Greatest Common Divisor: Algorithm and Proof

Mary Flagg*

January 5, 2019

Finding the greatest common divisor of two integers is foundational to a variety of mathematical problems from operations with fractions to modern cryptography. One common algorithm taught in primary school involves finding the prime factorization of the two integers, which is sufficient for finding the greatest common divisor of two small integers. However, the prospect of trying to find the prime factorization of two large numbers is daunting.

Instead of looking in our modern textbook for a better algorithm, let's go back to the source and discover simple, yet powerful, algorithms in the mathematics of ancient China and ancient Greece. We will discover that the two communities formulated similar algorithms for finding the greatest common divisor, yet they did so in completely different contexts.

The first section of this project introduces the mutual subtraction algorithm in ancient China, tracing its development through different texts dating from ca. 200 BCE to 263 CE. The mutual subtraction algorithm was introduced in the context of reducing fractions, still the first place it is used in modern mathematics education. The second section explores the algorithm from the text of Euclid's *Elements*, written ca. 300 BCE [Euclid, 2002]. In the *Elements*, Euclid developed the basic tenets of geometry and number theory. The geometric inspiration carried over into the number theory, as numbers were represented as line segments with length a multiple of a unit. The algorithm for finding the greatest common divisor was discussed in the context of measuring line segments. In modern mathematics, the algorithm is essential to many areas of number theory and algebra, including RSA cryptography. Where have you encountered the greatest common divisor?

The common subtraction algorithm is known as the Euclidean algorithm in Western mathematics. Along with the practical technique for finding the greatest common divisor, it is also often one of the first theorems students encounter in a proof-based course in number theory, discrete mathematics or abstract algebra. Students are expected to understand why the algorithm works, not simply know how to perform the calculations. The explanations for why the algorithm worked were very different in the ancient Chinese and Greek texts. This contrast in the ancient texts, and a comparison with a modern proof, is also a beautiful example of the history of mathematical proof. In this project we will explore the history of the Euclidean algorithm, both as a practical tool and as an example of the standard for proof at different times in different mathematical communities.

*Department of Mathematics, Statistics and Computer Science, University of St. Thomas, Houston, Texas 77096; flaggm@stthom.edu.

1 Mutual Subtraction in China

1.1 Background

1.1.1 The Texts

In the winter of 1983-1984, archeologists excavating the tomb of a provincial Chinese bureaucrat at a Western Han Dynasty site near Zhangjiashan discovered a number of books on bamboo strips. Among these was the *Suan Shu Shu* or *Book of Numbers and Computations* [Dauben, 2008], the earliest yet discovered book specifically devoted to mathematics from ancient China. The *Book of Numbers and Computations* has been dated with reasonable accuracy to the early second century BCE. The topics in the book include rules for multiplication, arithmetic with fractions, problems dealing with proportions and rates and finding the area or volume of simple geometric figures.

Rules for reducing fractions were included in the *Book of Numbers and Computations*, including multiple rules for finding the greatest common divisor of two numbers. The rules for fractions and the algorithm for finding the greatest common divisor receive a more thorough treatment in later classic texts, including the *Jiuzhang Suanshu* [1] or *The Nine Chapters on the Mathematical Art* [Shen et al., 1999].

The *Nine Chapters on the Mathematical Art*, hereafter referred to as the *Nine Chapters* for brevity, dominated the early history of Chinese mathematics [Shen et al., 1999, p. 1]. It played a central role in Chinese mathematics equivalent to that of Euclid's *Elements* in Western mathematics. It remains the fundamental source of traditional Chinese mathematics. The *Nine Chapters* is an anonymous text, compiled across generations of mathematicians. It is believed that the original text was compiled by the first century BCE, but it is difficult to date precisely. Western mathematical ideas were not introduced into China until the first Chinese translation of Euclid's *Elements* by Xu Guangqi (1562–1633) and Matteo Ricci (1552–1610) appeared in 1606 [Shen et al., 1999, p. 21].

The *Nine Chapters* is a series of 246 problems and their solutions organized into nine chapters by topic. The topics indicate that the text was meant for addressing the practical needs of government, commerce and engineering. The problems and solutions do not generally include an explanation of why a particular solution method worked. Unlike the Greek emphasis on proofs, the Chinese emphasized algorithms for solving problems. This does not mean that they did not know why an algorithm worked, it only shows that the most important goal was to show students how to perform the calculations correctly.

The chapters of the book demonstrate that an extensive body of mathematical knowledge was known to the ancient Chinese:

1. Rectangular Fields: This chapter is concerned with land measurement and gives the formulas for finding the areas of fields of several shapes.

2. Millet and Rice: Chapters 2 and 3 contain a variety of problems from agriculture, manufacturing and commerce.

3. Distribution by Proportion

4. Short Width: The problems in this chapter involve changing the dimensions of a field while maintaining the same area and includes algorithms for finding square roots and working with

[1] See [Shu-Chun Guo, 1990] for the Chinese text

circles.

5. Construction Consultations: This chapter includes formulas for volumes of various solids.

6. Fair Levies: The problems in this chapter come from taxes and distribution of labor.

7. Excess and Deficit: The rule of double false position for solving linear equations is used to solve a variety of problems in this chapter.[2]

8. Rectangular Arrays: The Fangcheng Rule is introduced to solve systems of linear equations.

9. Right-angled Triangles: This chapter includes the *Gougu Rule*, known to Western mathematicians as the Pythagorean Theorem.

The noted Chinese mathematician Liu Hui, who flourished in the third century CE, published an annotated version of the *Nine Chapters* in the year 263 [Shen et al., 1999, p. 3] with detailed explanations of many of the solution methods, including a justification of the algorithm for finding the greatest common divisor.

This project will look at the *Book of Numbers and Computations*, the *Nine Chapters* and the comments by Liu Hui to see how the Chinese understood the algorithm and its proof. Before we begin examining the text, a brief explanation of ancient Chinese computation will help the reader understand the wording of the ancient texts.

1.1.2 Counting Rod Numerals

Ancient China developed a very efficient system of computation by physically manipulating counting rods. Counting rods and rod arithmetic were used in China from 500 BCE until approximately 1500 CE when counting rods were gradually replaced with the abacus [Shen et al., 1999, pp. 11–17].

China used a base-ten place value system for numerals. Counting rods were used to represent the digits 1–9 and the arrangement of the rods on a counting board indicated the place value. Counting rods were small bamboo sticks, approximately 2.5 mm in diameter and 15 cm long. The rods were laid out either upright or horizontally, as in Figure 1. The numbers 1–5 were represented by laying the corresponding number of rods side by side, either horizontally or vertically. One horizontal rod set atop a number of vertical rods, or a vertical rod on top of some horizontal rods each represent five units in the digits 6, 7, 8 and 9. Numbers were formed by alternating upright numerals for units, hundreds, etc., with horizontal numerals for tens, thousands, etc. Places with zeros were left blank since there was no symbol for zero in the counting rod system. The alternating horizontal and vertical numerals helped distinguish the places in the base ten numeral. The alternating orientation of the counting rods also served as a point of demarcation when one of the digits in the number was zero and the place in the written numeral was left blank.

Figure 2 illustrates the usefulness of the alternating orientation of the counting rods in the representations of the numbers 328, 58, and 3028. Notice that the alternating directions of the rods for numerals of successive powers of ten separates the 3 in the hundreds place and the 2 in the tens place, easily distinguishing 328 from 58. The counting rod representation of 3028 differs from that of

[2]Double false position refers to a method of solving a linear equation using trial and error by using a series of prescribed steps to obtain the correct solution from information reported on incorrect guesses, and is still a viable method today.

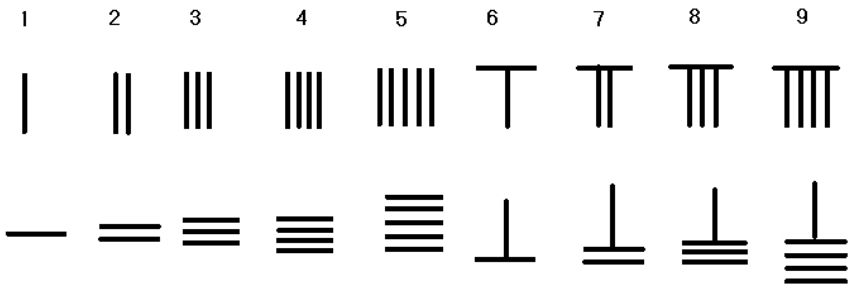

Figure 1: Vertical and Horizontal Counting Rod Numerals

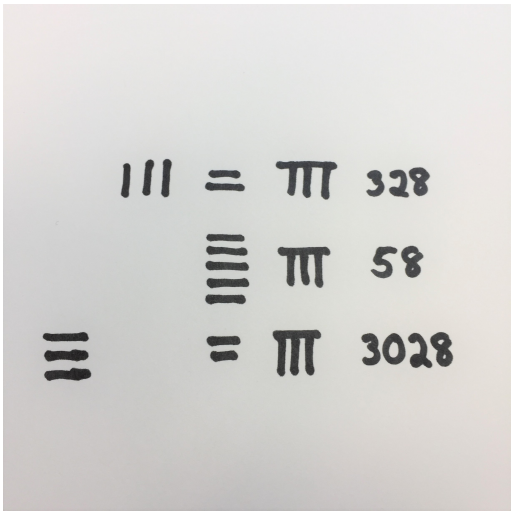

Figure 2: Examples of Rod Numbers

328 by the fact that the 3 is also horizontal, which indicates that there is zero in the hundreds place in 3028. Numbers with more than one consecutive zero, like 2003 or 400005, would need some context to help the reader interpret the space between the nonzero digits since the alternating horizontal and vertical rods would not obviously mark the missing digit. Do you see why zeros are so useful in our modern numerals?

Counting rod arithmetic was performed by manipulating the counting rods on a counting board. Unfortunately, we have no visual record of counting boards or how counting rod arithmetic was performed. However, references to the counting rods appear in the instructions for finding the greatest common divisor in the *Nine Chapters*.

1.2 The Algorithm

A Book of Numbers and Computations includes procedures for arithmetic with fractions. Before explaining how to add fractions, Problem 7 gives rules for simplifying fractions. Read a portion of the English translation from [Dauben, 2008] below.

Suan Shu Shu (Problem 7) Yue fen: Simplifying Fractions

The rule for simplifying fractions says: Take the numerator and subtract it (successively) from the denominator; also take the denominator and subtract it (successively) from the numerator; (when) the amounts of the numerator and denominator are equal, this will simplify it (the fraction will be simplified). Another rule for simplifying fractions says: if it can be halved, halve it; if it can be divided by a certain number, divide by it. Yet another rule says: Using the numerator of the fraction, subtract it (successively) from the denominator; using the remainder as denominator, subtract it (successively) from the numerator; use what is equal to (both) numerator and denominator as the divisor; then it is possible to divide both numerator and denominator by this number.

Did you notice that the 'rule for simplifying fractions' is a list of 3 rules? (Go back and look if you did not notice the first time.) *A Book of Numbers and Computations* simply lists mathematical algorithms without any attempt to interpret them, or reconcile different methods. It is an example of the early development of Chinese mathematics.

Task 1 Try to simplify the fraction $\frac{72}{112}$ using each of the three rules. Write down the questions you had about the instructions that were not clear. (Hint: Each subtraction step involves subtracting the smaller number from the larger number.)

Task 2 The second rule from the *Book of Numbers and Computations* says 'if it can be halved, halve it; if it can be divided by a certain number, divide by it'. This rule is very different from the first and third rules.

(a) Simplify the fraction $\frac{72}{112}$ by diving numerator and denominator by common factors.

(b) Explain how to find the greatest common divisor of 72 and 112 using this procedure.

(c) Given positive integers a and b, the second rule prescribes reducing the fraction $\frac{a}{b}$ by dividing by common factors until the resulting numerator and denominator have no factors in common. In this general case, explain how to find the greatest common factor of a and b.

The first and third rule are two different versions of the same mutual subtraction algorithm. The procedure began with the numerator and denominator of the fraction displayed as rod numerals on a counting board. A subtraction step consisted of subtracting the smaller number from the larger number while leaving the smaller number unchanged. Subtraction continued until both numbers were equal. Since subtraction was performed by physically removing the appropriate number of rods from the larger number, there was no record of the intermediate steps. Dividing the original numerator and denominator by the final equal number simplified the original fraction.

Task 3 Use the mutual subtraction algorithm to find the equal number for the fraction $\frac{72}{112}$. Is this number the greatest common divisor of 72 and 112?

Task 4 Problem 7 in the *Book of Numbers and Computations* goes on to apply this rule to the fraction $\frac{162}{2016}$. Use the mutual subtraction algorithm to find the greatest common divisor of 162 and 2016. Since the remainders at each step are important in the justification of the algorithm, keep a record of each step. To organize your work, create a two column table with the original numbers at the top of each column. After each subtraction step, carry the samller number down to the next line and put the subtraction remainder under the larger number.

$$\begin{array}{c|c} 162 & 2016 \\ \hline 162 & 2016 - 162 = 1854 \\ \vdots & \vdots \end{array} \tag{1}$$

Another method for simplifying fractions appears later in the *Nine Chapters* within the context of a more systematic development of the rules for arithmetic with fractions. It follows Problem 6 in Chapter 1, which asks the reader to simplify $\frac{49}{91}$.

The Method for Simplifying Fractions

If [both the numerator and the denominator] can be halved, halve them; if they cannot be halved, put down [on one side of the counting board] the numbers of the denominator and the numerator separately, subtract the smaller from the larger, and continue subtracting, seeking equality. Use the equal number to simplify the fraction. [YI DENG SHU YUE ZHI] [3]

Before we look carefully at the procedure, did you notice that this version of the rule instructs the user to copy the numerator and denominator on the side of their workspace, leaving the fraction intact?

Task 5 Why do you think the instructions included copying the numbers and performing mutual subtraction on the side of the counting board?

Now let's look a little closer at the rule in the *Nine Chapters*.

Task 6 Simplify the fraction $\frac{49}{91}$ using the instructions in the *Nine Chapters* and show your work as in Task 4. What is the 'equal number' obtained at the end of the mutual subtraction algorithm? Is this the greatest common divisor of 49 and 91?

Task 7 Use the instructions in the *Nine Chapters* to simplify $\frac{72}{112}$ and $\frac{162}{2016}$. How does the algorithm change if both numerator and denominator are even?

Task 8 In Task 7, the fraction $\frac{162}{2016}$ was simplified by first dividing numerator and denominator by 2, then performing the mutual subtraction algorithm on 81 and 1008. What was the 'equal number' obtained from subtraction? How is this equal number related to the greatest common divisor of 162 and 2016? The mutual subtraction algorithm was performed on 81 and 1008. Is the equal number the greatest common factor of 81 and 1008?

[3] [Dauben et al., 2013]

Task 9 Use the method outlined in the *Nine Chapters* to simplify $\frac{120}{168}$. Explain how to find the greatest common divisor of 120 and 168 from your work.

Task 10 Given positive integers a and b, the *Nine Chapters* simplified the fraction $\frac{a}{b}$ by first dividing numerator and denominator by 2 before performing mutual subtraction. Why do you think that the rule in the *Nine Chapters* includes this division step? If one is simply trying to find the greatest common divisor of a and b, do you think that first dividing by a power of 2 has any advantages? Explain.

A Book of Numbers and Computations listed two different methods for simplifying fractions: the mutual subtraction algorithm and simply dividing numerator and denominator by common factors. The *Nine Chapters* combined these two techniques by first dividing by a power of 2, followed by mutual subtraction.

The mutual subtraction algorithm was the method the Chinese used for finding the greatest common divisor. Given positive integers a and b, the 'equal number' obtained by the mutual subtraction algorithm on a and b is the greatest common divisor of a and b. The notation $gcd(a, b)$ will be used to denote the greatest common divisor of the numbers a and b.[4]

The mutual subtraction algorithm is most useful when the numbers are large and hard to factor.

Task 11 Use the mutual subtraction algorithm to find $gcd(70056, 20447)$. Is this task any more difficult than using the mutual subtraction algorithm with small numbers? Explain.

What happens if the fraction is already simplified? What number does the algorithm find to be the greatest common factor?

Task 12 Find $gcd(26, 33)$.

1.3 Justifying the Mutual Subtraction Algorithm

The Chinese word for the 'equal number' was 'deng shu'. By the time Liu Hui published his commentary on the *Nine Chapters* in 263 CE, deng shu was also the technical name of the mutual subtraction algorithm [Dauben, 2008]. Liu comments first on the reason why fractions need to be simplified, then comments on the deng shu algorithm.

> Simplifying fractions: quantities of things cannot always be expressed in whole numbers, and fractions must be used to express them. Fractions as numbers are difficult to use if they are not simplified. For example, $2/4$ can be expressed in a more complicated way as $4/8$, or in a simpler way as $1/2$. Although expressed differently, the number [these fractions represent] is the same. Numerators and denominators mutually interact, changes make them larger or smaller, which is why those who created these methods chose to deal with fractions first.

[4] The notation (a, b) is often used in modern textbooks for the greatest common divisor of a and b

> "Use the equal number to simplify the fraction [i.e. the numerator and denominator]" means to divide [both the numerator and denominator by the common factor (the 'equal number')]. That which is mutually subtracted one from the other are all multiples of the equal number, and that is why it is possible to use the equal number to simplify the fraction.[5]

Liu claimed that every number in the mutual subtraction algorithm is divisible by the equal number.

Task 13 Do you agree with Liu's claim that every remainder in the mutual subtraction algorithm is divisible by the equal number? Why or why not? Use your work in the previous tasks to justify your answer.

On the surface, Liu's claim that all of the remainders in the mutual subtraction algorithm are multiples of the equal number seems to only imply that the equal number is a common factor of the original numbers. It is not as obvious that the equal number is the *greatest* common factor of the two numbers. Let's take a closer look at the implications of Liu's statement.

First, justify that the equal number is a common factor of the two original numbers by reversing the subtraction.

Task 14

(a) Explain why every remainder in the mutual subtraction algorithm for $gcd(49, 91)$ is a multiple of the equal number by starting with the equal number and reversing the subtraction steps from the last step backwards.

(b) Do the same for $gcd(162, 2016)$ using your work from Task 4.

(c) Examine your work in Task 11, is every remainder a multiple of $gcd(70056, 20447)$?

(d) Explain why every remainder in the mutual subtraction algorithm is a multiple of the greatest common divisor in the general case.

Why is the equal number the greatest common divisor, not just any common divisor? Use the next tasks to explore this question.

Task 15 To explore the connection between common factors and the greatest common factor, find $gcd(36, 60)$ by expressing 36 and 60 as multiples of different common factors and performing the mutual subtraction algorithm with the factored forms.

(a) Since $c = 2$ is a common factor of 36 and 60, find $gcd(36, 60)$ by finding $gcd(18c, 30c)$ using the mutual subtraction formula. What is the equal number as a multiple of 'c'?

(b) Using a common factor of $f = 3$, then $36 = 12f$ and $60 = 20f$. Use the mutual subtraction algorithm to find $gcd(12f, 20f)$. What is the equal number as a multiple of 'f'?

(c) Try the same procedure when $g = 4$ for $gcd(9g, 15g)$, and $h = 6$ for $gcd(6h, 10h)$.

(d) Finally, since $d = 12$ is a common factor, find $gcd(3d, 5d)$. What is $gcd(36, 60)$ as a multiple of 'd'?

[5] [Dauben et al., 2013]

(e) What is the difference between factoring 36 and 60 as multiples of their greatest commoon divisor compared with factoring 36 and 60 as multiples of smaller common divisors when finding the $gcd(36, 60)$?

Task 16 Consider the following concrete representation of $gcd(36, 60)$. Use an egg to represent one, and use standard egg cartons that hold 12 eggs to group the eggs. Thus, 36 is 3 full cartons of eggs and 60 is 5 full cartons of eggs. Mentally perform the mutual subtraction algorithm on the numbers 36 and 60 by subtracting eggs, taking away a whole carton for removing 12 eggs if possible. Do you ever have to open a carton in the subtraction process? Why or why not?

Task 17 Use the results of the last two tasks to explain why the equal number must be the greatest common divisor of the two original numbers.

In [Shen et al., 1999] Liu's justification of the mutual subtraction algorithm is translated as follows:

> Subtract the smaller number from the greater repeatedly, because the remainders are nothing but the overlaps of the GCD, therefore divide by the GCD.

Task 18 Does Liu's explanation of the mutual subtraction algorithm convince you that the 'equal number' is the greatest common divisor? Explain.

2 Euclid's Method

Finding the greatest common divisor of two positive integers is not just needed for simplifying fractions. In fact, the concept of the greatest common divisor is foundational in modern algebra and number theory. Therefore, it should come as no surprise that an algorithm is found in ancient Greek mathematics as well. An algorithm for finding the greatest common divisor of two numbers appears in Euclid's *Elements*.

2.1 Historical Background

There is almost nothing known about the life of Euclid beyond his writings. It is believed that he flourished in Alexandria, Egypt during the reign of Ptolemy I Soter (323-285 BCE). He wrote other books besides the *Elements*, but his lasting legacy is the logical development of what is now called Euclidean geometry in the *Elements*.

The *Elements* of Euclid was the most important mathematical text of ancient Greece, and is one of the most important mathematical texts of all time. Most ancient mathematical texts presented techniques for solving computational problems in arithmetic or geometry. Yet Euclid's text contains no numbers, no specific numerical computation. Instead, the *Elements* consists of definitions, axioms, theorems and proofs. Euclid set the standard for future mathematicians to justify new mathematical

truths by proving them with deductive logic. As students of mathematics, you are now part of this ancient tradition.

Euclid's *Elements* consists of thirteen books on geometry and number theory. Books I – VI develop the essential theorems of plane geometry. Book I gives a systematic presentation of familiar properties of triangles and parallelograms, culminating in a proof of the Pythagorean Theorem. Books VII – IX contain the basic ideas of number theory, which are the properties of the positive integers. Book VII Propositions 1 and 2 present Euclid's algorithm for finding the greatest common divisor of two numbers. Book X of the *Elements* concerns magnitudes instead of numbers. By magnitudes, Euclid is referring to arbitrary length, represented in modern terms as real numbers. Books XI-XIII address geometry in three dimensions, with a development of the Platonic solids in Book XIII.

In this section we will examine Euclid's algorithm and the proof he provides. The first goal is to understand the mechanics of Euclid's algorithm and compare it with the algorithm proposed by the ancient Chinese. Our second goal is to understand Euclid's proof.

2.2 Euclid's Definitions

Euclid started Book VII with 22 definitions of number theory terms. The partial list below includes the defintions of standard number theory terms as Euclid understood them, several of which show the geometric context of Euclid's discussion of numbers.

Book VII Definitions

(1). A unit is that by virtue of which each of the things that exist is called one.

(2). A number is a multitude composed of units.

(3). A number is *part* of a number, the less of the greater, when it measures the greater,

(4). but *parts* when it does not measure it.

(5). The greater number is a multiple of the less when it is measured by the less.

(6). An *even number* is that which is divisible into two equal parts.

(7). An *odd number* is that which is not divisible into two equal parts, or that which differs by a unit from an even number.

(11). A *prime number* is that which is measured by a unit alone.

(12). Numbers *prime to one another* are those which are measured by a unit alone as a common measure.

(13). A *composite number* is that which is measured by some number.

(14). Numbers *composite to one another* are those which are measured by some number as a common measure.

(15). A number is said to *multiply* a number when that which is multiplied is added itself as many times as there are units in the other, and thus some number is produced.

(16). And when two numbers having multiplied one another make some number, the number so produced is called *plane* and the sides are the numbers which have multiplied one another.

(17). And, when three numbers having multiplied one another make some number, the number so produced is *solid*, and the sides are the numbers which have multiplied one another.

Did you notice the geometry in Euclid's definitions?

Task 19 In Definitions 16 and 17, Euclid gave a geometric interpretation of multiplication. Restate each definition in your own words. Is this how you understand multiplication?

Notice that Euclid defined a number as 'a multitude of units'.

Task 20 Did Euclid consider 1 a number? Explain.

Task 21 What is the difference between a number being 'part of a number' versus 'parts of a number', according to Definitions 3 and 4?

Euclid's definition of 'part of a number' implies dividing a larger number into equal parts, and the smaller number thus being a factor of the larger number.

Task 22 Does 4 measure 10? Does 5 measure 10? Justify your answer using a geometric argument, representing numbers as line segments which are multiples of a unit length.

Given two integers a and b, the modern terminology for 'a measures b' is that 'a is a factor of b' or 'a is a divisor of b'.

Task 23 Is 4 a factor of 10? Is 5 a factor of 10? Is 15 a factor of 285? If so, write 285 as the product of 15 and another factor.

Task 24 Is Euclid's definition of a prime number the same as the modern definition? Justify your answer.

Euclid's definitions of prime and composite numbers are equivalent to the modern definitions. Two numbers a and b which are prime to one another in Euclid's definitions are called *relatively prime* in modern mathematics.

2.3 The Euclidean Algorithm

Book VII of the *Elements* started with two propositions that together describe Euclid's method for finding the greatest common divisor of two numbers. Every number is measured by a unit, since a number is made up of units. Euclid treated the case that the unit is the only common measure first, before proving the more general result. The subtraction process presented in Proposition 1 is similar to that in Proposition 2, so let's look at the procedure before we explore the proof.

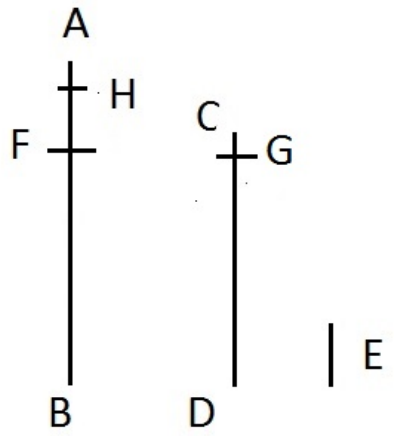

Figure 3: Book VII Proposition 1 Diagram

Book VII Proposition 1

Two unequal numbers being set out, and the less being continually subtracted in turn from the greater, if the number which is left never measures the one before it until a unit is left, the original numbers will be prime to one another.

Euclid's procedure sounds like the Chinese mutual subtraction algorithm, but let's look a little closer.

Task 25 When does the subtraction process stop, according to Euclid? Is this the same as the Chinese algorithm?

Task 26 Represent the numbers 21 and 25 as lines of respective lengths in units, either by physical manipulatives or as lines on ruled paper or graph paper. Subtract the smaller length from the lonnger length. Continue in this way until one remainder is a factor of the one before it. What happens? Are these numbers relatively prime?

Task 27 Try Euclid's procedure on the numbers 21 and 27. When does a remainder measure the one before it? Are 21 and 27 prime to one another?

Euclid's focus on geometry in much of the *Elements* spilled over into his representation of numbers as line segments of integral length, as we see in the diagram that accompanied his proof of Propostion I (shown in Figure 3). As you read this proof, notice that he did not prove that the numbers are relatively prime directly, but assumed that they are not and derived a logical contradiction.

Proposition 1 continued:

For, the less of two unequal numbers, AB, CD being continually subtracted from the greater, let the number which is left never measure the one before it until a unit is left.

I say that AB, CD are prime to one another, that is, that a unit alone measures AB, CD.

For if AB, CD are not prime to one another, some number will measure them.

Let a number measure them, and let it be E; let CD, measuring BF, leave FA less than itself, let AF, measuring DG, leave GC less than itself, and let GC, measuring FH, leave a unit HA.

Since, then, E measures CD, and CD measures BF, therefore E also measures BF.

But it also measures the whole BA, therefore it will also measure the remainder AF.

But AF measures DG, therefore E also measures DG.

But it also measures the whole DC, therefore it will also measure the remainder CG.

But CG measures FH, therefore E also measures FH.

But it also measures the whole FA, therefore it will also measure the remainder, the unit AH, though it is a number which is impossible.

Therefore no number will measure the numbers AB, CD, therefore AB, CD are prime to one another.

Task 28 When Euclid wrote 'For if AB, CD are not prime to one another, some number will measure them.', was he assuming that a unit is a number? Does this change your answer to Task 20? Why or why not?

To understand this proof, it will be helpful to first look at how the mechanics work with two specific numbers.

Task 29 Let $AB = 162$ and $CD = 31$.

(a) How many times must CD be subtracted from AB before the remainder is smaller than CD? Call this number k, and let $BF = k \times CD$ and FA be the remainder after the subtraction.

(b) Write $AB = BF + FA$ numerically.

(c) How many times must FA be subtracted from CD before the remainder is smaller than FA? Call this number m, and call the remainder DG. Also let $m \times FA = CG$.

(d) Write $CD = CG + GD$ numerically.

(e) How many times must DG be subtracted from FA before the remainder is smaller than DG? Let this number be s. Call this remainder HA, and let $FH = s \times DG$.

(f) Write $FA = FH + HA$ numerically.

(g) Explain why HA is a unit. Based on Proposition I, what can we conclude from this about $gcd(162, 31)$?.

Let's now return to the general proof of Proposition 1. Recall that Euclid proved that the numbers AB and CD are prime to one another by supposing that there is a number E which measures both and creating a contradiction.

Task 30

(a) Explain why E must be greater than 1.

(b) Since E measures CD and AB and $AB = BF + FA$, explain why E must also measure FA. Be sure to explain this carefully in the general case, not with specific numbers as in the previous task.

(c) Since E measures FA and CD, use $CD = CG + DG$ to explain why E must also measure DG. Again, justify this statement for arbitrary numbers, not just for a specific example.

(d) From $FA = FH + HA$ and the fact that E measures FA, explain why E must also measure HA.

(e) According to Euclid, HA is a unit. Why is the fact that E divides HA a contradiction?

Once Euclid established the method for determining if two numbers are prime to one another, Euclid's Book VII Proposition 2 explained how to find the greatest common divisor of two numbers which are not prime to one another. His presentation combined the proof and the method. Refer to Figure 4 for the diagram that accompanied Proposition 2.

Book VII Proposition 2

Given two numbers not prime to one another, to find their greatest common measure.

Let AB, CD be the two given numbers not prime to one another.

Then it is required to find the greatest common measure of AB, CD.

If now CD measures AB – and it it also measures itself – CD is a common measure of CD, AB. And it is manifest that it is also the greatest for no greater number than CD will measure CD.

But if CD does not measure AB, then, the less of the numbers AB, CD being continually subtracted from the greater, some number will be left which will measure the one before it.

For a unit will not be left; otherwise AB, CD will be prime to one another, which is contrary to the hypothesis.

Therefore some number will be left which will measure the one before it.

Now let CD, measuring BE, leave EA less than itself, let EA, measuring DF, leave FC less than itself, and let CF measure AE.

Since then CF measures AE, and AE measures DF, therefore CF will also measure DF.

But it also measures itself, therefore it will also measure the whole CD.

But CD measures BE, therefore CF also measures BE.

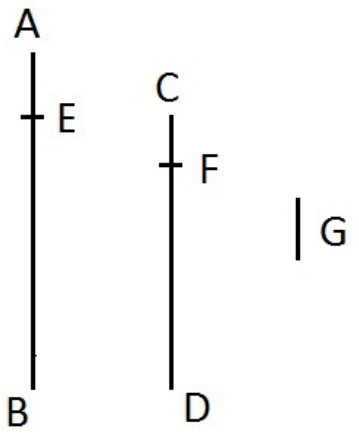

Figure 4: Book VII Proposition 2 Diagram

But it also measures EA, therefore it will also measure the whole BA.

But it also measures CD; therefore CF measures AB, CD. Therefore CF is a common measure of AB, CD.

I say next that it is also the greatest.

For if CF is not the greatest common measure of AB, CD, some number which is greater than CF will measure the numbers AB, CD.

Let such a number measure them, and let it be G.

Now, since G measures CD, while CD measures BE, G also measures BE.

But it also measures the whole BA, therefore it will also measure the remainder AE.

But AE measures DF, therefore G will also measure DF.

But it also measures the whole DC, therefore it will also measure the remainder CF, that is, the greater will measure the less, which is impossible.

Therefore no number which is greater than CF will measure the numbers AB, CD; therefore CF is the greatest common measure of AB, CD.

Porism

From this it is manifest that, if a number measures two numbers, it will also measure their greatest common measure.

A porism is a corollary to a theorem that arises as an immediate consequence of its proof.

Task 31 State Euclid's Porism in modern terminology. Do you believe that it is a direct consequence of the proof of Proposition 2? Explain.

Euclid first considered the case that CD measures AB. In this case, no subtraction is necessary. Go back and look at when the subtraction stopped in Proposition 1 and look at when the successive subtraction stopped in Proposition 2 to discover why no subtraction is necessary in this case.

Task 32 If CD measures AB, what is the greatest common divisor of CD and AB? Carefully explain why this number must be their greatest common divisor.

If neither of the two numbers is a divisor of the other, Euclid instructed us to subtract the smaller from the larger number successively until one remainder divides the one before it. Notice that this is the same instructions as in Proposition 1, but now the final remainder is not a unit. Euclid's proof of Proposition 2 first demonstrated that this final remainder, which is denoted CF in the proof, is a common measure to both AB and CD. Let's explore this with a concrete example, and then in general.

Task 33 Let $AB = 81$ and $CD = 33$.

(a) How many times must CD be subtracted from AB before the remainder is less than CD? Call this number q_1 and call the remainder EA.

(b) Write $AB = q_1 \times CD + EA$ numerically.

(c) Let $BE = q_1 \times CD$ and write $AB = BE + EA$.

(d) How many times must EA be subtracted from CD before the remainder is less than EA? Call this number q_2 and call the remainder CF.

(e) Write $CD = q_2 \times EA + CF$ numerically.

(f) Let $DF = q_2 \times EA$ and write $CD = DF + CF$ numerically.

(g) Does CF divide EA? If so, call the quotient q_3.

(h) Is CF the greatest common divisor of AB and CD?

Let's return to the proof of Proposition 2 in the general case.

Task 34 In Euclid's proof of Proposition 2, CF was the final result of the subtraction algorithm. Our goal in this task is to prove that CF is a common divisor of AB and CD for arbitrary numbers AB and CD.

(a) Does CF measure DF? Why or why not.

(b) Using the facts that CF measures EA and $CD = DF + CF$, carefully explain why CF also measures CD.

(c) Explain why CF measures BE.

(d) From $AB = BE + EA$, explain why CF measures AB.

(e) Explain why CF is a common divisor of AB and CD.

At this point, we have a proof that the final remainder in the successive subtraction procedure is a common divisor of our original two numbers, but this by itself does not prove that it is the largest common divisor. To prove that CF is the largest common divisor, use the next task to follow Euclid's method.

Task 35 Euclid supposed that G is greater than CF and is a common measure of AB and CD.

(a) Since G measures CD, explain why it also measures BE.

(b) From $AB = BE + EA$, explain why G measures EA.

(c) If G measures EA, explain why it also measures DF.

(d) From $CD = DF + CD$, explain why G measures CF.

(e) What contradiction is created by G measuring CF?

Consider a second numerical example now that you have practiced the mechanics of Euclid's proof.

Task 36 Let $AB = 171$ and $CD = 120$.

(a) How many times must CD be subtracted from AB before the remainder is less than CD? Call this number q_1 and call the remainder EA.

(b) Write $AB = q_1 \times CD + EA$ numerically.

(c) How many times must EA be subtracted from CD before the remainder is leass than EA? Call this number q_2 and call the remainder CF.

(d) Write $CD = q_2 \times EA + CF$ numerically.

(e) Does CF divde EA? If not, continue subtracting until the final remainder divides the one before it.

(f) What is the greatest common divisor of 171 and 120?

Euclid's proof assumed that CF divides EA, yet Task 36 shows us that does not work in every case.

Task 37 Is Euclid's proof invalid because CF does not divide EA in every example? Explain.

Task 38 Explain how to adapt Euclid's proof to cases where more subtraction steps are needed.

Many mathematicians, including the author of this project, consider Euclid's proof of the Euclidean Algorithm to be very elegant.

Task 39 What do you think are the characteristics of Euclid's proof of Proposition 2 that leads modern mathematicians to think that it is elegant? Do you agree or disagree with their assessment of this proof?

3 A Modern Approach

The Euclidean algorithm is essentially the same as that described by Euclid 2300 years ago. However, in this section the algorithm will be presented in modern language with formal algebraic notation. As you read, notice the similarities and differences between the ancient and modern presentation.

3.1 Integer Division and the Greatest Common Divisor

Task 40 Consider the set of non-negative integers $\mathbb{Z}^+ = \{0, 1, 2, 3, 4, 5, \dots\}$. List as many properties of this set as you can.

Here is one of the fundamental properties of the set of non-negative integers. Did you include it in your list of properties? Notice that it is called an axiom, a property that is assumed without proof.

Theorem 1 (Well-Ordering Axiom) *Every non-empty subset of non-negative integers contains a smallest element*

The Well-Ordering Axiom seems obvious, but it is not trivial.

Task 41

(a) Given any non-empty set of integers, must it have a smallest element?

(b) Does the set of positive rational numbers satisfy the Well-Ordering Axiom? If so, explain why. If not, give an example of a non-empty set without a smallest element.

(c) Does the set of positive real numbers satisfy the Well-Ordering Axiom? If so, explain why. If not, give an example of a non-empty set without a smallest element.

It is a well-known fact that the product of any two positive integers is a positive integer. However, division does not always work out evenly. In order to restrict our domain of interest to integers, it is necessary to consider division with quotient and remainder. For example, 15 divided by 6 is not an integer, but 6 goes into 15 twice with a remainder of 3. The formal algorithm for this is called the Division Algorithm, and its proof relies on the Well-Ordering Axiom.

Theorem 2 (The Division Algorithm) *Let a and b be integers with $b > 0$. Then there exists unique integers q and r such that*

$$a = qb + r \quad \textit{and} \quad 0 \leq r < b$$

The division algorithm first asserts that the quotient and remainder always exist. The next task proves this claim.

Task 42 Let a and b be integers with $b > 0$. Construct the set $S = \{a - kb | k \in \mathbb{Z}\}$ and let S^+ be the set of non-negative integers in S.

(a) Suppose $a = 27$ and $b = 6$. Describe the set S for this specific example. What is the smallest non-negative integer in S?

(b) Find the quotient and remainder when 27 is divided by 6. How are these numbers related to the smallest non-negative integer in S?

(c) For the general case of arbitrary values of a and b as stated in the theorem, explain why S^+ must be non-empty.

(d) In the general case, justify the claim that S^+ has a least element.

(e) Let r be the least element in S^+. Define q such that $r = a - bq$. Why must r be less than b?

(f) Find r and q when $a = 40$ and $b = 12$.

The existence of the quotient, q, and remainder, r, is only part of the division algorithm. The full statement of the algorithm asserts that q and r are unique. Use the next task to justify this claim.

Task 43 One technique for proving uniqueness of a number is to assume that two possibilities exist and then demonstrate that these two numbers are in reality the same. Given any integer a and any positive integer b, assume that there exists integers r_1 and q_1 such that $a = q_1 b + r_1$ with $0 \leq r_1 < b$. Further assume that there exists a second pair of integers q_2 and r_2 such that $a = q_2 b + r_2$ and $0 \leq r_2 < b$. Assume that we have labeled the integers so that $r_2 \geq r_1$.

(a). Find an algebraic expression for $r_2 - r_1$ in terms of b, q_1 and q_2.

(b). If $r_2 - r_1 = 0$, explain what this means about q_2 and q_1.

(c). Why is $r_2 - r_1 > 0$ impossible?

(d). Use the results of Parts (a)-(c) to prove that the quotient and remainder in the division algorithm are unique.

With integer division (with quotient and remainder) as one of our useful tools, there is special notation for when the remainder is zero. Informally, if $a = qb + 0$, b is called a factor of a, or b is a divisor of a. In formal abstract algebra, we say b divides a.

Definition 3 *Given integers a and b. Then b divides a, denoted $b|a$, if there exists an integer k such that $a = bk$.*

Task 44 Given integers a and b. Prove that if $b|a$, then $|b| \leq |a|$.

Since the positive divisors of a positive integer a are less than or equal to a, there are a finite number of divisors of a.

Task 45 Given integers a and b, why must they have a common divisor?

Any two positive integers have a common divisor, so the question that the ancients asked is still interesting: What is their *greatest* common divisor? The following is a formal definition of the greatest common divisor.

Definition 4 *Let a and b be positive integers. The positive integer d is called the greatest common divisor of a and b, denoted $gcd(a, b)$, if the following conditions hold:*

1. *$d|a$ and $d|b$,*
2. *If there exists an integer c such that $c|a$ and $c|b$, then $c \leq d$.*

How do we find the greatest common divisor of two positive integers? The algorithm of the ancients is still the simplest and most efficient choice. The Euclidean algorithm is restated below using modern variable notation. Notice that in this statement the two original numbers are called a_0 and a_1 and the successive remainders at step i are denoted a_{i+1}.[6]

[6]There are multiple ways to write this notation, but this particular notation was chosen to create the sequence of original numbers and remainders with consistent notation.

Theorem 5 (The Euclidean Algorithm) *Let a_0 and a_1 be positive integers, and assume $a_0 \geq a_1$. There exists a non-negative integer n, a sequence of non-negative integers $a_0, a_1, a_2, a_3, a_4, a_5, \ldots, a_{n+1}$ and a sequence of integer multipliers $q_1, q_2, q_3, \ldots, q_n$ such that*

$$\begin{aligned} a_0 &= q_1 a_1 + a_2 & 0 < a_2 < a_1 \\ a_1 &= q_2 a_2 + a_3 & 0 < a_3 < a_2 \\ &\vdots \\ a_{k-1} &= q_k a_k + a_{k+1} & 0 < a_{k+1} < a_k \\ &\vdots \\ a_{n-1} &= q_n a_n + a_{n+1} & 0 < a_{n+1} < a_n \\ a_n &= q_{n+1} a_{n+1}. \end{aligned} \tag{2}$$

Then a_{n+1} is the greatest common divisor of a_0 and a_1.

Task 46 Why did Euclid treat relatively prime numbers as a separate proposition, but the modern statement of the algorithm does not make that distinction?

3.2 Modern Proofs

We will examine two different approaches to the proof of the Euclidean algorithm in this section.

3.2.1 Proof 1

The goal of the first proof is to show that the last nonzero remainder is a common factor of the original numbers a_0 and a_1 and then show that it must be the greatest common factor. Notice that the structure of this proof is similar to Euclid's proof..

First, it is necessary to show that a_{n+1} ia a common factor of a_0 and a_1.

Task 47 First, if $n = 0$ (if $a_0 = q_1 a_1$), explain why $gcd(a_0, a_1) = a_1$.

Task 48 For an integer $0 < k \leq n$, if $a_{n+1} | a_{k+1}$ and $a_{n+1} | a_k$, explain why $a_{n+1} | a_{k-1}$. Use this information and the previous task to construct an recursive proof that a_{n+1} is a common divisor of a_0 and a_1.

At this point, we know $a_{n+1} | a_0$ and $a_{n+1} | a_1$. In order to prove that $a_{n+1} = gcd(a_0, a_1)$, it is necessary to prove that it is the greatest common divisor. The next task will accomplish this.

Task 49

(a) Suppose $c | a_0$ and $c | a_1$. Why does $c | a_2$?

(b) Use a recursive proof to show that $c | a_i$ for all $0 \leq i \leq n + 1$.

(c) Explain why $c \leq a_{n+1}$.

Note that the previous task shows that $c | gcd(a_0, a_1)$ whenever c is a common divisor of a_0 and a_1. We could restate the definition of the greatest common divisor in the following manner.

Definition 6 *Let a and b be positive integers. The positive integer d is called the greatest common divisor of a and b, denoted $gcd(a, b)$, if the following conditions hold:*

1. *$d|a$ and $d|b$,*

2. *If there exists an integer c such that $c|a$ and $c|b$, then $c|d$.*

Task 50 Explain how Definition 6 is connected to Euclid's Porism.

Task 51 [Optional] Prove that Definition 4 and Definition 6 are logically equivalent.

3.2.2 Proof 2

The second approach focuses on the full implications of a single division step on the greatest common divisor. This is encapsulated in the following lemma.

Lemma 7 *Given positive integers a and b with $a > b$. Applying the division algorithm, there exists integers q and r with $0 \leq r < b$ such that $a = qb + r$. Then $gcd(a, b) = gcd(b, r)$.*

The next task proves Lemma 7.

Task 52 Follow the following steps to prove Lemma 7.

(a) First, it is necessary to prove that if $d = gcd(a, b)$, then d is also the greatest common divisor of b and r. To begin, assume $d = gcd(a, b)$. Show that $d|b$ and $d|r$. This shows that d satisfies the first property of the $gcd(b, r)$.

(b) Given an integer w, suppose $w|b$ and $w|r$. Explain why w divides a.

(c) Still assuming $w|b$ and $w|r$, prove that $w < d$.

(d) Explain why $d = gcd(b, r)$.

(e) Prove the reverse implication. Assume that $d = gcd(b, r)$ and use a similar argument to show that $d = gcd(a, b)$.

With the proof of Lemma 7 in hand, the proof of the Euclidean algorithm starts from the last step of the algorithm.

Task 53

(a) Since $a_n = q_{n+1}a_{n+1}$, explain why $gcd(a_n, a_{n+1}) = a_{n+1}$.

(b) Let k be an integer such that $0 < k \leq n$. If $gcd(a_{k+1}, a_k) = a_{n+1}$, explain why $gcd(a_k, a_{k-1}) = a_{n+1}$.

(c) Use the ideas from parts (a) and (b) to construct a proof of the Euclidean algorithm.

4 A Comparison of Proof Methods

The Euclidean algorithm appeared in the *Elements* ca. 300 BCE and independently in China in the *Book of Numbers and Computations* ca. 200 BCE. The algorithm remains the most efficient method for finding the greatest common divisor of two large integers 2300 years later. The ancient mathematicians in Greece and China understood the fundamental properties of integer division and knew how to utilize them effectively to create a timeless algorithm. Although the algorithm is

essentially the same across the centuries, how it was justified was very different in different times and places.

The mathematics presented in the *Book of Numbers and Computations* and the *Nine Chapters* was very practical and concrete. Problems were solved with specific numbers, not with general terms. Procedures were spelled out for solving common problems encountered in government, business and engineering. There were no theorems or proofs with deductive logic as seen in Greek mathematics. Some have drawn the conclusion that the ancient Chinese were not concerned with proofs at all. However, this is not a fair assessment of ancient Chinese mathematics [Chemla, 2012].

The *Nine Chapters* contains 246 specific problems, yet it also contains general rules, like the 'Rule for Simplifying Fractions'. The instructions for finding the equal number were clearly meant for arbitrary positive integers, not just the specific problems in the text. Even the specific problems were meant to be generalized. Liu's comments make it clear that Chinese mathematicians were concerned with the correctness of the algorithms. However, their justifications of the algorithms were much more concrete. As Dauben pointed out, this can be explained in part by linguistic issues [Dauben, 1998]. The ancient Chinese language did not easily generalize from concrete properties to abstract concepts, as moving from 'soft' to 'softness'. The ancient Chinese thus did not have the language of abstract deductive logic readily available. Their focus was on the practical solution to problems and concrete explanations of the correctness of the procedures to solve them.

Another distinction in ancient Chinese mathematics is the absence of proof by counter-factual reasoning (proof by contradication)[Dauben, 1998]. In fact, this type of reasoning is not present in any logical or philosophical work. The strategy of proving that the equal number is the largest of the possible common divisors by assuming that it is not and deriving a contradiction simply would not have occurred to Liu Hui.

Task 54 Did you use a proof by logical contradiction in your justification of the Chinese mutual subtraction algorithm in Task 17? If so, why? If not, would it be easier to assume that the equal number is not the greatest common divisor and then derive a logical contradiction?

Task 55 Do you think that proof by contradiction is a believable method of proof? Why or why not?

Modern mathematicians comparing ancient Chinese and Greek mathematics often point to the lack of proofs in the Chinese texts. However, the real story is the presence of proofs in ancient Greece. Greek mathematics was unique in the ancient world for its focus on abstract ideas and formal proofs using deductive logic. Euclid set the standard for carefully proving mathematical truths from axioms and definitions. His proof of the Euclidean algorithm is well constructed. Yet there are two points in which his proof is different from modern proofs. First, Euclid did not consider one a number, requiring the separation of the case in which the numbers are prime to one another from the case in which the greatest common divisor is greater than one. Second, Euclid did not explicitly address the iterative nature of the algorithm in that he assumed that the subtraction stopped after a certain number of steps. Neither issue implies his proof is incorrect, each illustrates the notational limitations of his time and place.

Modern mathematicians see the value in both the practical and the theoretical. The explanation that the remainders in the mutual subtraction algorithm are all multiples of the greatest common divisor would satisfy most people as to the correctness of the algorithm. However, an algorithm as important as the Euclidean algorithm can also be formally proven from the basic properties of the integers. As students of mathematics, you may have encountered topics in which the obvious is not

the whole story (non-Euclidean geometry being one example). Therefore, you will need to know on which principles a mathematical truth is based, and be able to justify it using these principles and the tools of deductive logic.

Task 56 Some would contrast the Chinese and Euclid's proofs and claim one was 'better' than the other. Explain in your own words why this is not a proper comparison.

Finally, it is important to recognize the similarities in the proofs.

Task 57 Given positive integers a and b, let d be the number found by the subtraction algorithm.

(a) How does Liu's explanation of the ancient Chinese algorithm explain why d is a common divisor of a and b?

(b) How does Euclid explain the fact that d is a common divisor of a and b?

(c) Does the modern proof explain why d is a common divisor of a and b? Which version of the modern proof gives a clearer explanation?

Task 58 The Euclidean algorithm would not be nearly as useful if it only found a common divisor, not necessarily the greatest common divisor. In the justification of the algorithm, it is necessary to convince the reader that the number the algorithm produces is really the largest common divisor. Examine each of the justifications given in this lesson (ancient Chinese, Euclid or one of the two modern proofs), specifically looking at how they justify the "greatest" claim in the greatest common divisor.

(a) Do Liu's comments convince you that the equal number is the greatest of common divisors? Explain why or why not.

(b) Does Euclid prove this claim? Explain.

(c) How is the "greatest" claim proven in the modern proofs? Which proof would you use to convince another person that the claim is true? Explain.

Task 59 Which proof is most convincing to you? Explain why.

(a). Greek vs. Chinese

(b). Greek vs. Chinese vs. Modern

(c). Modern Proof 1 vs. Modern Proof 2

In the final analysis, the commonality of the algorithms and the proofs is more important than the differences. The end result is a correct and beautifully simple algorithm for finding the greatest common divisor of two integers, which relies solely on subtraction (or division with quotient and remainder as a shortcut for repeated subtraction). The differences in the proofs are most important as illustrations of the ways different communities have understood the nature of mathematics. This understanding continues to evolve, and you will play a role in its evolution.

References

Karine Chemla. Different concepts of equations in the Nine Chapters on Mathematical Procedures and in the commentary on it by Liu Hui (3rd century). *Historica Scientarum*, 4(2):113–137.

Karine Chemla. *The history of mathematical proof in ancient traditions / edited by Karine Chemla.* Cambridge University Press, 2012.

Joseph W. Dauben. Ancient Chinese mathematics: the Jui Zhang Suan Shu vs. Euclid's Elements. aspects of proof and the linguistic limits of knowledge. *International Journal of Engineering Science*, 36:1339–1359, 1998.

Joseph W. Dauben. Suan shu shu a book on numbers and computations: English translation and commentary. *Arch. Hist. Exact Sci.*, 62:91–178, 2008.

Joseph W. Dauben, GUO Shuchun, and XU Yibao. *Nine Chapters on the Art of Mathematics. A Critical Edition and English Translation based upon a New Collation of the Ancient Text and Modern Chinese Translation. Library of Chinese Classics.* Number 6. Shenyang: Liaoning Education Press, 2013.

Euclid. *Euclid's Elements : all thirteen books complete in one volume : the Thomas L. Heath translation / Dana Densmore, editor.* Green Lion Press, Santa Fe, N.M., 2002.

Victor J. Katz. *A history of mathematics: an introduction.* Harper Collins College Publishers, New York, 1993.

Jean-Caude Martzloff. *A History of Chinese Mathematics.* Springer-Verlag, Berlin Heidelberg.

Kangshen Shen, John N. Crossley, and Anthony W.-C. Lun. *The nine chapters on the mathematical art: companion and commentary.* Oxford University Press, New York; Science Press Beijing, Beijing, 1999.

Shu-Chun Guo. *Jui Zhang Suan Shu Hui Jiao (Comprehensive annotation of the Jui Zhang Suan Shu).* Liaoliang Jiao Yu Press, Shenyang and Taiwan Nine Chapters Press, Taipei, 1990.

Alexei Volkov. Commentaries upon commentaries: The translation of the jiu zhang suan shu by karine chemla and guo shuchun (book review). *Historia Mathematica*, 37(2):281–301, 2010. ISSN 0315-0860.

Notes to Instructors

This project introduces the Euclidean algorithm and its proof both in the texts of ancient China and in Euclid's *Elements*. It is designed for an introduction to proof class in number theory, discrete math or abstract algebra. No previous experience in number theory is assumed, although it assumes students have some familiarity with recursion. A short introduction in the context of the Modern Proof section may be included if an instructor wishes.

The most important goal of this project is a study of proof techniques from ancient times to today's modern proofs. The simple justification of the Chinese algorithm by Liu Hui and Euclid's elegant and involved proof are so different and yet so similar. This story is a beautiful study in language and convention across the ages. The culmination of the project examines the language and conventions that are accepted within today's context of formal mathematics.

Another goal of this project is to show the common origins of the Euclidean algorithm in China and Greece. Although Euclid's algorithm appeared first in the historical record, the Chinese version is discussed first because the author wishes to emphasize that Euclid was not the only mathematician who discovered the algorithm. This is followed by a presentation of Propositions 1 and 2 of Book VII of Euclid's *Elements*.

The third goal is to show the same algorithm in different contexts, just as the greatest common divisor appears in multiple different contexts in modern mathematics. The Chinese algorithm was intended for reducing fractions, which remains the first place a student will encounter the need for it. The project presents the Chinese algorithm in multiple sources from different times, giving students the opportunity to see it's historical development in China. Euclid's presentation is the beginning of his books on number theory, which is the application undergraduate students are likely to need. Yet, Euclid's number theory results are in the middle of his geometry book, hence the numbers have a geometric interpretation. His description of dividing is exactly measuring a line segment of integral length.

Implementation Suggestions

The full PSP may be covered in 3-4 75-minute class sessions, using a combination of preparatory reading, class discussion and small group work. Instructors with a 50-minute class period should adjust this schedule to fit their needs. Instructors may address an individual development in China or Greece separately, omitting the comparison questions with the other. The following sample implementation plan was developed by the author for a junior level course on discrete mathematics (which is also the introduction to proofs course in many mathematics programs).

Day 1: Ancient China

Preparation: Students are asked to read pages 1–5 as introduction and work Tasks 1–4 on the mutual subtraction algorithm from the *Suan Shu Shu*. These tasks check reading comprehension and ask the students to try two algorithms, finding common factors and mutual subtraction.

Class Work: Work in small groups (3–4) is suggested, along with students sharing results and questions with the whole class. The work is accomplished in three steps.

1. The procedure from the *Suan Shu Shu* assigned for reading is discussed by the group with work on Task 4, followed by a short class discussion of results.

2. The procedure from the *Nine Chapters* is read with group work chosen from Tasks 5–12.
3. The justification is examined by having groups read Liu's comments and work on Tasks 13–16.

Homework: Unfinished tasks and especially Tasks 17 and 18 would work well as reflective questions on the Chinese algorithm.

Day 2: Euclid

Preparation: Read Sections 2.1, 2.2 and up through Task 25 in Section 2.3. Work some or all of Tasks 18-25.

Class Work:
1. Class discussion on Euclid's definitions and questions that arose while reading the preparatory assignment.
2. Group work on Tasks 25–27 on the implementation of the algorithm and comparison with the Chinese mutual subtraction algorithm.
3. Group work on the proof of Proposition 1. Encourage students to use Task 29 to follow the proof in a concrete manner.
4. Group work on Euclid's Porism in Task 31 and the proof of Proposition 2 with the aid of Tasks 32, 33 and 36.

Homework: Instructors should ask students to generalize their proofs as homework. (Tasks 30, 34, 35). One option is to require formal proofs completely as homework due a week later. A second option is to use these exercises as the preparation for the next class in which groups will work together on the formal proofs.

Optional Day 3 on Euclid

A four day implementation of the PSP would include a second day of class work on understanding Euclid's proof, using Tasks 30, 34 and 35 with group presentations. The class would also investigate Tasks 36–38 on the issue of requiring more subtraction steps than those written in Euclid's proof. Instructors may also opt to assign this material as homework done individually outside of class.

Day 3 or 4 Modern Notation and Proof

- Class discussion on Section 3.1 on the modern presentation of the Euclidean algorithm.
- Group work on modern proofs, Section 3.2.
- Finish with a comparison of the proofs and assign tasks in Section 4 as individual homework due a week later.

Content and Intentions of the Tasks

China

1. Instructors may ask students how to find the greatest common divisor of two small numbers before introducing the PSP. Answers are likely to involve prime factorization, which provides a point of conversation about the difficulties of factoring.

2. The chart in Task 4 is meant to help them organize the subtraction. The Chinese rod arithmetic literally removed rods from a number to subtract, so there was no record of the steps. However, we want a record of the steps for observing claims about the remainders in Task 13.

3. Task 15 asks students to consider the original numbers as groups of common size, demonstrating common divisors. A physical illustration of grouping helps students understand the concepts.

4. The concrete egg carton grouping in Task 16 was very helpful to the author's students.

5. There are no wrong answers to whether Liu's explanation is convincing

Euclid

1. Proposition 1 of Book VII is presented, then the tasks ask students to compare the instructions with those of the Chinese, before reading the rest of the proof. This is done so that the student's may explore the differences in the instructions for subtraction right when they are presented, before the line segments are introduced.

2. It is extremely helpful to follow Euclid's proof with concrete numbers before explaining it abstractly, hence the concrete tasks first.

3. Task 36 asks students to perform the Euclidean algorithm with two numbers that require more subtraction (division) steps than given in the proof. The purpose is to ask the students to generalize the method.

Modern Proofs

1. Tasks 48, 49 and 53 require a recursive argument to prove properly in the sense that recursion guarantees that the claims hold regardless of the number of steps in the algorithm.

2. Two different proofs are given. Proof 1 is similar to Euclid's, first proving that the final number is a common divisor, then showing it must be the greatest one. Proof 2 is based on the fact that the greatest common divisor of the two remainders (including the original numbers) does not change with each subtraction step.

3. Task 51 is optional for the argument, yet is essentially the proof of Euclid's Porism in modern language.

A Comparison of Proof Methods

1. Task 54 asks students to go back and look at Liu's argument in the light of the fact that proof by contradiction was not part of the ancient Chinese vocabulary. Did they use a proof by contradiction developed from the ideas presented?

2. Tasks 57 and 58 ask students to find the common themes in all four proofs presented in the lesson.

3. Task 59 is a tough call for the author, Liu's remainders as 'overlaps of the greatest common divisor', Euclid's beautiful (but tedious) proof or modern language and notation. Encourage a thoughtful answer!

LaTeX code of this entire PSP is available from the author by request to facilitate preparation of 'in-class task sheets' based on tasks included in the project. The PSP itself can also be modified by instructors as desired to better suit their goals for the course.

Acknowledgments

The development of this project has been partially supported by the TRansforming Instruction in Undergraduate Mathematics vis Primary Historical Sources (TRIUMPHS) Project with funding from the National Science Foundation's Improving Undergraduate STEM Education Program under Grants No. 1523494, 1523561, 1523747, 1523753, 1523898, 1524065, and 1524098. Any opinions, findings, conclusions or recommendations expressed in this project are those of the author and do not necessarily reflect the views of the National Science Foundation.

For more information about TRIUMPHS, visit `http://webpages.ursinus.edu/nscoville/TRIUMPHS.html`.