzero integers a and b. First, we need a lemma.

Lemma 6.22. If $a = bq + r$ then $(a, b) = (b, r)$.

Note. The Euclidean Algorithm allows us to find a greatest common divisor. It is stated and proved in Elementary Number Theory (MATH 3120) on Section 1. Integers (see Theorem 1.3). It appears in Euclid's *Elements* as Proposition 2 of Book VII; for more history, see my online notes for Introduction to Modern Geometry-History (MATH 4157/5157) on Section 2.4. Books VII and IX. Number Theory.

Note 6.23. Euclid's Algorithm for Computation of (a, b).

As opposed to stating Euclid's Algorithm as a theorem (as is done in Section 1. Integers of Elementary Number Theory, MATH 3120), we just give a description of it and explain why it works. We start with integers a and b, where $b > 0$.

Divide b into a, getting a quotient q_1 and remainder r_1: $a = bq_1 + r_1$ with $0 \leq r_1 < b$. If $r_1 = 0$ then $b = (a, b)$.

If $r_1 \neq 0$ then divide r_1 into b to get quotient q_2 and remainder r_2: $b = r_1q_2 + r_2$ with $0 \leq r_2 < r_1$. If $r_2 = 0$ then $r_1 = (a, b)$.

If $r_2 \neq 0$ then divide r_2 into r_1 to get quotient q_3 and remainder r_3: $r_1 = r_2q_3 + r_3$ with $0 \leq r_3 < r_2$. If $r_3 = 0$ then $r_2 = (a, b)$.

$\vdots$

If $r_i \neq 0$ then divide r_i into r_{i-1} to get quotient q_{i+1} and remainder r_{i+1}: $r_{i-1} = r_iq_{i+1} + r_{i+1}$ with $0 \leq r_{i+1} < r_i$. If $r_{i+1} = 0$ then $r_i = (a, b)$.

Notice that the process has to end because we have $0 \leq r_{i+1} < r_i$ for each i. It ends at some nonzero r_k By repeated application of Lemma 6.22,

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_k, r_{k-1}) = (r_k, 0) = r_k.$$

Examples 6.24 and 6.25. Applying the Euclidean Algorithm to find $(2880, 504)$ we have:

$$
\begin{array}{rrl}
 & 5 & \\
b \longrightarrow 504 & \overline{)\,2880} & \longleftarrow a \\
 & \underline{2520} & \\
r_1 \longrightarrow 360 & \overline{)\,504} & \longleftarrow b \\
 & \underline{360} & \\
r_2 \longrightarrow 144 & \overline{)\,360} & \longleftarrow r_1 \\
 & \underline{288} & \\
r_3 \longrightarrow 72 & \overline{)\,144} & \longleftarrow r_2 \\
 & \underline{144} & \\
r_4 \longrightarrow & 0 & \qquad (2880, 504) = 72
\end{array}
$$

Corollary 6.21 claims that there are integers x and y such that $(a, b) = ax + by$. We can find x and y for $a = 2800$ and $b = 504$ from the above computation as follows. Converting these first three computations from division to multiplicative statements we have $2880 = 504 \cdot 5 + 360$, $504 = 360 \cdot 1 + 144$, and $360 = 144 \cdot 2 + 72$. Combining these equations gives

$$72 = 360 + 144 \cdot (-2) = 360 + (504 - 360) \cdot (-2) = 360 \cdot 3 + 504 \cdot (-2)$$

$$= (2880 - 504 \cdot 5) \cdot 3 + 504 \cdot (-2) = 2880 \cdot 3 + 504 \cdot (-17).$$

So we have $(a, b) = ax + by$ where $(a, b) = (2800, 504) = 72$, $x = 3$, and $y = -17$.

Note. In Theorem 2.71 we say that every integer $n \geq 2$ can be expressed as a product of primes factors. The Fundamental Theorem of Arithmetic claims that this factoring is unique. The next step in this direction is the following lemma.

Theorem 6.26. Let p be a prime number and let a and b be integers. Then the following implication holds: If $p \,|\, ab$ then either $p \,|\, a$ or $p \,|\, b$.

Note. The net corollary follows from Theorem 6.26 by the Principle of Mathematical Induction.

Corollary 6.27. Let p be prime, and let $a_1, a_2, \ldots, a_t \in \mathbb{Z}$. If $p \mid a_1 a_2 \cdots a_t$, then $p \mid a_i$ for some index i.

Note. The next corollary shows that the converse of Theorem 6.26 actually holds.

Corollary 6.28. Let m be an integer greater than 1. Then m is prime if and only if the following implication holds for all $a, b \in \mathbb{Z}$: If $m \mid ab$ then either $m \mid a$ or $m \mid b$.

Note. We are now equipped to prove our main result of this section.

Theorem 6.29. The Fundamental Theorem of Arithmetic.
Let n be an integer greater than 1. Then there are prime numbers $p_1, p_2, \ldots, p_r$ such that $n = p_1 p_2 \cdots p_r$. Moreover, this factorization of n is unique in the following sense: If $n = q_1 q_2 \cdots q_s$ also, with the q's prime, then the q's are just a rearrangement of the p's. That is, $r = s$ and, if we label the primes so that $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$, then $p_i = q_i$ for $1 \leq i \leq r$.

Corollary 6.30. Let $n \in \mathbb{Z}$ with $|n| \geq 2$. Then n has a unique factorization of the form $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ where $t \geq 1$, the p_i are distinct primes satisfying $p_1 \leq p_2 \leq \cdots \leq p_t$, and $\alpha_i \geq 1$ for $1 \leq i \leq t$. This factorization is the *standard* or *canonical factorization* of n.

Note. With what we have established, proving the irrationality of $\sqrt{2}$ is straightforward. The existence of irrational numbers were known to the Pythagoreans, according to Proclus (412 AD–485 AD). For more historical details, see my online notes for Introduction to Modern Geometry-History (MATH 4157/5157) on Section 1.4. The Regular Pentagon (in which the main irrational number of interest is the golden ration, $\Phi = (\sqrt{5}+1)/2$).

Theorem 6.31. The real number $\sqrt{2}$ is irrational.

Exercise 6.33. Suppose a and b are integers such that for distinct primes $p_1, p_2, \ldots, p_t$, and integers $\alpha_i \geq 0$ and $\beta_i \geq 0$ for $1 \leq i \leq t$ we have $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ and $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$. Then

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_i^{\min\{\alpha_i, \beta_i\}} \cdots p_t^{\min\{\alpha_t, \beta_t\}}.$$

Definition 5.43. Let S be a set of integers that contains at least one nonzero integer. The *least common multiple* of S is the smallest positive integer that is a multiple of every member of S. The least common multiple of $\{r_1, r_2, \ldots, r_m\}$ is denoted $\text{lcm}(r_1, r_2, \ldots, r_m)$ or $[r_1, r_2, \ldots, r_m]$.

Note 6.3.A. Suppose, as in the notation above, that $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ and $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_t^{\beta_t}$. Let

$$R = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_i^{\max\{\alpha_i,\beta_i\}} \cdots p_t^{\max\{\alpha_t,\beta_t\}}.$$

Notice that R is a positive multiple of a and of b, so that the lcm satisfies $[a, b] \leq R$. Since $a \,|\, [a, b]$ and $b \,|\, [a, b]$, then $p_i^{\alpha_i}$ and $p_i^{\beta_i}$ both divide $[a, b]$, and hence $p_i^{\max\{\alpha_i,\beta_i\}}$ divides $[a, b]$ for $1 \leq i \leq t$. So in the standard factorization of $[a, b]$, prime $p_i$appears at least to the power $\max\{\alpha_i, \beta_i\}$. Hence $R \,|\, [a, b]$, and so $R \leq [a, b]$. Therefore, $R = [a, b]$ and the lcm of a and b is

$$[a, b] = p_1^{\max\{\alpha_1,\beta_1\}} p_2^{\max\{\alpha_2,\beta_2\}} \cdots p_i^{\max\{\alpha_i,\beta_i\}} \cdots p_t^{\max\{\alpha_t,\beta_t\}}.$$

We can now related (a, b) and $[a, b]$.

Theorem 6.35. If a and b are nonzero integers, then $[a, b] = |ab|/(a, b)$.

Revised: 2/21/2022