Summer 2020

Cross-Cultural Comparisons: The Art of Computing the Greatest Common Divisor

Mary K. Flagg

University of St. Thomas - Houston, flaggm@stthom.edu

Cross-Cultural Comparisons:
The Art of Computing the Greatest Common Divisor

Mary Flagg*

August 18, 2020

Foundational mathematical concepts appear in the written record of many different ancient civilizations. Each group independently figured out how to do essential arithmetic and geometry, discovering the same relationships. The greatest common divisor of two counting numbers is one of these foundational ideas in arithmetic. In this project we will encounter the ideas of the ancient Chinese and Greek mathematicians, and discover that they had similar algorithms for finding the greatest common divisor.

This shared ancient algorithm for finding the greatest common divisor is called the Euclidean algorithm in Western mathematics and it appears in important texts from ancient China and Greece. Sections 1 and 3 describe the history and content of these two texts. The Euclidean algorithm itself remains important in many branches of modern mathematics. It is used in elementary mathematics to simplify fractions, and also in basic number theory. Beyond abstract mathematics, it is used to find keys for the RSA cryptosystem, which is the basis for all internet encryption. The Chinese version of the algorithm in the context of simplifying fractions is the topic of Section 2. Section 4 introduces the ancient Greek definitions in basic number theory and presents Euclid's version of the algorithm. Sections 2 and 4 are organized similarly: context, then computation and finally a discussion of how each civilization justified the correctness of their algorithm. Section 5 compares the ancient algorithms and contrasts the ancient subtraction method to factoring methods taught in primary schools today. The purpose is to discover that the Euclidean algorithm is a simple and efficient method for finding the greatest common divisor, suitable for elementary school students.

1 A Classic Chinese Mathematical Text: *The Nine Chapters on the Mathematical Art*

The algorithm for finding the greatest common divisor appeared in foundational mathematics texts from ancient China and Greece [Katz, 1993]. This section is a brief overview of the history and content of the Chinese text that you will study in this project.

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

1.1 The Text

The rules for fractions and the algorithm for finding the greatest common divisor appeared in the *Jiuzhang Suanshu*[1] which has been translated into English as *The Nine Chapters on the Mathematical Art* in [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 remains the fundamental source of traditional Chinese mathematics. *The Nine Chapters* was an anonymous text, compiled across generations of mathematicians. It is believed that the original text was compiled before the end of the first century BCE, but it is difficult to date precisely.

The Nine Chapters is a series of 246 problems and their solutions organized into nine chapters by topic. The topics indicated that the text was meant for addressing the practical needs of government, commerce and engineering. The problems and solutions did 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, gives the rules for arithmetic with fractions, 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: The problems in this chapter involve distribution of commodities using direct, inverse or compound proportions.

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 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.

[1] See [Guo, 1990] for the Chinese text.

[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.

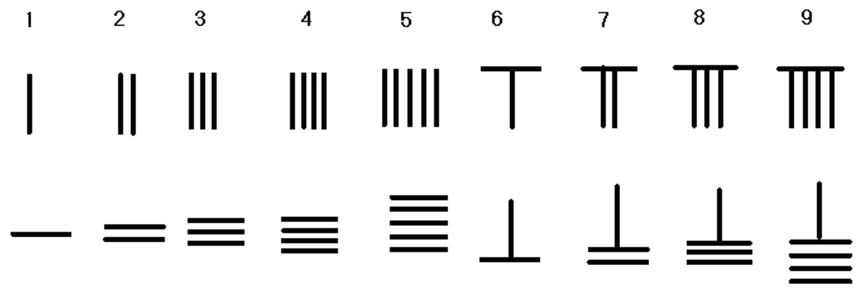

Figure 1: Vertical and Horizontal Counting Rod Numerals

The noted Chinese mathematician Liu Hui, who lived in the third century CE, published an annotated version of *The Nine Chapters* in the year 263 CE [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.

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 approximately 500 BCE until 1500 CE. Counting rods were gradually replaced with the abacus during the Ming Dynasty (1368–1644 CE) [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 a base ten number. 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 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 a symbol for zero is so useful in our modern system of numeration?

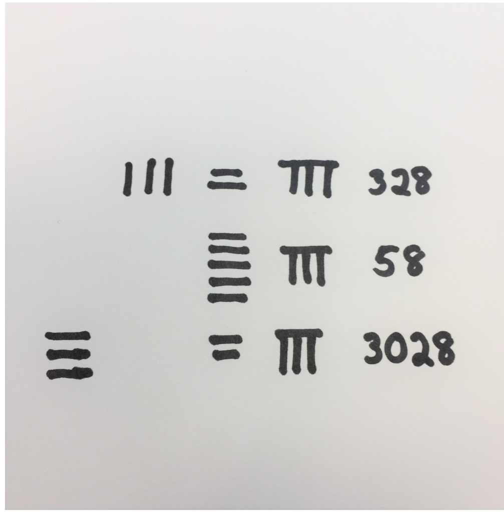

Figure 2: Examples of Rod Numbers

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 appeared in the instructions for finding the greatest common divisor in *The Nine Chapters*.

2 The Mutual Subtraction Algorithm from China

Problems 5–24 of Chapter 1 of *The Nine Chapters* concerned arithmetic with fractions and mixed numbers.

2.1 Context: Simplifying Fractions

The algorithm for finding the greatest common divisor of two whole numbers appeared as the first rule for fraction arithmetic. The presentation of fractions began with the following two problems:

Problem 5: Suppose there are $12/18$.
The Question: Simplifying the fraction gives how much?
The Answer: $2/3$.

Problem 6: Again, suppose there are $49/91$.
The Question: Simplifying the fraction gives how much?
The Answer: $7/13$.[3]

Task 1 Explain what simplifying fractions means in your own words.

[3] The English translation of this excerpt is taken from [Dauben et al., 2013].

In his comments, Liu Hui explained why he thought the rules for fractions appeared so early in *The Nine Chapters* and why simplifying fractions was so important.

[Liu Hui] comments: 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]

Task 2 According to Liu Hui, is $\frac{2}{4}$ a simplified version of $\frac{4}{8}$? Explain why or why not. Do you agree with him? Again, explain why or why not.

Did you notice that the simple examples given in Problems 5 and 6 at the start of this subsection only gave the answers, without explaining how they were found? *The Nine Chapters* did give a general rule for simplifying fractions, which presumably was used to find those answers. We will look at that rule in the next subsection of this project. Because those two problems are fairly simple, however, they can also easily be done using an older rule for simplifying fractions found in a text from the early second century BCE. 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 the following rule:

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.[5]

Some mathematical methods have not changed in thousands of years. We still teach students to simplify fractions by dividing by common factors.

[4] The English translation of this excerpt is taken from [Dauben et al., 2013].
[5] The English translation of this excerpt is taken from [Dauben, 2008].

$\boxed{\textbf{Task 3}}$ Simplify the fractions $\frac{12}{18}$ and $\frac{49}{91}$ by using the rule from the *Suan She Shu.*.

Simplifying a fraction by dividing numerator and denominator by common factors may require more than one division step if all of the common factors are not immediately obvious.

$\boxed{\textbf{Task 4}}$ Simplify the fraction $\frac{84}{126}$ by dividing by common factors. How many division steps did you need to simplify the fraction?

Did you start the last task by noticing that 84 and 126 are both even and divide by 2? There are other common factors between 84 and 126, but dividing by 2 first is an obvious first step. When the numerator and denominator are not both even, finding common factors may require more effort.

$\boxed{\textbf{Task 5}}$ Consider the fraction $\frac{399}{714}$.

(a) Find a common factor between 399 and 714.

(b) Simplify the fraction by dividing the numerator and the denominator by this common factor.

(c) Is the resulting fraction in simplest form? How do you know?

(d) Explain how you can determine if the fraction found in part (b) is in simplest form.

2.2 Computation: Mutual Subtraction

Simplifying fractions formed from larger numbers, like those in Task 5, illustrates the usefulness of having a better algorithm for finding the greatest common divisor of two numbers. In this subsection, we will take a closer look at how to compute the greatest common divisor with the ancient Chinese algorithm given in *The Nine Chapters*.

Let's start by reading the algorithm.

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.[6]

$\boxed{\textbf{Task 6}}$ Write at least one comment and at least one question about the statement of this algorithm.

[6] The English translation of this excerpt is taken from [Dauben et al., 2013].

Task 7 Why do you think that the rule for simplifying fractions in *The Nine Chapters* included the instructions for dividing numerator and denominator by 2, but did not suggest finding any other common factors?

Computation was done in ancient China by physically manipulating counting rods on a counting board. Do you see the reference to the counting board in the instructions? Counting rod numerals are unfamiliar to most modern readers, and therefore they will not be used in this project. However, representing numbers with base ten blocks will recreate the "hands-on nature" of ancient Chinese computation.

Task 8 In this task, you will find the greatest common divisor of 12 and 30 using base ten blocks and the method for simplifying fractions from the *Nine Chapters*.

(a) Use base ten blocks to represent the numbers 12 and 30 in two distinct sides of your workspace.

(b) Subtract according to the rule above. A subtraction step leaves the smaller number unchanged, while the larger number is replaced by the remainder from the subtraction.

(c) Continue subtracting until the two numbers remaining are equal. What is this equal number?

(d) Is the equal number the greatest common divisor of 12 and 30? Explain how you know.

Task 9 Did you notice that the statement of the rule instructed the person doing the computation to copy the numerator and denominator "on one side of the counting board"? This meant that the fraction itself was left intact throughout the process of finding the equal number on the other side of the counting board. Why do you think the instructions specified that the numerator and denominator should be copied on one side and the mutual subtraction process performed on the other side?

Our goal in the remainder of this section is to understand how and why the ancient Chinese algorithm worked. Retaining a record of the subtraction steps will help us analyze the algorithm, and a two-column 'paper workspace' is suggested for doing this task. For example, to find the greatest common divisor of 12 and 30 using pencil and paper, begin by creating a two-column chart with 12 at the top of one column, and 30 at the top of the second column.

12	30

(1)

A step in the algorithm begins with the two numbers on the last line written. Compare, and then bring the smaller number straight down to the next line. Under the larger number, write the difference between the smaller number and the larger number, as the instructions said to 'subtract the smaller from the larger'. Continue this pattern of subtracting until the two numbers on the same line are equal. The procedure is illustrated for 12 and 30 below.

12	30	
12	30-12=18	(2)
12	18-12=6	
12-6=6	6	

To reduce the fraction, divide the numerator and denominator by the equal number, giving $\frac{12\div 6}{30\div 6} = \frac{2}{5}$ in this case.

Did you notice that the numbers were not halved before using the subtraction algorithm?

Task 10 Reduce the fraction $\frac{12}{30}$ by first dividing numerator and denominator by 2, then performing the mutual subtraction algorithm on the smaller numbers. Record the subtraction procedure in a two-column table to compare it with the two-column table for 12 and 30 printed above. Use the resulting equal number to simplify the fraction. Is the equal number 6? Explain why or why not.

The equal number obtained by the mutual subtraction algorithm on positive integers a and b is what we today call 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.

Task 11 Use the mutual subtraction algorithm to find $\gcd(49, 91)$. To organize your work, construct a two-column table like the one above.

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

Task 12 Problem 7 in the *Suan Shu Shu* used the fraction $\frac{162}{2016}$ to illustrate the rules for simplifying fractions.Find $\gcd(162, 2016)$ using the mutual subtraction algorithm. What arithmetic operation can we use to complete the repeated subtraction steps more efficiently?

Task 13 Use the mutual subtraction algorithm to find $\gcd(4108, 468)$, using the more efficient arithmetic operation found in the previous task.[7]

Task 14 Are you surprised that only subtraction is needed to find the greatest common divisor of two numbers, even though the concept references division? Why or why not?

[7] This problem is represented by counting rod numerals in a diagram that is reproduced in the Appendix to this project. It is found in another Chinese text *Shushu Jinzhang* (*Mathematics of Nine Sections*) which was written by Qin Jiushao in about 1247 CE, and is analyzed in [Shen, 1988].

2.3 Chinese Justification

In this section we will look at how the ancient Chinese understood the algorithm, and use concrete examples with physical manipulatives to formulate our own explanation of why the algorithm works. Using today's expression 'gcd' for what the Chinese called 'the equal number,'[8] here is a translation of Liu Hui's justification of the mutual subtraction algorithm:

> Subtract the smaller number from the greater repeatedly, because the remainders are nothing but the overlaps of the gcd, therefore divide by the gcd.[9]

Liu claimed that every remainder in the mutual subtraction algorithm is divisible by the equal number. Use the next three tasks to discover why the equal number is a common factor of every remainder.

Task 15 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?

The egg carton exercise suggests that every time the smaller number is subtracted from the larger number, the subtraction involves removing multiples of the greatest common divisor. Another example with physical manipulatives will help us generalize this idea. In this case we will look at the mutual subtraction algorithm 'forward and backward' to notice how the original numbers are built from their greatest common divisor.

Task 16 (a) Use the mutual subtraction algorithm to find gcd$(54, 78)$ and record each subtraction step to finish the two-'column table below.

$$\begin{array}{c|c} 54 & 78 \\ \hline 54 & 78 - 54 = 24 \\ 54 - 24 = 30 & 24 \\ \dots & \dots \end{array} \tag{3}$$

(b) Place a group of 54 blocks and a group of 78 block on your workspace. Group the numbers as multiples of the equal number found in Part (a). Perform the mutual subtraction algorithm with the blocks. When removing blocks, just set them to the side, do not remove then completely from the workspace. What is gcd$(54, 78)$?

[8] The Chinese word for the 'equal number' was '*deng shu*'. As noted in [Dauben, 2008], 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.

[9] The English translation of this excerpt is taken from [Shen et al., 1999, p. 64].

(c) Reverse the subtraction steps in Part (b). Start with the equal number on both sides and replace the blocks you removed, step-by-step. Use the table you created in Part (a) to help you reverse the process. As you are adding, notice whether the groups of the same color blocks are kept together.

(d) Do you agree with Liu Hui when he said that all of the remainders of the subtraction algorithm are simply 'overlaps of the gcd'? Explain.

Reversing the subtraction algorithm helps to emphasize that the equal number is a common factor of the two original numbers. However, it is not as obvious why it must be the *greatest* common factor. Would the same procedure work with a common factor that is not the largest one? Use the next task to explore this question.

Task 17 In this exercise we will explore the algorithm for finding $\gcd(36, 60)$ by considering each number as a multiple of a common factor of 36 and 60. Use blocks or counters to create each number, stacking blocks are suggested.

(a) Place 60 blocks, grouped in groups of 2 on one side of the workspace, and 36 blocks, also grouped in groups of 2 on the other side of the workspace. Physically perform the mutual subtraction algorithm on 60 and 36 by subtracting the smaller number from the larger number until both sides have the same number of blocks. Start by removing 36 blocks from the side that had 60 blocks on it. What is the equal number? How many groups of 2 are in the equal number?

(b) Repeat the mutual subtraction algorithm as in Part (a), except this time group 36 and 60 in groups of 3. How many groups of 3 are in the equal number?

(c) Repeat the subtraction process with 36 and 60 grouped into groups of 4. How many groups of 4 are in the equal number?

(d) Repeat the process with groups of 6 and then groups of 12. What happens?

(e) Is the equal number the greatest common factor? Explain.

The last task also shows us something important about the relationship between any common factor divisor of the original numbers and the greatest common divisor.

Task 18 (a) If a number is a common factor of 36 and 60, explain why it is also a factor of $\gcd(36, 60)$?

(b) Rework Task 17 with the numbers 24 and 40 grouping according to their common factors 2, 4 and 8. Are all common factors also factors of $\gcd(24, 40)$? Explain.

Task 18 indicates that any common factor of two numbers is also a factor of their greatest common divisor. This is a very useful result, but only if it holds for any two numbers, not just a few well-chosen examples. Generalize the ideas in Task 17 to argue that this result holds for an arbitrary choice of two positive integers.

Task 19 Given whole numbers a and b, suppose f is a common divisor of both a and b. Then f also a factor of $\gcd(a, b)$. Use the results of Tasks 17 and 18 to explain why the remainders in the subtraction process are all multiples of f.

Task 20 If a student asked you why the mutual subtraction algorithm worked, what would you tell them?

3 A Classic Greek Mathematical Text: The *Elements*

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 this procedure was found in ancient Greek mathematics as well. In particular, an algorithm for finding the greatest common divisor of two numbers appeared in Euclid's *Elements* [Euclid, 2002]. 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 Katz [1993]. Most ancient mathematical texts presented techniques for solving computational problems in arithmetic or geometry. Yet Euclid's text contained no numbers, no specific numerical computation. Instead, the *Elements* consisted of definitions, axioms, theorems and proofs. Euclid set the standard for future mathematicians to justify new mathematical truths by proving them with deductive logic. Euclid's *Elements* consisted of thirteen books on geometry and number theory. Books I–VI developed the essential theorems of plane geometry. Book I gave a systematic presentation of familiar properties of triangles and parallelograms, culminating in a proof of the Pythagorean Theorem and its converse[10]. Books VII–IX contained the basic ideas of number theory. Number theory is the study of the properties and relationships between numbers, especially the positive integers. Book VII, Propositions 1 and 2, presented Euclid's algorithm for finding the greatest common divisor of two numbers. Book V and Book X of the *Elements* concerned "magnitudes" (arbitrary lengths), represented today as positive real numbers. Books XI–XIII addressed geometry in three dimensions, with a development of the Platonic solids in Book XIII.

4 The Euclidean Algorithm from Ancient Greece

4.1 Context: Number Theory

The foundations of number theory begin with the language of multiplication and division including multiples, divisors, primes and composite numbers.

Book VII of Euclid's *Elements* begins with 22 definitions of number theory terms. Since Euclid's *Elements* is famous as a geometry text, you may be wondering why it would include a discussion of number theory. The simple answer is that numbers are also geometric. For example, if you choose a unit length, a rod of length 3 units is 3 times longer than one unit. Or consider arranging a certain number of items in a geometric pattern, like arranging 9 tiles into the shape of a square with 3 tiles

[10] The converse of the Pythagorean theorem states: If the sum of the squares of the two shortest sides of a triangle is equal to the square of the longest side, then the triangle is a right triangle.

on each side. Euclid represented a number as a line segment which was made up of copies of the unit length. The language of multiplication and division was then placed in the context of measuring these line segments. Of the 22 definitions given at the beginning of Book VII, only the terms needed to explain the Euclidean algorithm are given in this project.

Task 21 Read the definitions below and write down at least three questions and three comments you have about them as you read.

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.

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

(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.

Euclid's definitions were for familiar concepts, yet his wording may seem very strange or awkward. Reading mathematics is sometimes difficult. Even experienced mathematicians may struggle to comprehend new terminology. It is tempting to read quickly through something you may not understand and decide that you will never understand it. Yet, often a slow careful reading with hints will help you master difficult mathematics. In this spirit, we will examine Euclid's definitions in more detail in the remainder of this section.

4.1.1 The Unit

Euclid begins by defining a unit.

Task 22 What is a unit, according to Euclid?

Euclid represented numbers as line segments of particular length, so 1 was a line segment of a particular unit length. It did not matter what unit length was chosen, only that it was specified. All numbers were defined in relation to this unit.

Task 23 Using blocks, rods or lines on paper, choose a length to be defined as a unit. Illustrate the numbers 3 and 7 in relation to your unit. Compare with your classmates: did they choose the same unit? Explain the importance of defining a standard unit for measuring.

One obvious "fix" to the uncertainty of the exact definition of the unit as a specific length is to define it as a single object. Does this always make the definition clear?

Task 24

(a) If you are counting eggs, do you use one single egg or one carton of eggs as your unit? Explain your choice.

(b) If you are counting socks in your drawer, what do you define to be 'one'?

(c) Think of another example of objects for which there is more than one natural definition of one unit?

(d) Explain why a clear definition of 'one' is important.

4.1.2 Numbers, Measuring and Multiples

The idea of a 'number' seems so obvious.

Task 25 Define the word number in your own words. Give several examples of numbers according to your definition.

Once Euclid defined the unit, he continued by defining what he meant by a number. He followed that definition by defining multiples of a number.

Book VII Definitions

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

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

Task 26 Which of the following are numbers according to Euclid's definition? Which are numbers according to your definition?

(a) 17	(b) 47402485	(c)4.9	(d) $\frac{3}{4}$
(e) -5	(f) 0	(g) $\sqrt{2}$	

Task 27 Explain what Euclid meant by a number. Do you think Euclid included 1 as a number? Why or why not?

The fraction $\frac{3}{4}$ is not a "multitude of units" and thus would not be a number according to Euclid's definition. Neither would 4.9 or $\sqrt{2}$ be considered numbers since they are not copies of a unit. Negative numbers were not used in ancient Greece. Zero was not considered a number in the same way that we understand it, although the concept of zero was certainly understood. Therefore, Euclid restricted his "numbers" to counting numbers.

Once numbers were defined, Euclid turned to how numbers were related to each other. A smaller number 'measuring' a larger number implies that some copies of the smaller length, laid end-to-end, is exactly equal to the longer length. For example, 3 measures 6 since two three unit lengths form a line of length exactly 6 units long.

Task 28 Does 4 measure 10? Does 5 measure 10? Justify your answer by representing 4, 5 and 10 as lengths using physical manipulatives.

Task 29 Translate "3 measures 6" into modern terminology in at least two different ways.

Task 30 Explain the phrase "b is a multiple of a" in your own words.

4.1.3 Prime and Composite Numbers

Definitions (11)–(13) concern prime and composite numbers.

Book VII Definitions

(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.

A prime number is defined in many modern textbooks as a positive integer greater than 1 which has only two positive integer factors, 1 and itself.

Task 31 (a) Is Euclid's definition of a prime number the same as the modern definition? Justify your answer.

(b) Explain the definition of a composite number in your own words.

Task 32 Determine whether each number below is prime or composite. If it is composite, list all of its factors.

(a) 37 (b) 57 (c)460 (d) 91

Task 33 **(a)** Are 21 and 35 "prime to one another"?

(b) Are 15 and 22 "prime to one another"?

(c) Explain what the phrase "prime to one another" means in your own words.

Two numbers a and b which are "prime to one another" by Euclid's definition are called *relatively prime* in modern mathematics.

4.2 Computation: Euclid's Proposition 1

Book VII of the *Elements* started with two propositions that together described Euclid's method for finding the greatest common divisor of two numbers. Proposition 1 addressed the case that the greatest common divisor was 1. Then Proposition 2 considers the more general case. In this section, Euclid's subtraction algorithm will be introduced by examining Proposition 1.

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 34 When does the subtraction process stop, according to Euclid? Compare Euclid's instructions with the ancient Chinese rule from *The Nine Chapters*.

Euclid's algorithm is best understood in the context in which it was written, using line segments of specified lengths. A simple way to model such line segments is to use stacking blocks, with one block representing the unit, and line segments representative of different numbers formed by joining the blocks end-to-end. Construct the lines horizontally on your workspace. A subtraction step is performed by comparing the two lines, and removing the number of blocks in the smaller length from the longer length, leaving the remainder on the workspace along with the smaller number.

Task 35

(a) Represent the numbers 21 and 25 as line segments with respective lengths in units using stacking blocks. Subtract the smaller length from the longer length. Continue in this way until one remainder exactly measures the one before it. What happens?

(b) According to Euclid's Proposition 1, are these numbers relatively prime?

(c) Do you agree with what Euclid's Proposition says about whether these numbers are relatively prime? Explain why or why not.

Task 36 Try Euclid's procedure on line segments of length 35 and 24 using stacking blocks. Are these numbers relatively prime? Explain how you know.

Task 37 Apply the procedure with stacking blocks to line segments of lengths 21 and 30 until you reach a remainder that measures the one before it.

(a) What is the value of that final remainder? That is, what is the value of the remainder that measures the one before it?

(b) According to Euclid's Proposition I, are 21 and 30 relatively prime?

(c) Is the remainder that measures the one before it equal to the greatest common divisor of 21 and 30? Explain how you know.

The two-column pencil-and-paper method used for performing mutual subtraction from ancient China is also useful in the case of Euclid's algorithm. The direct comparison will clarify the differences between the Chinese and Greek algorithms.

Task 38 Perform Euclid's subtraction algorithm on the following sets of numbers, recording the subtraction in a two-column pencil-and-paper format as explained for Chinese mutual subtraction.

(a) 21 and 25 (b) 35 and 48
(c) 21 and 30 (d) 49 and 91

Task 39 What are the differences between Euclid's algorithm and the mutual subtraction algorithm of the ancient Chinese? What are the similarities?

We've seen that Euclid's Proposition 1 was only concerned with determining whether or not two numbers were relatively prime. However, he also prescribed subtracting the smaller number from the larger number 'until the remainder measures the one before it' as part of his procedure for finding the greatest common divisor in the case of non-relatively prime numbers. These instructions were embedded in his proof that the algorithm itself works, which appeared in Proposition 2 of Book VII. Accordingly, that proof is the topic of the next section, in which we examine the justification for why Euclid's algorithm works.

4.3 Greek Justification

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 were not prime to one another. Refer to Figure 3 for the diagram that accompanied Proposition 2.

Task 40 Euclid's Proposition 2 (below) may appear long and complicated when you read it for the first time. The description of the algorithm and the proof that certified that it worked are intertwined and the statements that one line measures another may be confusing in a quick read. However, there is a beautiful structure to the proof, and this structure helps the reader follow the argument. Read the text of Book VII Proposition 2 and identify the lines of the proof that correspond to each of the following steps in the argument.

Step 1 Euclid stated the purpose of the proposition.

Step 2 Euclid represented the numbers as line segments of specific lengths which are multiples of a unit length. What were the names of the two numbers?

Step 3 Euclid assumed first that the smaller number measured the larger number, and stated their greatest common divisor in this case. Then, he justified his claim.

Step 4 Euclid explained the subtraction algorithm in the case that the smaller number did not measure the larger number. Notice when the subtraction is supposed to stop.

Step 5 Euclid argued that the last remainder in the subtraction algorithm was a common divisor or factor of the two original numbers.

Step 6 Euclid argued that the last remainder was the **greatest** common divisor.

Step 7 Euclid stated a fact about common divisors that was a consequence of the rest of the proof. Euclid called it a "Porism". In modern terms, this could be called a "Corollary."

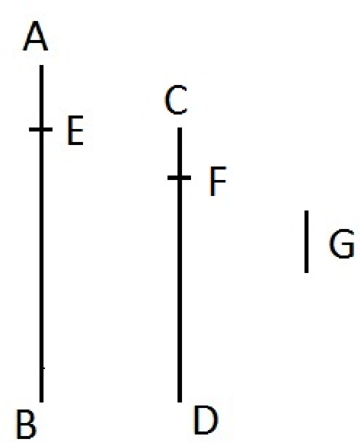

Figure 3: Book VII Proposition 2 Diagram

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 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.

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.

Breaking down the proposition step by step will aid in following the argument. The first three steps are reprinted below.

Book VII Proposition 2, Steps 1–3

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 if 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.

After having stated the goal of the proposition, Euclid represented the two numbers as the lengths of the line segments AB and CD. Step 3 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 steps stopped in Proposition 2 to discover why no subtraction is necessary in this case.

Task 41

(a) Suppose $AB = 42$ and $CD = 6$. Find their greatest common divisor and justify your answer.

(b) 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 was a divisor of the other, Step 4 instructed the reader to subtract, and gave names to the line segments formed in the subtraction process.

Book VII Proposition 2, Step 4

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.

The next task illustrates this algorithm with the numbers 21 and 51, represented physically as line segments constructed from stacking blocks.

Task 42 Let $AB = 51$ and $CD = 21$. Represent each line segment as a length of stacking blocks. Label the ends of each line segment with its appropriate letter using a small sticky note or tape.

(a) Starting from point B, measure as many copies of $CD = 21$ on line $AB = 51$ as possible. Divide the AB line into two pieces, one the multiple of 21 you just measured, and the other the remainder. Label as E the new points of division you just created in the segment AB. (The line segment AB is now two lines segments: BE, which is a multiple of 21, and AE, which is the remainder.)

(b) Measure CD with AE, starting at point D. Separate the segment CD into two pieces and label the new point of division 'F.' Then DF is a multiple of AE and the remainder is CF (which is less than AE). Keep the line segments AE, BE, DF and CF on your workspace to use in the next task.

(c) Does CF exactly measure AE? If so, then Euclid went on (in the last two steps of his proof) to claim that CF was the greatest common divisor of AB and CD. Is this true for this example? That is, is the value you found CF the greatest common divisor of 81 and 33? Explain how you know.

The remainder of Proposition 2 was the proof that CF is the greatest common divisor of AB and CD. Euclid accomplished this in two steps. First, Step 5 of Euclid's proof demonstrated that CF was a common measure of both AB and CD.

Book VII Proposition 2, Step 5

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.

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.

This argument is again best understood by working a concrete example. The following task is a visual demonstration of the argument using stacking blocks.

Task 43 Let $AB = 51$ and $CD = 21$.

(a) Use the line segments AE, BE, DF and CF from Task 42 to complete this task. (Or, if you no longer have those on your workspace, perform the subtraction algorithm in Task 42 to re-create the line segments AE, BE, DF and CF on your workspace.)

(b) Since CF measures AE, express AE as a multiple of CF as an equation. For example, if AE was 5 copies of CD, this would be written $AE = 5 \times CD$.

(c) How many copies of AE make up the length DF? From part (b), we know that AE is a multiple of CF. Explain why DF is a multiple of CF. Express DF as a multiple of CF as an equation.

(d) Explain why CD is a multiple of CF, using your answers to parts (b) and (c). How many copies of CF make up CD? Write this down as an equation.

(e) Express BE as a multiple of CD. Explain why BE must also be a multiple of CF. How many copies of CF form the length BE?

(f) Since AE and BE are multiples of CF, explain why AB must also be a multiple of CF. How many copies of CF form the length AB?

(g) Explain why CF is a common measure of AB and CD.

Task 44 Repeat Tasks 42 and 43 with the numbers $AB = 56$ and $CD = 21$. Did the process work in the same way? If not, explain how it was different and why you think this happened. If so, do you think that the argument given in the last task would work for another pair of numbers AB and CD? Explain why or why not you think this.

At Step 5, Euclid proved that the final remainder CF in the repeated subtraction procedure was a common divisor of the original two numbers, but this by itself does not prove that it is the *greatest* common divisor. Step 6 of Proposition 2 proved that CF must be the largest of all common divisors. Euclid's proof technique is called "proof by contradiction". He assumed that there was a larger common divisor of AB and CD and carefully explained the consequences of this assumption.

Book VII Proposition 2, Step 6

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.

Proof by contradiction often feels awkward because you assume something that cannot be true. However, as a logical exercise, it may not be as difficult as it sounds. The next task uses the concrete example when $AB = 81$ and $CD = 33$ to step through the argument.

Task 45 Assume as Euclid did that G is greater than CF and is a common measure of AB and CD. Use the lines $AB = 51$ and $CD = 21$ divided as AE, BE, CF and DF as in Tasks 42 and 43, but do not physically make G out of blocks. Imagine G as a number that exactly measures 51 and 21 and is bigger than CF, where we know from Task 42 that CF=3.

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

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

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

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

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

The logical consequences included the strange and ridiculous conclusion that a large number measured a smaller one. In concrete terms with $AB = 51$ and $CD = 21$, this would imply that some number greater than 3 is a factor of 3. This cannot be true. Therefore, the assumption that resulted in this conclusion must not be true to begin with, or G cannot be larger than CF and a common factor of AB and CD.

Task 46 Do you think that proof by contradiction is a believable method of proof? Why or why not?

Notice that the logical contradiction occurred when we assumed that G was larger than CF. If G was smaller than CF, there would have been no logical problem. If we assumed that G was a common divisor of AB and CD, then Step 6 showed that G was also a divisor of CF. The next task explores this possibility.

Task 47 Perform Euclid's algorithm with the numbers $AB = 60$ and $CD = 36$. Keep the line segments AE, BE, CF and DF on your workspace as in Tasks 42 and 43. Let $G = 4$.

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

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

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

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

(e) If G were any other common divisor of $AB = 60$ and $CD = 36$, would it also be divisor of the final remainder? Explain why or why not.

The fact that a common divisor of AB and CD was also a divisor of CF was the last statement of Euclid's proof (Step 7). It was called a "Porism" because it was a direct consequence of the proof.

Book VII Proposition 2 Porism, Step 7

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

Task 48 State Euclid's Porism in your own words.

Euclid's proof of the subtraction algorithm assumed that the subtraction algorithm ended after three measurement steps. The reality is that it may take more subtraction steps to find the greatest common divisor. Try the next task using pencil and paper, but keep the idea of measuring line segments in mind as you work.

Task 49 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 less than EA? Call this number q_2 and call the remainder CF.

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

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

(f) Are all of the remainders from the various steps of the subtraction process multiples of the final remainder?

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

Task 50 If the number of subtraction steps is different from that in Euclid's proof, that doesn't change the fact that the last remainder is the greatest common divisor of the original numbers. Explain why the essential argument still works in this case.

5 Cross-Cultural Comparisons

5.1 A Comparison of Ancient Mathematical Cultures

The Euclidean algorithm appeared in Greece in the *Elements* and independently in China in *The Nine Chapters*. The algorithm remains one of the most efficient methods 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.

There are two major differences between the algorithms of ancient China and ancient Greece. The first is the point at which the subtraction stopped. The ancient Chinese continued to subtract until both remainders were equal, while Euclid stopped the subtraction when the last remainder measured (or divided) the one before it.

Task 51 Explain the advantages and disadvantages of continuing the mutual subtraction algorithm until both remainders are equal.

The second major difference between the Chinese and Greek algorithms was the way they were justified. The mathematics presented in *The Nine Chapters* was very practical and concrete. Problems were solved with specific numbers, not with abstract symbols. 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. For a careful explanation of this thesis, see [Chemla, 2012].

The *Nine Chapters* contained 246 specific problems, yet it also contained general rules, like the 'Method for Simplifying Fractions.' The instructions for finding the equal number (or greatest common divisor) were clearly meant for arbitrary positive integers, not just the specific numbers presented in the text. Problems with specific numbers served as examples and were understood to be generalizable. Liu's comments made it clear that Chinese mathematicians were concerned with the correctness of their algorithms. However, their justifications were much more concrete. As Dauben has 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 that readily allowed for abstract deductive logic. 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, (for example, proof by contradiction) [Dauben, 1998]. In fact, this type of reasoning was not present in any logical or philosophical work at that time. The strategy of proving that the equal number was the largest of the possible common divisors by assuming that it was not and deriving a contradiction simply would not have occurred to Liu Hui.

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.

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 should also be formally proven from the basic properties of the integers. Teachers of elementary mathematics will never have to produce a formal proof of the Euclidean algorithm, yet understanding the method of proof gives the teacher a deeper appreciation of the concepts employed by the algorithm.

Task 52 Which method of justification of the Euclidean algorithm do you find most convincing, the informal explanation of Liu Hui (found in Subsection 2.3 of this project) or the formal proof of Euclid (found in Subsection 4.3 of this project)? Explain.

5.2 Mutual Subtraction versus Factorization Techniques

The 'Method for Simplifying Fractions' appeared in Chapter 1 of *The Nine Chapters* at the beginning of the discussion of arithmetic with fractions. Students in elementary school are taught the same rules for arithmetic with fractions, yet they are usually taught to find the greatest common divisor using different methods. To conclude this project, we compare the mutual subtraction algorithm with other common methods for finding the greatest common divisor.

The most naive method for finding the greatest common divisor of two numbers is to take the words 'greatest', 'common' and 'divisor' in reverse order: list the divisors of each number, identify the numbers common to both lists and then choose the largest common divisor. For example, the divisors of 24 are $\{1, 2, 3, 4, 6, 8, 12, 24\}$ and the divisors of 32 are $\{1, 2, 4, 8, 16, 32\}$. The numbers common to both lists are $\{1, 2, 4, 8\}$ and thus the largest of these is 8. Therefore, $\gcd(24, 32) = 8$.

Task 53

(a) Find the greatest common divisor of 12 and 20 by listing their divisors and identifying the largest common divisor.

(b) Find the greatest common divisor of 60 and 84 using the list method.

(c) What are the advantages and disadvantages of this method?

Listing all the factors of each number is not practical when the numbers are large. A more frequently used technique is to find common factors and reduce each number by the common factors until the two remaining numbers are relatively prime. Then, the greatest common divisor is the product of the common factors removed. For example, $24 = 6 \times 4$ and $32 = 8 \times 4$, so removing a common factor of 4 leaves 6 and 8. Further dividing 6 and 8 by 2 leaves remainders of 3 and 4, which are relatively prime. Therefore, the greatest common divisor of 24 and 32 is $4 \times 2 = 8$. This method is similar to the ancient Chinese instructions in the *Suan Shu Shu* to reduce a fraction by dividing numerator and denominator by common factors [Dauben, 2008]

.

A more systematic version of the common factor method is to factor both numbers into their prime factorizations. Recall that every positive integer is either prime or may be expressed uniquely, up to the order of the factors, as a product of prime numbers. If we factor each number into a product of primes, then the greatest common divisor is the product of the primes common to both lists. For example,

$$84 = 2 \times 2 \times 3 \times 7 \text{ and } 90 = 2 \times 3 \times 3 \times 5$$

and thus, $\gcd(84, 90) = 2 \times 3$.

Task 54 Find the greatest common divisor of 60 and 84 using their prime factorizations.

The factorization of a whole number is most compactly written in power notation, listing the prime factors, in order from smallest to largest, raised to the appropriate powers. For example, $24 = 2^3 \times 3$. Then the greatest common divisor of the two numbers is a product of the primes common to both factorizations, raised to the minimum power present in both lists. For example, $84 = 2^2 \times 3 \times 7$ and $90 = 2 \times 3^2 \times 5$. Their greatest common divisor is 2×3.

Task 55 (a) Find the greatest common divisor of 120 and 171 using prime factorizations.

(b) What are the advantages and disadvantages of using prime factorizations to find the greatest common divisor? (Refer to your work in Task 49 using the Euclidean algorithm.)

Modern algorithms taught in school use factoring, while the ancient algorithm utilized subtraction. Subtraction is easier than factoring, especially for larger numbers. Why do we teach factoring to find the greatest common divisor?

Task 56 What mathematical concepts do students learn from finding the prime factorizations of two numbers that they will not encounter using the mutual subtraction algorithm to find the greatest common divisor?

Task 57 What mathematical concepts are illustrated in the mutual subtraction algorithm that are not as easily seen when finding the greatest common divisor by prime factorization?

It is also important for the algorithm used to find the greatest common divisor to be performed efficiently and accurately.

Task 58 Find the greatest common divisor of 156 and 114. Which algorithm did you use? Why?

Task 59 Do you prefer factoring methods or a mutual subtraction algorithm for finding the greatest common divisor? Explain your choice.

As Liu Hui explained, the mutual subtraction algorithm of ancient China (and the Euclidean version of it) worked because the remainders in every step of the process are all multiples of the greatest common divisor. The method needs only subtraction, and thus is simple to implement. Factoring methods are more complicated, since finding the factors of a number involve division, but the resulting factored form of each number may be important to the solution of the problem at hand. Each method has a place in the toolbox of the modern mathematician. Therefore, teachers of elementary mathematics may want introduce both algorithms in their classrooms.

Task 60 What would be the advantages and disadvantages of teaching mutual subtraction to elementary or middle school students?

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, 1994.

Karine Chemla, editor. *The History of Mathematical Proof in Ancient Traditions*. 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. *Archive for History of Exact Sciences*, 62:91–178, 2008.

Joseph W. Dauben, Shuchun Guo, and Yibao Xu. *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*. Number 6 in Library of Chinese Classics. Shenyang: Liaoning Education Press, 2013.

Euclid. *The Elements: All Thirteen Books Complete in One Volume*. Green Lion Press, Santa Fe, NM, 2002. The Thomas L. Heath translation, edited by Dana Densmore.

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.

Victor J. Katz. *History of Mathematics: An Introduction*. Harper Collins College Publishers, New York, 1993.

Jean-Caude Martzloff. *A History of Chinese Mathematics*. Springer-Verlag, Berlin Heidelberg, 1997.

Kangshen Shen. Mutual-Subtraction Algorithm and its Applications in Ancient China. *Historia Matthematica*, 15:135–147, 1988.

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.

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.

Appendix

The following figure comes from [Shen, 1988] and shows the diagram from Problem 3, Section 2, in *Shushu Jiuzhang* (*Mathematics of Nine Sections, 1247*), written by Qin Jiushao, which asks for $\gcd(4108, 468)$. Ancient Chinese was read from top to bottom and right to left, so the reader would begin with the rightmost strip.

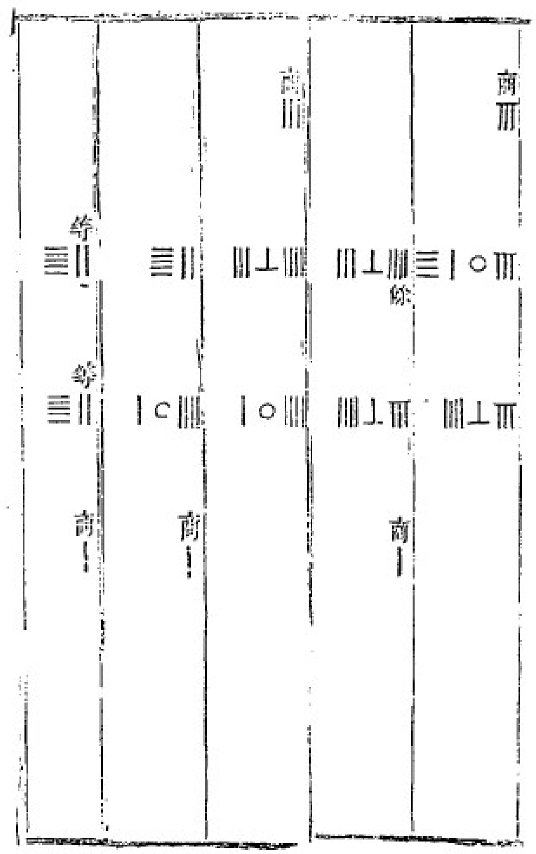

FIG. 1. Episode from section 2, *SSJZ*. The processes of finding (4108, 468) = 52 by the mutual-subtraction algorithm. It reads

		quotient		quotient
Dengshu		3		8
52	52	364	364	4108
Dengshu				
52	104	104	468	468
	quotient		quotient	
	1		1	

Figure 4: Finding $\gcd 4108, 468$ *The Mathematics of the Nine Sections, 1247 CE*

Notes to Instructors

5.3 Intended Audience and Student Prerequisites

This PSP is intended for pre-service teachers, particularly elementary and middle school teachers. It was designed to be used in a mathematical content course on numbers and operations (or algebra). The text only assumes that the reader is familiar with basic arithmetic. The material is also suitable for a general education course for non-majors, with only minor modifications to the wording of several tasks. The algorithms are presented in a more sophisticated way in the PSP *Greatest Common Divisor: Algorithm and Proof*, intended for an upper division mathematics course in number theory, discrete mathematics or other similar topics.

PSP Content and Goals

This PSP introduces algorithms for finding the greatest common divisor developed in ancient China and ancient Greece. The Chinese algorithm appears in *The Nine Chapters on the Mathematical Art*, compiled by the first century CE, and the Greek algorithm comes from the *Elements* of Euclid, written circa 300 BCE. The two communities independently introduced similar algorithms, commonly known as "the Euclidean algorithm" in Western mathematics. This algorithm uses repeated subtraction to find the greatest common divisor of two positive integers. The main goal of this PSP is to present the Euclidean algorithm as a simple and efficient alternative to factoring methods for finding the greatest common divisor.

Mathematical ideas do not emerge without context, and the algorithm for finding the greatest common divisor is no different. Therefore, the Chinese and Greek algorithms are presented in the context in which they appear. Both Chinese and Greek texts also included justifications of their algorithms, and these arguments are also included because teaching an algorithm without attempting to explain why it works is only part of the story.

Content Outline by PSP Section

Section 1 A Classic Chinese Mathematical Text: *The Nine Chapters on the Mathematical Art*

- History and content of the text
- Counting rod numerals in ancient China

Section 2 The Mutual Subtraction Algorithm from China

- In context of simplifying fractions
- Computation with the algorithm using physical manipulatives and written numerals
- Justifying the algorithm, using physical manipulatives to understand Liu Hui's explanation of the mutual subtraction algorithm

Section 3 Euclid's *Elements* as a classic Greek mathematics text

Section 4 The Euclidean Algorithm

- Establishing basic number theory as the underlying context, presenting Euclid's definitions of basic terms

- Book VII Proposition 1 illustrates the mechanics of the algorithm and is implemented using physical manipulatives and written numerals
- Book VII Proposition 2 illustrates the algorithm in its more general setting and proposes a proof, illustrated in student tasks with stacking blocks

Section 4 Cross Cultural Comparisons

- A Comparison of Ancient Mathematical Cultures — The contrast between the concrete and practical Chinese presentation and justification of the algorithm and the very abstract presentation and formal proof by Euclid
- Mutual Subtraction versus Factorization Techniques — A discussion of common methods for finding the greatest common divisor taught in primary school and the advantages and disadvantages of these methods

PSP Goals

1. Students will calculate the greatest common divisor of two positive integers using the Euclidean algorithm, both in the Chinese and Greek versions.
2. Students will understand the connections between the greatest common divisor and simplifying fractions.
3. Students will be able to explain why the mutual subtraction algorithm produces the greatest common divisor.
4. Students will be able to define the basic number theory concepts of unit and number, factors and multiples, primes and composites.
5. Students will compare and contrast the Euclidean algorithm and the prime factorization method of finding the greatest common divisor, and compare the pedagogical advantages and disadvantages of each method.

Suggestions for Classroom Implementation

The PSP is designed to be implemented with a combination of individual reading, group work in class and whole class discussion. The material may be adapted to any teaching style.

Concrete Numbers with Blocks

The author strongly encourages instructors to use manipulatives to work the tasks in which they are suggested. The author's students found the concrete illustrations set on the workspace in front of them tremendously helpful in understanding the procedures. (The PSP material has been used with both math majors and pre-service elementary teachers; both groups found the blocks helpful.) Unifix Cubes or other stacking or linking blocks are preferred since they may be connected into horizontal lines of the required length for understanding Euclid's proof. As a practical matter, it is best if the stacking blocks are all of the same brand and fit together tightly when forming line segments to investigate Euclid's proof, otherwise measuring line segments will be prone to errors.

Base ten blocks are also suggested for learning the ancient Chinese algorithm with a concrete representation of the numbers. The Chinese would have performed the computation using counting rods. The author chose not to include counting rods in the tasks as subtraction would be much more difficult in this unfamiliar setting. However, displaying the numbers using base ten blocks and subtracting the blocks is pedagogically equivalent to manipulating counting rods in ancient China.

Full Implementation in a Pre-Service Teacher Class

The full PSP is estimated to take 6 hours of class instruction in a course for pre-service elementary teachers using group work, class discussion, individual preparation and homework. The following is a sample lesson plan based on a 50-minute class period.

- Day 1 Sections 2.1 and 2.2 The Algorithm from China
  - Assign Section 1 and the beginning of Section 2.1 up until Task 3 as background reading, and assign Tasks 1, 2 and 3 as preparation for class
  - Class discussion of the history of the Chinese text and the importance of simplifying fractions
  - Group work from Tasks 4–12, especially Tasks 4, 5, 8, 10, 11, 12
  - Assign Tasks 5, 6, 7, 9, 13, 14 as homework
- Day 2 Section 2.3 Justifying the Chinese Algorithm
  - Assign as preparatory reading everything from the beginning of Section 2.3 through Task 15, and assign Task 15
  - Group work on Tasks 16–18 in class
  - Assign Tasks 19 and 20 as homework
  - Whole class discussion on the Chinese method and background on Euclid's *Elements*
- Day 3 Number Theory from Euclid
  - Assign Section 3 and the beginning of Section 4.1 through Task 21 as preparatory reading, and assign Task 21
  - Group work through the definitions, Tasks 22–33, with whole class discussion of "measuring", factors, primes, composites support understanding of Euclid's definitions
  - Assign as homework full write-ups of selected Tasks in Section 3.1, especially Tasks 24(d), 25, 27, 30, 31, 33(c)
  - Explain the goal of Task 34 to prepare students to complete the task before the next class meeting
- Day 4 The Euclidean Algorithm
  - Assign Task 34 as class preparation
  - Whole class discussion of prepatory work
  - Group work step–by–step through Tasks 35–37 with manipulatives
  - Task 38 in groups
  - Whole class discussion of Task 40 to prepare students to complete this task before the next class meeting

- Day 5 Proposition 2 and Proof
  - Assign Task 40 as preparation, and begin class by sharing results
  - Group work on Tasks 41–44, followed by a whole class discussion of results
  - Instructor led discussion of Task 45
  - Group work on Tasks 47 and 49
  - Assign Tasks 44, 46, 48 and 50 as homework
- Day 6 Comparison
  - Assign Section 5.1 as preparatory reading, and assign Tasks 51 and 52
  - Whole class discussion on the comparison of the ancient Chinese and ancient Greek algorithms and proofs
  - Group work on Tasks 53–55
  - Whole class discussion on the concepts involved in each method of finding the greatest common divisor.
  - Assign reflection homework from Tasks 56–60

Partial Implementation Suggestions

The PSP, or portions thereof, would also be suitable for general education classes, a history of mathematics class or in an algebra class for secondary pre-service teachers.

In the case of an algebra class for secondary teachers, it would be appropriate to cover the entire lesson, but prepare students to do more preparatory and follow-up work outside of class. In-class group work on the concrete examples with stacking blocks is still encouraged.

Sections 1 and 2 would make an excellent lesson for a general education course or a history of math course, using 1.5–2 hours of class time to work Tasks 1–20.

Sections 3 and 4 alone, on the Euclidean algorithm, would be an excellent 3 hour lesson in a history of mathematics class or an introductory number theory course. Instructors teaching a more advanced number theory course should consider using the PSP, *Greatest Common Divisor: Algorithm and Proof*, which presents the same material in this PSP, but at a more advanced level.

PSP Design and Task Commentary

China

Task 7 The purpose of this task is begin a conversation on the advantage of simply subtracting versus spending time finding common factors. Clearly, a common factor of 2 is obvious, but finding more common factors may not be an efficient use of time. Note that dividing the numbers by common factors does not change the number of subtraction steps needed to perform the mutual subtraction algorithm, it only makes the numbers smaller.

Task 9 The Chinese subtracted by removing counting rods from the number on the counting board, which erased the original numbers. If the mutual subtraction algorithm was performed on the side of the counting board, the original numbers would remain on the board.

Tasks 12 and 13 These tasks ask the students to find the greatest common divisor for numbers that the Chinese used as examples. A Chinese diagram illustrating the procedure with the numbers in Task 13 is included in the Appendix. Instructors may want to explore this diagram as an example of Chinese rod numerals, subtraction by division with quotient and remainder and the differences between reading ancient Chinese and modern English. However, the author found that explaining this diagram distracted from the focus of the lesson with pre-service elementary teachers.

Task 15 The concrete egg carton grouping in Task 14 was very helpful to the author's students.

Task 17 When working with stacking blocks, especially when reexamining the algorithm after performing it once, the author's students found it helpful to form stacks of blocks grouped according to the gcd so that each group was the same color. For example, if the gcd is 4, the stacks would be 4 of one color, and different stacks would be of different colors.

Euclid

Task 27 Note that a number being a 'multitude of units' implies that one is not treated as a number in the same way as the other positive integers. Hence the need to have two separate propositions for finding the greatest common divisor, one when the gcd is equal to 1, and the second for the case that the gcd is greater than 1.

Tasks 34–39 Euclid's Book VII Proposition 1 is presented, then the tasks ask students to compare the instructions with those of the Chinese. The proof of Proposition 1 is not presented because it is similar to the proof of Proposition 2.

Task 40 This task asks students to identify the logical steps in Book VII Proposition 2 and its proof. The purpose is to help students read the source and focus on the overall structure instead of getting stuck in which line measures another.

Tasks 41–50 The proof of Proposition 2 is broken down into 7 steps to make it less intimidating, and focus on the purpose of each step instead of the details. The proof of Proposition 2 is a bit intimidating, but the concrete process with line segments constructed from blocks is very straightforward.

Tasks 49 and 50 These tasks asks students to perform the Euclidean algorithm with two numbers that require more subtraction (division) steps than given in the proof. These tasks are included because the number of subtraction steps varies with each problem, even though Euclid only addressed a single case. The method generalizes, and this task and the next ask the students to generalize.

Cross Cultural Comparison

Task 52 This task asks students whether they would choose to explain the mutual subtraction algorithm's correctness in concrete terms as the Chinese did, or in a more detailed logical proof as Euclid did. A preference for the Liu Hui's "overlaps of the gcd" explanation is expected, but could lead to a discussion of why the formal logical proof is important.

Tasks 53–60 The Mutual Subtraction versus Prime Factorization Techniques section was written specifically for pre-service teachers. It asks students to think about why they were taught to find the greatest common divisor by prime factorization, and whether the mutual subtraction algorithm should also be taught as an alternative.

Recommendations for Further Reading

The book *The Nine Chapters on the Mathematical Art: Companion and Commentary* [Shen et al., 1999] contains a wealth of information about the history of Chinese mathematics, with comparisons to the mathematical development in other cultures. The introductory material is suitable for both instructors and students.

A very interesting discussion of the difficulty of translating *The Nine Chapters on the Mathematical Art* is given in Volkov [2010]. The author gives an example of the translation of Liu Hui's explanation on why fractions need to be simplified. The discussion is a wonderful illustration of the challenges of explaining fractions, both in ancient times and in the modern classroom.

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 student project has been partially supported by the TRansforming Instruction in Undergraduate Mathematics via Primary Historical Sources (TRIUMPHS) Program with funding from the National Science Foundation's Improving Undergraduate STEM Education Program under Grant Nos. 1523494, 1523561, 1523747, 1523753, 1523898, 1524065, and 1524098. Any opinions, findings, and conclusions or recommendations expressed in this project are those of the author and do not necessarily represent the views of the National Science Foundation.

For more information about TRIUMPHS, visit `https://blogs.ursinus.edu/triumphs/`.