# Section 2.4. Books VII and IX. Number Theory

**Note.** In this section we briefly explore the number theory results of Book VII, with a particular interest in the Euclidean Algorithm. We consider two results from Book IX, related to an $\varepsilon$ argument and the idea of continued fractions.

**Note.** Book VII has 22 definitions and 39 propositions. Definition 1 sets up a scale by defining a "unit"; interpret this a given line segment, the length of which sets 1 unit of length. Definition 2 defines "number" in such a way that indicates that Euclid is using the term number to denote the positive integers (or the natural numbers $\mathbb{N}$). Definition 3 shows that Euclid uses the term "measures" to indicate "divides," and he uses the term "part" to represent a divisor of a natural number. Definition 5 shows that Euclid is using the term "multiple" in the familiar way.

**Book VII, Definition 1.** A *unit* is that by virtue of which each of the things that exist is called one.

**Book VII, Definition 2.** A *number* is a multitude composed of units.

**Book VII, Definition 3.** A number is a *part* of a number, then less of the greater, when it measures the greater.

**Book VII, Definition 5.** The greater number is a *multiple* of the less when it is measured by the less.

The other definitions include the familiar ideas of even/odd number, prime number, relatively prime numbers, composite numbers, numbers which are squares, numbers which are cubes, and perfect numbers.

**Note.** Since numbers are dealt with in terms the lengths of line segments, Euclid gives somewhat of a geometric approach to number theory. In Book V in the setting of proportions, Euclid has already addressed the idea that if a number divides two quantities, then it divides the sum of the quantities (Euclid V.1) and the difference of the quantities (Euclid V.5). These are illustrated geometrically in Figure 2.19. These ideas are used in the proof of the Euclidean algorithm (Book VII, Proposition 2).

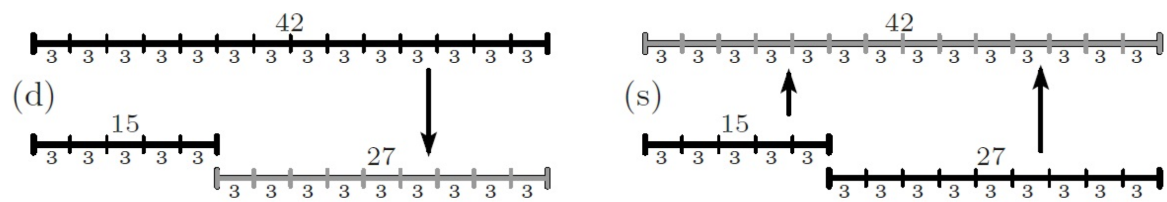


Figure 2.19. Divisibility of the difference (d) and sum (s) of two numbers

**Note.** The "Euclidean Algorithm" produces the greatest common divisor of two (non-relatively prime) natural numbers. This is a topic one would encounter early on in a class on number theory. For example, see my online class notes for Elementary Number Theory (MATH 3120) on Section 1. Integers. In these Elementary Number Theory notes, Lemma 1.1 is the same as Euclid V.1 and V.5 (but in the number theory notes, the numbers under consideration are integers instead of natural numbers and so there is no need to distinguish between sums and differences). The notes also include some history related to Euclid. Euclid states the Euclidean Algorithm as:

**Euclid, Book VII, Proposition 2.** To find the greatest common measure of two given numbers not relatively prime.

The Euclidean Algorithm is a constructive, iterative process that produces the greatest common divisor. Suppose the two natural numbers are $a$ and $b$ where $a > b$. Subtract the smaller from the larger (Euclid only considers *positive* integers). Repeat his process by applying it to the new pair $a - b$ and $b$ (the Elementary Number Theory notes use the Division Algorithm here). Any common divisor of $a$ and $b$ also divides $a - b$ and $b$, and conversely. So continuing this process of subtracting smallest from largest numbers in the pair, until a pair is produced where one of the elements in the pair is 0. The step previous to the step producing 0 has the greatest common divisor as both entries of the pair. For example, to find the greatest common divisor of $a = 42$ and $b = 15$, we subtract to get the new pair $a = 27$ and $b = 15$, then subtract to get the pair $b = 12$ and $a = 15$ (keeping $a$ as the larger of the two). We repeat the process by taking differences to get the pairs $a = 12$ and $b = 3$, $a = 9$ and $b = 3$, $a = 6$ and $b = 3$, $a = b = 3$, and finally the pair 0 and 3. So the greatest common divisor of 42 and 15 is 3. This is illustrated in terms of line segments in Figure 2.20 (both by taking differences (d) and by running the algorithm backwards starting with 3 and adding (s) to produce 42 and 15).

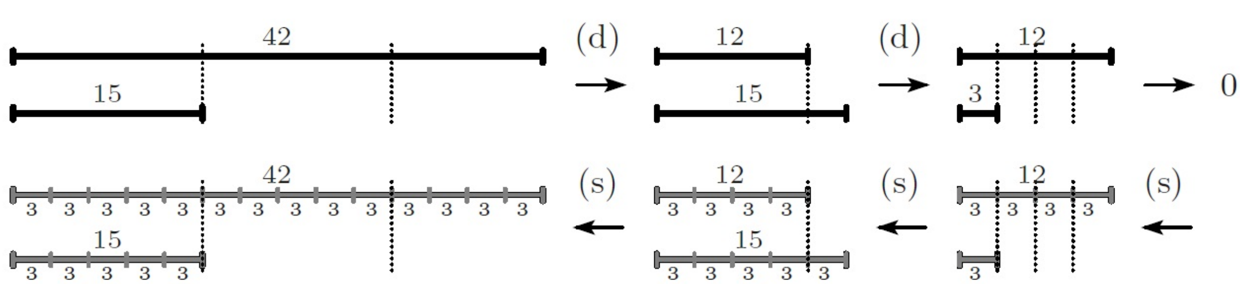


Figure 2.20. An example of the Euclidean Algorithm to find the greatest common divisor of 42 and 15 (top)

**Note.** Also in Book VII, Proposition 34 gives a construction of the least common multiple of two numbers. In Book IX, Proposition 20 proves the famous result that there are an infinite number of prime numbers:

**Euclid, Book IX Proposition 20.** Prime numbers are more than any assigned multitude of prime numbers.

Euclid's proof involves (roughly) assuming that there are a finite number $n$ of primes, taking the product of the $n$ primes and adding 1, and concluding that there is some prime divisor of this new number that is not included in the original list of $n$ primes (this is a proof by contradiction)

**Note.** Book X has a total of 10 definitions and 115 propositions. Euclid relates the idea of commensurable with rational numbers, and the idea of incommensurable with irrational numbers (though he does so in defining rational and irrational "straight lines"). In the following conversation, we concentrate on the first two propositions of Book X.

**Note.** Euclid X.1 is, according to Ostermann and Wanner, "the first convergence result in history" (see page 44). Euclid states it as:

**Euclid, Book X Proposition 1.** Two unequal magnitudes being set out, if from the greater there is subtracted a magnitude greater than its half, and from that which is left a magnitude greater than its half, and if this process is repeated continually, then there will be left some magnitude less than the lesser magnitude set out. And the theorem can similarly be proven even if the parts subtracted are halves.

The process involves (effectively) halving a given quantity $a$ repeatedly (as Euclid puts it, "is subtracted a magnitude greater than its half"). This is very much an $\varepsilon$ argument! As Euclid says "then there will be left some magnitude less than the lesser magnitude set out," so with $\varepsilon > 0$ as the "lesser magnitude set out," the process is iterated sufficiently many times (making $n$, say, sufficiently large) so that the quantity produced (say $a/2^n$) is less than $\varepsilon$. This is pretty much the same definition you see in Calculus 2 (MATH 1920) for the definition of the limit of a sequence (see my online notes on Section 10.1. Sequences).

**Note.** Euclid X.2 concerns applying the Euclidean Algorithm to any "magnitude" (that is, to any positive real number). When applied to rational numbers, the process terminates with the greatest common divisor as a rational number. For example, the greatest common divisor of $1/2$ and $1/3$ is $1/6$ since both $1/2$ and $1/3$ are natural number multiples of $1/6$ and $1/6$ is the greatest such rational number with this property. What Euclid does is give a condition under which a quotient of positive real numbers is irrational in terms of the the termination of the Euclidean Algorithm. As he puts it:

**Euclid, Book X Proposition 2.** If, when the less of two unequal magnitudes is continually subtracted in turn from the greater that which is left never measures the one before it, then the two magnitudes are incommensurable.

**Example.** We now illustrate Euclid X.2 for two cases where the Euclidean Algorithm does not terminate. First, suppose $a = \Phi$ (the "golden ratio" of Section 1.4. The Regular Pentagon) and $b = 1$. The algorithm starts by producing $c = a - b = \Phi - 1 = 1/\Phi$ (because $\Phi = 1 + 1/\Phi$), then $d = b - c = 1 - (\Phi - 1) = 1 - 1/\Phi$, $e = c - d = (1/\Phi) - (1 - 1/\Phi) = 2/\Phi - 1$, etc. In Figure 2.21 (left), we start with a right triangle with hypotenuse $\Phi$ and legs of lengths $\sqrt{\Phi}$ and 1 (recall that $\Phi^2 = \Phi + 1$). From $\Phi$ we have first subtracted 1 to give $1/\Phi$. Geometrically, this corresponds to dividing each side of the triangle in Figure 2.21 (left) by $\Phi$ to produce the triangle in the left part of the original triangle, with hypotenuse 1 and legs of lengths $1/\sqrt{\Phi}$ and $1/\Phi$. In the next step, each side of the second triangle is divided by $\Phi$ giving a triangle of hypotenuse $1/\Phi$ and legs of lengths $1/\Phi^{3/2}$ and $1/\Phi^2$ (the triangle in the lower right of the original triangle). So as the process continues, the triangles continue to shrink by a linear factor of $\Phi$ and can be represented by the infinite sequence of little triangles embedded in the first triangle, as suggested by Figure 2.21 (left). So by Euclid X.2, $\Phi$ is irrational.

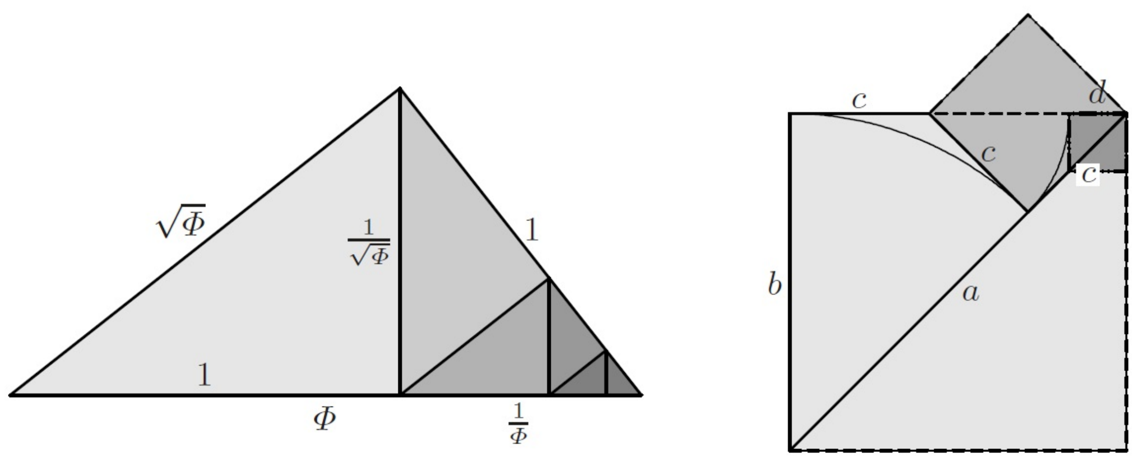


Figure 2.21. The Euclidean Algorithm applied to $a = \Phi$ and $b = 1$ (left), and $a = \sqrt{2}$ and $b = 1$ (right)

Similarly, with $a = \sqrt{2}$ and $b = 1$, we get $c = a - b = \sqrt{2} - 1$, $d = b - c = (1) - (\sqrt{2} - 1) = 2 - \sqrt{2}$, $3 = c - d = (\sqrt{2} - 1) - (2 - \sqrt{2}) = 2\sqrt{2} - 3$, etc. In Figure 2.21 (right), we start with a square of side $b = 1$ and diagonal $a = \sqrt{2}$, cut the length of $b = 1$ from the diagonal $a$ produces a square of sides of length $c = a - b = \sqrt{2} = 1$. Next we cut the diagonal of this second square by an amount $c$ producing the third square with sides of length $d$. This leads to an infinite sequence of little square that converge to the upper right point on the first square, as suggested by Figure 2.21 (right). So by Euclid X.2, $\sqrt{2}$ is irrational.

**Note.** Book X also contains the result that every natural number that is not a perfect square, has an irrational square root (Euclid X.9); for example, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, etc. are irrational. In a lemma to Euclid X.28, the technique for constructing Pythagorean triples is given; three natural numbers $a$, $b$, $c$ for a Pythagorean triple if $a^2 + b^2 = c^2$. Pythagorean triples are explored in Elementary Number Theory (MATH 3120) in Section 16. Pythagorean Triangles.

*Revised: 1/26/2022*