Section 1. Integers

Note. In this section, we consider properties of the integers related to divisibility, the greatest common divisor, the Division Algorithm, and the Euclidean Algorithm. Some 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.

Note. An axiomatic development of the integers starts with an axiomatic development of the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$ (sometimes 0 is excluded from the natural numbers). The integers, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, then result by introducing additive inverses of the natural numbers. The rational numbers, $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$, then result by introducing multiplicative inverses of nonzero integers and requiring closure under addition and multiplication. The real numbers, $\mathbb{R}$, then result by introducing an "Axiom of Completeness" which effectively, plugs up the wholes in the rational numbers. An axiomatic development of the natural numbers would be given in a set theory class (see my online notes for such a class; notice in particular "Chapter 3. Natural Numbers"). The precise way in which the rational numbers are built from the integers is explored in Introduction to Modern Algebra (MATH 4127/5127); see my online notes on Section IV.21. The Field of Quotients of an Integral Domain. The formal definition of the real numbers is given (as a "complete ordered field") in Analysis 1; see my online notes on Section 1.2. Properties of the Real Numbers as an Ordered Field and Section 1.3. The Completeness Axiom.

Note/Definition. In this course, we depend on your intuitive understanding of the integers. We take as given the usual properties of addition, subtraction, multiplication, division (that is the algebraic properties). We also take the order of the integers as understood (that is, the idea of "greater than" and "less than"). We also assume the *Least-Integer Principle*: A nonempty set of integers that is bounded below contains a smallest element. From this follows the *Greatest-Integer Principle*: A nonempty set of integers that is bounded above contains a greatest element. This idea is addressed in Theorem 2.5 in "Section 3.1. Introduction to Natural Numbers" of Karel Hrbacek and Thomas Jech's *Introduction to Set Theory*, Second Edition Revised and Expanded (Dekker, 1984); This is the source for my online Set Theory notes. We largely use lower case *italic* letters to represent integers.

Definition. We say that integer a *divides* integer b, denoted $a \,|\, b$, if there is an integer d such that $ad = b$. If a does not divide b then we write $a \nmid b$.

Note. The next two results give some properties of divisibility.

Lemma 1.1. If $d \,|\, a$ and $d \,|\, b$, then $d \,|\, (a + b)$.

Lemma 1.2. If $d \,|\, a_1$, $d \,|\, a_2$, $\ldots$, $d \,|\, a_n$, then $d \,|\, (c_1a_1 + c_2a_2 + \cdots + c_na_n)$ for any integers $c_1, c_2, \ldots, c_n$.

Example 1.A. We now consider a "real world" application of Lemma 1.2 (though our motivation for considering almost all of the results in this course is to reach a deeper understanding and not to solve applied problems). We want to see if we can use 100 coins consisting of pennies, dimes, and quarters to make exactly \$5.00. ASSUME that this is possible and let c denote the number of pennies, d the number of dimes, and q the number of quarters in such an arrangement. Then we need

$$(1)\ c + d + q = 100 \text{ and } (2)\ c + 10d + 25q = 500.$$

Subtracting equation (1) from equation (2) implies that (3) $9d + 24q = 400$. Since $3 \,|\, 9$ and $3 \,|\, 24$, so by Lemma 1.2 we have that $3 \,|\, (9d + 24q)$ for all integers d and q. Hence $3 \,|\, 400$. But this is not the case so we have a CONTRADICTION. So the assumption is false and no such collection of 100 such coins can make \$5.00. It turns out that there are five different ways of making \$4.99 out of 100 such coins, as we will explore later.

Definition. Integer d is the *greatest common divisor* of integers a and b if

(i) $d \,|\, a$ and $d \,|\, b$, and

(ii) if $c \,|\, a$ and $c \,|\, b$, then $c \leq d$.

This is denoted $d = (a, b)$. (Another common notation is $d = \gcd(a, b)$.)

Note. Condition (i) in the definition of greatest common divisor implies that d is a common divisor of a and b, and condition (ii) implies that any other common divisor of a and b is less than or equal to c so that c is the greatest such divisor. We

leave $(0, 0)$ undefined (there is no greatest divisor of 0 since every integer divides 0). If both a and b are nonzero, the the set of common divisors of a and b is a set of integers bounded above by the largest of a, b, $-a$, and $-b$. So by the Greatest-Integer Principle for integers, the set has a largest element and so the greatest common divisor of a and b exists and is unique. Since for any integers a and b we have $1 \mid a$ and $1 \mid b$, then $(a, b) \geq 1$. The next result gives a property of greatest common divisors.

Theorem 1.1. If $(a, b) = d$ then $(a/d, b/d) = 1$.

Definition. If $(a, b) = 1$ then a and b are *relatively prime* (also called *coprime*).

Note. We will use the Euclidean Algorithm (stated below as Theorem 1.3) to find a greatest common divisor. We need the following before proving the Euclidean Algorithm. This result, The Division Algorithm, will look familiar to you, and it turns out to be very useful.

Theorem 1.2. The Division Algorithm.
Given positive integers a and b, there exist unique integers q and r with $0 \leq r < b$ such that $a = bq + r$.

Note. The Division Algorithm also holds for negative integers a and b where the condition "$0 \leq r < b$" is replace with the condition $0 \leq r < -b$. More generally, we can state:

The Division Algorithm.

Given integers a and b, $b \neq 0$, there exist unique integers q and r with $0 \leq r < |b|$ such that $a = bq + r$.

A proof of this general form can be found in my online notes for Introduction to Modern Algebra (MATH 4127/5127); see Theorem 6.3 in Section 6. Cyclic Groups.

Definition. For integers a and b, $b \neq 0$, where $a = bq + r$ for integers q and r with $0 \leq r < |b|$ (as given in The Division Algorithm), integer q is the *quotient* of a and b and nonnegative integer r is the *remainder* that results from diving a by b.

Note. Theorem 1.2 and the next lemma are needed to prove the Euclidean Algorithm.

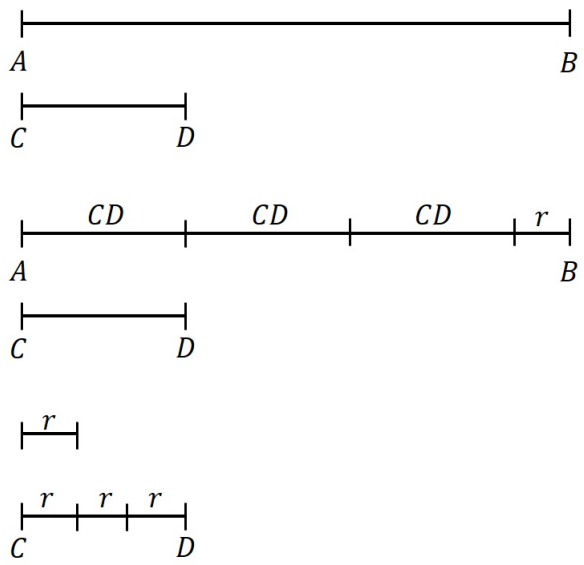
Lemma 1.3. If $a = bq + r$, then $(a, b) = (b, r)$.

Example. Consider $(70, 21)$. To apply Lemma 1.3, we take $a = 70$ and $b = 21$. Then $70 = 3 \cdot 21 + 7$ or, in the notation of Lemma 1.3, $q = 3$ and $r = 7$. So Lemma 1.3 then implies that $(70, 21) = (21, 7) = (7 \cdot 3, 7) = 7$.

Note. If we iterate Lemma 1.3 then we get "The Euclidean Algorithm," to be stated below as Theorem 1.3. This is named after Euclid, because it appears in Euclid's *Elements of Geometry*. Actually, it is Lemma 1.3 that appears as Proposition 2 of Book VII of the *Elements*. Euclid's approach to arithmetic (and "number theory" in particular) is to consider numbers as lengths of line segments. It is stated as:

> **Proposition VII.2.** *To find the greatest common measure of two given numbers not relatively prime.*
>
> Let AB and CD be the two given numbers not relatively prime. It is required to find the greatest common measure of AB and CD.

The notation "AB" and "CD" is used because these represent lengths of line segments with the given points (points A, B, C, and D) as endpoints. We can illustrate the first step in the previous example geometrically as follows:



Think of $AB = 70$ and $CD = 21$. Then $q = 3$ and $r = 7$. We then have $(AB, CD) = (70, 21)$ and $(CD, r) = (21, 7) = 3$.

Note. For details on the content of Euclid's *Elements of Geometry*, see my online presentation Euclid's Elements-A 2,500 Year History. An excellent version of the *Elements* is online on David Joyce's *Euclid's Elements* webpage. Euclid's version of Lemma 1.3 from this source is at: *Euclid's Elements*, Book VII, Proposition 2; notice that there is also a discussion of the Euclidean Algorithm on this webpage.

Note. Euclid of Alexandria (circa 325 BCE–circa 265 BCE) and his book, *The Elements of Geometry*, have influenced mathematics through history more than any other single person or work. The Axiom/Definition/Theorem/Proof approach is reflected in most math books to this day! The limited biographical information on Euclid is largely from Proclus' *A Commentary on the First Book of Euclid's Elements* which was written around 450 AD (hundreds of years after Euclid lived). He places Euclid as living after Plato (427 BCE–347 BCE) but before Eratosthenes (276 BCE–194 BCE) and Archimedes (287 BCE–212 BCE). Little is actually known about Euclid, though it is though that he spent time in Alexandria, Egypt and died there. It may be that Euclid was, in fact, a person who wrote the *Elements* himself. It may be that Euclid was the leader of a team (in Alexandria) that compiled the *Elements*... or it may be that Euclid was not an actual person and that the *Elements* were written by a team that of mathematicians who, in honor of the historical person "Euclid of Mergara" (who lived about 100 years before the *Elements* appeared), listed the author as Euclid. The *Elements* consists of 13 "books," which are better described in modern terms as 13 chapters. Books I–VI are on plane geometry, Books VII-X are on arithmetic (including number theory), and Books XI–XIII are on solid geometry. The geometry is very much motivated

by a compass and straight-edge construction approach. Numbers are dealt with in terms of the construction of line segments of certain lengths (given a line segment of length 1), so the books on arithmetic state relationships between numbers in terms of lengths of line segments. Other works attributed to Euclid include:

- *The Data.* This concerns elementary geometry and may be thought of as elementary exercises in analysis.
- *The Book On Divisions (of Figures).* This work is lost in Greek but has been discovered in the Arabic.
- *The Conics.* This is lost, but is said to have consisted of four books and was used by Apollonius.
- *Elements of Music.* This is a work credited to Euclid, but no longer exists.

Surprisingly, little geometry predating Euclid's *Elements* survives today. It is likely that the *Elements* were so thorough and circulated so widely that it simply replaced earlier works (which certainly existed; Euclid did not work in a vacuum). This information is from the MacTutor History of Mathematics Archive page on Euclid.

Image from World History Encyclopedia article on Euclid (accessed 7/1/2021)

Theorem 1.3. The Euclidean Algorithm.

If a and b are positive integers, $b \neq 0$, and

$$\begin{aligned} a &= bq + r, & 0 \leq r < b, \\ b &= rq_1 + r_1, & 0 \leq r_1 < r, \\ r &= r_1q_2 + r_2, & 0 \leq r_2 < r_1, \\ &\vdots & \vdots \\ r_k &= r_{k+1}q_{k+2} + r_{k+2}, & 0 \leq r_{k+2} < r_{k+1}, \end{aligned}$$

then for k large enough, say $k = t$, we have $r_{t-1} = r_tq_{t+1}$, and $(a, b) = r_t$.

Note. If either a or b is negative, then we can use the fact that $(a, b) = (-a, b) = (a, -b), (-a, -b)$ to show that the Euclidean Algorithm also hold for general integers a and b with $b \neq 0$. Working through the Euclidean Algorithm backward, we get the following.

Theorem 1.4. If $(a, b) = d$, then there are integers x and y such that $ax + by = d$.

Note. We will have a better method for solving $ax+by = (a, b)$ in Section 3. Linear Diophantine Equations (see Theorem 3.1). The existence of solutions allows us to deduce the following three corollaries.

Corollary 1.1. If $d \,|\, ab$ and $(d, a) = 1$, then $d \,|\, b$.

Corollary 1.2. Let $(a, b) = d$, and suppose that $c \mid a$ and $c \mid b$. Then $c \mid d$. That is, every common divisor of integers a and b is a divisor of the greatest common divisor of a and b.

Corollary 1.3. If $a \mid m$, $b \mid m$, and $(a, b) = 1$, then $ab \mid m$.

Revised 7/26/2023