PROJECTS FOR STUDENTS OF DISCRETE MATHEMATICS VIA PRIMARY HISTORICAL SOURCES: Euclid on his algorithm

Janet Heine BARNETT* Jerry LODDER* David PENGELLEY*

Mathematics and Physics, Colorado State University - Pueblo, Pueblo, CO 81001, USA
Mathematics, New Mexico State University, Las Cruces, NM 88003, USA
Mathematics, New Mexico State University, Las Cruces, NM 88003, USA

ABSTRACT

We analyze our student project *Euclid's Algorithm for the Greatest Common Divisor*. The project was written for students to decipher Euclid's verbal description of his famous algorithm for calculating the greatest common divisor of two numbers, convert it to a modern mathematical formulation, consider various issues that arise, and prove its correctness. We will discuss how the project design achieves specific pedagogical goals for teaching directly from primary historical sources.

Keywords: Euclidean algorithm, greatest common divisor, primary sources, original sources, pedagogy

1 Introduction

We analyze pedagogically the project *Euclid's Algorithm for the Greatest Common Divisor*, written for student study at beginning undergraduate or pre-college level. In the core of the project students are guided to decipher Euclid's verbal description of his famous algorithm for calculating the greatest common divisor of two numbers, convert it to a modern mathematical formulation, consider various questions and issues that arise, and prove its correctness. Along the way the Euclid source naturally raises questions about the nature of numbers, divisibility, algorithms, efficiency of computation, correctness, and proof. We will discuss how the project design achieves specific pedagogical goals.

This student project is part of a larger endeavor. Over the past nine years, with support from the US National Science Foundation, our interdisciplinary team of seven mathematicians and computer scientists has been developing and testing student projects based directly on primary historical sources for studying discrete mathematics and related subjects. Our 34 projects for students are based on primary sources encompassing discrete mathematics, combinatorics, abstract algebra, logic, and computer science, and have been extensively tested with students at varied institutions. The goal is to study mathematics directly from the minds of the pioneers, such as Euclid, Archimedes, Fermat, Pascal, Bernoulli, Lagrange, Cauchy, Cayley, Boole, Venn, Dedekind, Frege, Russell, Whitehead, and others. All our projects are available, along with guidance for instructors and our philosophy of teaching with them, at [**?**, **?**]. Our overall program for developing, testing, and evaluating the use of these projects is also discussed in [**?**].

Designed to capture the spark of discovery and motivate subsequent lines of inquiry, each project is built around primary source material close to or representing the discovery of a key concept. Through guided reading and directed questions and activities, students explore the mathematics of the original discovery and develop their own understanding of the subject. To place the source in context, a project also provides biographical information about its author, and historical background about the problems with which the author was concerned. Advantages include providing context and direction for the subject matter, honing students' verbal and deductive skills through reading the original work of some of the greatest minds in history, and the rediscovery of conceptual roots. Additionally, students practice the skill of moving from verbal descriptions to precise mathematical formulations, and must often recognize an organizing concept for a detailed procedure.

2 Mathematical aims of the Euclid project

Each of our projects provides a summary of the project along with suggestions about class activities for instructors. For our project *Euclid's Algorithm for the Greatest Common Divisor*, the notes to the instructor are:

> "The project is meant for use in an introductory computer science or discrete mathematics class. The project can be used to introduce students to the notion of "computation method" or "algorithm" and to explore concepts like iteration in a basic setting. It allows them to practice their skills in doing proofs but more importantly to observe the evolution of what is accepted as a valid proof or a well-described algorithm. The students will easily notice that the method presented by Euclid to compute the GCD and the proof of its correctness that he provided would not be formally accepted as correct today. They will also notice, however, that Euclid is somehow able to convey his ideas behind his method and proof in a way that they can be easily translated into a modern algorithm and proof of its correctness. In this way, it will provide them a sense of connection to the past.
>
> A basic knowledge of programming is essential to successfully complete some of the components of the project."

3 Pedagogical design goals

In [**?**] we distilled a set of pedagogical goals informing our selection of primary source material and the design of projects. We list these here in preparation for analyzing the Euclid project.

Fifteen Pedagogical Goals Guiding the Development of Primary Source Based Projects

1. Hone students' verbal and deductive skills through reading.
2. Provide practice moving from verbal descriptions of problems to precise mathematical formulations.
3. Promote recognition of the organizing concept behind a procedure.

4. Promote understanding of the present-day paradigm of the subject through the reading of an historical source which requires no knowledge of that paradigm.
5. Promote reflection on present-day standards and paradigm of subject.
6. Draw attention to subtleties, which modern texts may take for granted, through the reading of an historical source.
7. Promote students' ability to equally participate, regardless of their background or capability.
8. Offer diverse approaches to material which can serve to benefit students with different learning styles through exposure to multiple approaches.
9. Provide a point of departure for students' work, and a direction for their efforts.
10. Encourage more authentic (versus routine) student proof efforts through exposure to original problems in which the concepts arose.
11. Promote a human vision of science and of mathematics.
12. Provide a framework for the subject in which all elements appear in their right place.
13. Promote a dynamical vision of the evolution of mathematics.
14. Promote enriched understanding of subject through greater understanding of its roots, for students and instructors.
15. Engender cognitive dissonance (dépaysement) when comparing a historical source with a modern textbook approach, which to resolve requires an understanding of both the underlying concepts and use of present-day notation.

4 The Euclid project and its pedagogy

We will present the complete student project based on Euclid's text, and intersperse commentary discussing how it addresses our various pedagogical goals. We will find that every one of the goals in our list is addressed.

Euclid's Algorithm for the Greatest Common Divisor

Numbers, Division and Euclid

People have been using numbers, and operations on them like division, for a very long time for practical purposes like dividing up the money left by parents for children, or distributing ears of corn equally to groups of people, and more generally to conduct all sorts of business dealings. It may be a bit of a surprise that things like calculating divisors of numbers also form the core of today's methods ensuring security of computer systems and internet communications. The RSA cryptosystem that is

used extensively for secure communications is based on the assumed difficulty of calculating divisors of large numbers, so calculating divisors is important even today.

A related and even more basic notion is that of multiples of quantities. A natural way to compare quantities is to "measure" how many times we need to aggregate the smaller quantity to obtain the larger quantity. For example, we may be able to compare two unknown lengths by observing that the larger length can be obtained by "aggregating" the smaller length three times. This provides a sense of how the two lengths compare without actually knowing the two lengths.

The larger quantity may not always be obtainable from the smaller quantity by aggregating it an integral number of times. In this scenario, one way to think would be to imagine each of the two quantities to be made up of smaller (identical) parts such that both the quantities can be obtained by aggregating these smaller parts an integral number of times. Obviously, we will need a greater number of these parts for the larger quantity than for the smaller one. For example, when comparing two weights, one might observe that the larger one can be obtained by aggregating some weight 7 times whereas the smaller weight can be obtained by aggregating the same weight 5 times. This provides a basis for comparing the two weights. Of course, in the above scenario, one can also observe that if we chose even smaller parts to "split" the weights (say a quarter of the first one), the first weight would be obtained by aggregating this even smaller weight 28 times and the smaller of the two original weights would be obtained by aggregating this smaller part 20 times, which also provides us a sense of the relative magnitudes of the two weights. However, using smaller numbers like 7 and 5 to describe relative magnitudes seems intuitively and practically more appealing than using larger numbers, like 28 and 20. This leads us to think about what would be the greatest magnitude such that two given magnitudes will both be multiples of that common magnitude.

This question was considered by Greek mathematicians more than 2000 years ago. One of those Greeks was Euclid, who compiled a collection of mathematical works called *Elements* that has a chapter, interestingly called a "Book", about numbers. During the course of this project you will read a translation of part of this chapter to discover Euclid's method (algorithm) to compute the greatest common divisor of two numbers. It is not clear if Euclid was the first person to discover this algorithm, but his is the earliest known written record of it.

Commentary. *This brief introductory mathematical discussion and thought experiment sets the stage both for modern practical applications and historical context. It provides a motivational point of departure for students, and highlights the issue of choice of unit for measurement, something that is often glossed over today, but whose importance is brought out naturally through reading ancient texts.*

Euclid of Alexandria

Euclid lived around 300 B.C.E. Very little is known about his life. It is generally believed that he was educated under students of Plato's Academy in Athens. According to Proclus (410–485 C.E.), Euclid came after the first pupils of Plato and lived during the reign of Ptolemy I (306–283 B.C.E.). It is said that Euclid established a mathematical school in Alexandria. Euclid is best known for his mathematical compilation *Elements* in which among other things he laid down the foundations of geometry and number theory. The geometry that we learn in school today traces its roots to this book, and Euclid is sometimes called the father of geometry.

Euclid did not study mathematics for its potential practical applications or financial gains. He studied mathematics for a sense of order, structure and the ideal form of reason. To him geometrical objects and numbers were abstract entities, and he was interested in studying and discovering their properties. In that sense, he studied mathematics for its own sake. One story that reveals his disdain for learning for the purpose of material gains concerns a pupil who had just finished his first geometry lesson. The pupil asked what he would gain from learning geometry. As the story goes, Euclid asked his subordinate to give the pupil a coin so that he would be gaining from his studies. Another story that reveals something about his character concerns King Ptolemy. Ptolemy asked the mathematician if there was an easier way to learn geometry. Euclid replied, "There is no royal road to geometry", and sent the king to study.

Euclid wrote several books such as *Data, On Divisions of Figures, Phaenomena, Optics*, and the lost books *Conics* and *Porisms*, but *Elements* remains his best known compilation. The first "book" [chapter] in this compilation is perhaps the most well-known. It lays down the foundations of what we today call "Euclidean" geometry (which was the only plane geometry people studied until the Renaissance). This book has definitions of basic geometric objects like points and lines along with basic postulates or axioms. These axioms are then used by Euclid to establish many other truths (*Theorems*) of geometry. Euclid's *Elements* is considered one of the greatest works of mathematics, partly because it is the earliest we have that embodies an axiomatic approach. It was translated into Latin and Arabic and influenced mathematics throughout Europe and the Middle East. It was probably the standard "textbook" for geometry for more than 1500 years in western Europe and continues to influence the way geometry is taught to this day.

Book 7 of *Elements* provides foundations for number theory. Euclid's Algorithm for calculating the greatest common divisor of two numbers was presented in this book. As one will notice later, Euclid uses lines to represent numbers and often relies on visual figures to aid the explanation of his method of computing the greatest common divisor (GCD) of two numbers. As such, he seems to be relating numbers to geometry, which is quite different from the present day treatment of number theory.

Today, erroneously, many different methods are called Euclid's algorithm. By reading the original writings of Euclid you will discover the real Euclidean algorithm and appreciate its subtlety. In any case, "Euclid's Algorithm" is one of the most cited and well-known examples of an (early) algorithm. To quote Knuth **[?]** :

By 1950, the word algorithm was mostly associated with "Euclid's Algorithm".

Commentary. *This biographical and historical background gives students a sense of the human aspect of the creation of mathematics, including the interplay between studying mathematics for its own sake and for applications, as well as a sense for the evolution of mathematics over a very long period. By pointing out the relationship between number and geometry for Euclid, it also fosters a framework in the mind of the student in which the different parts of mathematics are interrelated, unlike the way they are often taught today.*

Prelude

We say that a number[1] x divides another number y if y is a multiple of x. For example, $1, 2$, and 3 all divide 6 but 5 does not divide 6. The only divisors of 17 are 1 and 17. The notation $x|y$ is a shorthand

[1]The word number in this section means a positive integer. That is what it meant to Euclid.

for "x divides y". We denote by $divisors(x)$ the set of all the numbers y such that $y|x$. So, for example, $divisors(6) = \{1, 2, 3, 6\}$ and $divisors(60) = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60\}$.

A number z is called a common divisor of two numbers x and y if $z|x$ and $z|y$. We denote by $cd(x, y)$ the set of all common divisors of x and y. For example, $cd(6, 8) = \{1, 2\}$ and $cd(40, 180) = \{1, 2, 4, 5, 10, 20\}$.

Exercise 4.1. *What is the set of divisors of the number* 315*?*

Exercise 4.2. *Calculate the set* $cd(288, 216)$*.*

While it is relatively easy to calculate the divisors of a number and common divisors of two numbers when the numbers are small, the task becomes harder as the numbers becomes larger.

Exercise 4.3. *Calculate* $divisors(3456)$*.*

Exercise 4.4. *Calculate* $cd(3456, 4563)$*.*

Exercise 4.5. *A rather naive method for computing the divisors of a number x is to test whether each number from 1 to x inclusive is a divisor of x. For integers $n = 1, 2, 3, \ldots, x$, simply test whether n divides x. Using this naive algorithm, write a computer program in the language of your choice that accepts as input a positive integer x and outputs all divisors of x. Run this program for:*

(a) $x = 3456$,

(b) $x = 1009$,

(c) $x = 1080$.

Exercise 4.6. *The naive method for computing the common divisors of two numbers x and y is to test whether each number from 1 to the least of $\{x, y\}$ divides x and y. In modern notation, let m denote the minimum (least of) $\{x, y\}$. For $n = 1, 2, 3, \ldots, m$, first test whether n divides x, and, if so, then test whether n divides y. If n divides both x and y, record n as a common divisor. Using this naive algorithm, write a computer program in the language of your choice that accepts as input two positive integers x, y, and outputs their common divisors. Run this program for:*

(a) $x = 3456$, $y = 4563$,

(b) $x = 625$, $y = 288$,

(c) $x = 216$, $y = 288$,

(d) $x = 147$, $y = 27$.

As you might have noticed the number 1 divides every number. Since there is no number smaller than 1, 1 is the **smallest** common divisor for any two numbers x and y. What about the **greatest** common divisor? The greatest common divisor of two numbers x and y, denoted by $gcd(x, y)$, is the largest number z such that $z|x$ and $z|y$. Finding the greatest common divisor is not nearly as easy as finding the smallest common divisor.

Commentary. *This prelude prepares students for reading the primary source directly, since Euclid does not provide definition, motivation or context for questions about the greatest common divisor of two numbers. This short section explores the issue through a number of concrete examples and exercises, and encourages students to program naive algorithms. We intentionally make the prelude no longer than necessary for students to dive into Euclid, since our goal is to have students engage the primary source as quickly and as deeply as possible.*

*We intersperse exercises throughout the project, encouraging students and instructors who wish to engage the project in small stages, as regular day-by-day classroom work and homework. The logistics of ways to use a project in class are discussed further at [**?**].*

Euclid's Algorithm

Here we present the translations of (relevant) Definitions, Proposition 1 and Proposition 2 from Book VII of Euclid's *Elements* as translated by Sir Thomas L. Heath [**?**]. Euclid's method of computing the GCD is based on these propositions.

BOOK VII of *Elements* by Euclid

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 **a part** of a number, the less of the greater, when it measures the greater.
4. but **parts** when it does not measure it.[2]
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 differs by a unit from an even number.
8. An **even-times even number** is that which is measured by an even number according to an even number.
9. An **even-times odd number** is that which is measured by an even number according to an odd number.
10. An **odd-times odd number** is that which is measured by an odd number according to an odd number.
11. A **prime number** is that which is measured by a unit alone.[3]
12. Numbers **prime to one another** are those which are measured by a unit alone as a common measure.

[2] While this definition is not relevant here, what is meant by this definition is quite subtle and the subject of scholarly mathematical work.

[3] Reading further work of Euclid, e.g. Proposition 2, it is clear that Euclid meant that a prime number is that which is measured only by the unit and the number itself.

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.

Exercise 4.7. *Discuss how Euclid's "unit" relates to the number 1. Does Euclid think that 1 is a number?*

Exercise 4.8. *What is likely meant when Euclid states that a number "measures" another number? Express Euclid's notion of "measures" in modern mathematical notation.*

Exercise 4.9. *Does the number 4 measure number 72? Does 5 measure 72? Briefly justify your answer.*

Exercise 4.10. *Euclid never defines what is a "common measure," but uses that in definition 12 and 14. What is your interpretation of Euclid's "common measure"?*

Exercise 4.11. *Find a number (other than the unit) that is a common measure of the numbers 102 and 187. According to Euclid's definitions, are the numbers 102 and 187 composite to one another? Why or why not?*

Exercise 4.12. *According to Euclid's definitions, are the numbers 21 and 55 composite to one another? Justify your answer.*

Commentary. *Euclid's definitions provide considerable grist for mathematical questions, intentionally left unexplained by us, for students to grapple with in exercises. Such basic questions as whether "one" is a number, and what "measures" means and why Euclid leaves it undefined, reflect the rich intellectual stimulation a primary source can provide, even before anything particularly technical is encountered.*

Already here deductive skills through reading the primary source are naturally emphasized, as well as the challenge of moving between verbal and symbolic formulations, e.g., in divining the meaning of "measures" and comparing it to the concept of a "multiple".

We now present Proposition 1 from Euclid's book VII. The proposition concerns numbers that are prime to one another.

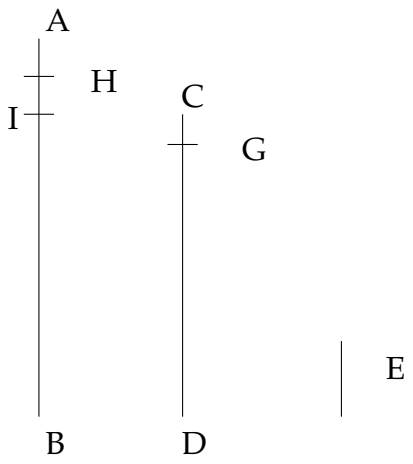
PROPOSITION 1.

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.

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 BI, leave IA less than itself,

let, AI measuring DG, leave GC less than itself,

and let GC, measuring IH, leave a unit HA.

Since, then E measures CD, and CD measure BI, therefore E also measures BI.

But it also measures the whole BA;

therefore it will also measure the remainder AI.

But AI 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 IH;

therefore E also measures IH.

But it also measures the whole IA;

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. [VII. Def 12]

Q. E. D.

Exercise 4.13. *Euclid begins with two unequal numbers AB, CD, and continually subtracts the smaller in turn from the greater. Let's examine how this method proceeds "in turn" when subtraction yields a new number that is smaller than the one subtracted. Begin with $AB = 162$ and $CD = 31$.*

(a) How many times must CD be subtracted from AB until a remainder is left that is less than CD? Let this remainder be denoted as IA.

(b) Write $AB = BI + IA$ numerically using the given value for AB and the computed value for IA.

(c) How many times must IA be subtracted from CD until a remainder is left that is less than IA? Let this remainder be denoted as GC.

(d) Write $CD = DG + GC$ numerically using the given value for CD and the computed value for GC.

(e) How many times must GC be subtracted from IA until a remainder is left that is less than GC? Let this remainder be denoted as HA.

(f) Is HA a unit?

(g) Write $IA = IH + HA$ numerically using the computed values of IA and HA.

Exercise 4.14. *Apply the procedure outlined in Proposition 1 to the numbers $AB = 625$ and $CD = 288$. Begin by answering questions (a)–(f) above except with the new values for AB and CD.*

(g) In this example, how should the algorithm proceed until a remainder is reached that is a unit?

Exercise 4.15. *Euclid claims that if the repeated subtraction algorithm of Proposition 1 eventually produces a unit as a remainder, then the original numbers AB, CD are prime to one another. He does so by using a "proof by contradiction." Suppose the result, namely that AB and CD are prime to one another, is false. In this exercise we examine the consequences of this.*

(a) If AB and CD are not prime to one another, must these numbers have a common measure E that is greater than 1? Justify your answer by using Euclid's definitions.

(b) From $AB = BI + IA$, why must E also measure IA ? Be sure to carefully justify your answer for general numbers AB and CD (not tied to one particular example).

(c) From $CD = DG + GC$, why must E also measure GC? Be sure to carefully justify your answer.

(d) From $IA = IH + HA$, why must E also measure HA? Carefully justify your answer.

(e) If according to Euclid, HA is a unit, what contradiction has been reached in part (d) ?

Commentary. *Euclid's Proposition 1 and the exercises achieve a number of our pedagogical goals. To decipher and understand Euclid students will use considerable verbal and deductive skills through reading, practice moving from a verbal description to a precise mathematical formulation, puzzle out the organizing concept behind a procedure, and gain perspective on present-day paradigms through translating to modern formulas. Moreover, Euclid's approach through imagining geometric measurement is quite different from a modern one,*

providing students with a diversity of viewpoints and enabling students with different backgrounds and learning styles to benefit. The exercises also explore the phenomenon of iterative procedures and when they terminate, raising questions about Euclid's description, which does not directly address this issue.

We now present proposition 2 from Book VII of Euclid's elements. This proposition presents a method to compute the GCD of two numbers which are not prime to each other and provides a proof of the correctness of the method. Euclid's presentation intermixes the proof and the method to some extent. Despite this the elegance of his method and the proof is striking.

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.

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

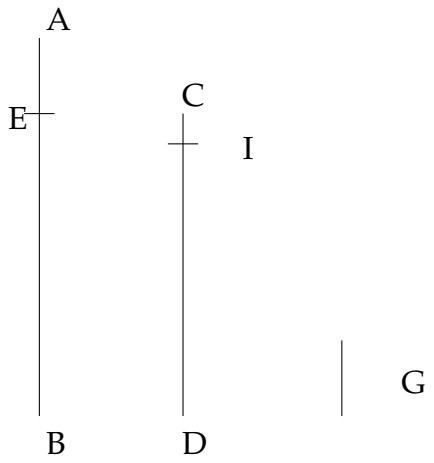
If now CD measures AB - and it also measures itself - CD is a common measure of CD, AB.

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.[4]

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

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



[4]This is the heart of Euclid's description of his algorithm. The statement is somewhat ambiguous and subject to at least two different interpretations.

Now let CD, measuring BE, leave EA less than itself, let EA, measuring DI, leave IC less than itself, and let CI measure AE.

Since then, CI measures AE, and AE measures DI,

therefore CI will also measure DI.

But it also measures itself;

therefore it will also measure the whole CD.

But CD measures BE;

therefore CI also measures BE.

But it also measures EA;

therefore, it will also measure the whole BA.

But it also measures CD;

therefore CI measures AB, CD.

Therefore CI is a common measure of AB, CD.

I say next that it is also the greatest.

For, if CI is not the greatest common measure of AB, CD, some number which is greater than CI 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 DI;

therefore G will also measure DI.

But it will also measure the whole DC;

therefore it will also measure the remainder CI, that is, the greater will measure the less: which is impossible.

Therefore no number which is greater than CI will measure the numbers AB, CD;

therefore CI is the greatest common measure of AB, CD.

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

Exercise 4.16. *In Proposition 2 Euclid describes a procedure to compute the greatest common measure of two numbers AB, CD, not prime to one another. The method again proceeds by repeatedly subtracting the smaller in turn from the greater until some number is left, which in this case divides the number before it. Let's examine this process for $AB = 147$ and $CD = 27$.*

(a) Does CD measure AB? If so, the process stops. If not, how many times must CD be subtracted from AB until a positive remainder is left that is less than CD. Let EA denote this remainder.

(b) Write $AB = BE + EA$ numerically using the given value for AB and the computed value for EA. Also find a positive integer q_1 so that $BE = q_1 \cdot CD$.

(c) Does EA measure CD? If so, the process stops. If not, how many times must EA be subtracted from CD until a positive remainder is left that is less than EA. Let IC denote this remainder.

(d) Write $CD = DI + IC$ numerically using the given value for CD and the computed value for IC. Also, find a positive integer q_2 so that $DI = q_2 \cdot EA$.

(e) Does IC measure EA? If so, the process stops. If not, how many times must IC be subtracted from EA until a positive remainder is left that is less than IC ?

(f) Find a positive integer q_3 so that $EA = q_3 \cdot IC$.

Exercise 4.17. *Apply Euclid's procedure in Proposition 2 to compute the greatest common measure of $AB = 600$ and $CD = 276$ outlined in the steps below.*

(a) To streamline the process, let $a_1 = AB = 600$, $a_2 = CD = 276$, and $a_3 = EA$. Compute a_3 numerically for this example. Write the equation $AB = BE + EA$ entirely in terms of a_1, a_2 and a_3.

(b) Let $a_4 = IC$. Compute a_4 for this example. Write the equation $CD = DI + IC$ entirely in terms of a_2, a_3 and a_4.

(c) Does IC measure EA in this example? If so, the process stops. If not, how many times must IC be subtracted from EA until a positive remainder is left that is less than IC? Denote this remainder by a_5.

(d) Write an equation using a_3, a_4 and a_5 that reflects the number of times IC must be subtracted from EA so that the remainder is a_5.

(e) Does a_5 measure a_4? If so, the process stops. If not, how many times must a_5 be subtracted from a_4 until a positive remainder is left that is less than a_5?

Exercise 4.18. *In modern notation, the Euclidean algorithm to compute the greatest common measure of two positive integers a_1 and a_2 (prime to each other or not) can be written as follows. Find a sequence of positive integer remainders $a_3, a_4, a_5, \ldots, a_{n+1}$ and a sequence of (positive) integer multipliers $q_1, q_2, q_3, \ldots, q_n$ so that*

$$\begin{aligned}
a_1 &= q_1 a_2 + a_3, \quad 0 < a_3 < a_2 \\
a_2 &= q_2 a_3 + a_4, \quad 0 < a_4 < a_3 \\
a_3 &= q_3 a_4 + a_5, \quad 0 < a_5 < a_4 \\
&\vdots \\
a_{i-1} &= q_{i-1} a_i + a_{i+1}, \quad 0 < a_{i+1} < a_i \\
a_i &= q_i a_{i+1} + a_{i+2}, \quad 0 < a_{i+2} < a_{i+1} \\
&\vdots \\
a_{n-1} &= q_{n-1} a_n + a_{n+1}, \quad 0 < a_{n+1} < a_n \\
a_n &= q_n a_{n+1}
\end{aligned}$$

(a) Why is a_{n+1} a divisor of a_n ? Briefly justify your answer.

(b) Why is a_{n+1} a divisor of a_{n-1}? Carefully justify your answer.

(c) In a step-by-step argument, use (backwards) mathematical induction to verify that a_{n+1} is a divisor of a_i, $i = n, n-1, n-2, \ldots, 3, 2, 1$.

(d) Why is a_{n+1} a common divisor of a_1 and a_2?

(e) In a step-by-step argument, use (forwards) mathematical induction to verify that if G is a divisor of a_1 and a_2, then G is also a divisor of a_i, $i = 3, 4, 5, \ldots, n+1$. First, carefully explain why G is a divisor of a_3. Then examine the inductive step.

(f) From part (d) we know that a_{n+1} is a common divisor of a_1 and a_2. Carefully explain how part (e) can be used to conclude that a_{n+1} is in fact the greatest *common divisor of a_1 and a_2. A proof by contradiction might be appropriate here, following Euclid's example.*

Exercise 4.19. *In Proposition 1 Euclid describes an algorithm whereby, given two unequal numbers, the less is continually subtracted in turn from the greater until a unit is left. While in Proposition 2, Euclid describes an algorithm, whereby, given two unequal numbers, the less is continually subtracted from the greater until some number is left which measures the one before it.*

(a) To what extent are these algorithms identical?

(b) How are the algorithms in Proposition 1 and Proposition 2 designed to differ in application?

(c) *Does Euclid consider a unit as a number? Justify your answer citing relevant passages from the work of Euclid. Does Euclid consider a common measure as a number? Again, justify your answer from the work of Euclid.*

(d) *Why, in your opinion, does Euclid describe this algorithm using two separate propositions, when a single description could suffice?*

Exercise 4.20. *In the modern description of the Euclidean algorithm in Exercise* (4.18)*, the last equation written is*

$$a_n = q_n a_{n+1} \, ,$$

meaning that after n-steps, the algorithm halts and a_{n+1} divides (measures) a_n. Given any two positive integers a_1 and a_2, why must the Euclidean algorithm halt in a finite number of steps? Carefully justify your answer using the modern version of the algorithm.

Exercise 4.21. *Write a computer program in the language of your choice that implements Euclid's algorithm for finding the greatest common divisor of two positive integers. The program should accept as input two positive integers a_1, a_2, and as output print their greatest common divisor. Run the program for:*

(a) $a_1 = 3456$, $a_2 = 4563$,

(b) $a_1 = 625$, $a_2 = 288$,

(c) $a_1 = 216$, $a_2 = 288$.

Commentary. *The core of the project addresses many of our pedagogical goals, guided in exercises. Students must engage considerable subtleties, since there is more than one way to interpret what Euclid is saying. Moreover, it is intellectually useful to ask why for Euclid the algorithm is separated into two procedures, when today we make no distinction whether the GCD is one or greater. Justifying the algorithm from a modern viewpoint requires double mathematical induction, connecting ancient with modern methods and promoting understanding of modern standards and paradigms. And justifying the correctness of Euclid's claims provides an authentically important and worthwhile challenge for students, along with a clear sense for the roots of a critical piece of modern mathematics. Finally, the difference between Euclid's verbal presentation and our modern terminology and methods engenders considerable healthy cognitive dissonance for students to resolve.*

Acknowledgement

The development of curricular materials for discrete mathematics has been partially supported by the National Science Foundation's Course, Curriculum and Laboratory Improvement Program under grants DUE-0717752 and DUE-0715392 for which the authors are most appreciative. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

– projects-bookBarnett, J., Bezhanishvili, G., Leung, H., Lodder, J., Pengelley, D., Pivkina, I., Ranjan, D., Zack, M., *Primary Historical Sources in the Classroom: Discrete Mathematics and Computer Science*, book manuscript submitted.

– grant-web-siteBarnett, J., Bezhanishvili, G., Leung, H., Lodder, J., Pengelley, D., Pivkina, I., Ranjan, D., *Learning Discrete Mathematics and Computer Science via Primary Historical Sources*, `http://www.cs.nmsu.edu/historical-projects/`.
– designingBarnett, J., Lodder, J., Pengelley, D., Pivkina, I., Ranjan, D., Designing student projects for teaching and learning discrete mathematics and computer science via primary historical sources, in *Recent Developments in Introducing a Historical Dimension in Mathematics Education* (eds. V. Katz and C. Tzanakis), Mathematical Association of America, Washington, D.C, 2011, 189–201.
– TLHHeath, T., *Euclid: The Thirteen Books of the Elements*, Volume 2, Second Edition, Dover Publications, New York, 1956.
– KnuKnuth, D., *The Art of Computer Programming*, Volume 1, Addison-Wesley, Reading, Mass., 1968.
– lodder-hpm-2012Lodder, J., *Historical Projects in Discrete Mathematics*, HPM 2012, Daejeon, Korea.