Euclid's Algorithm for the Greatest Common Divisor

Desh Ranjan
Department of Computer Science
New Mexico State University

1 Numbers, Division and Euclid

It should not surprise you that people have been using numbers (and operations on them like division) for a very long time for very practical purposes like dividing up the money left by parents equally among 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 surprise to some of you that things like calculating divisors of numbers actually form the very core of methods that ensure security of all computer systems and internet communications. The RSA cryptosystem that is used extensively for secure communications is based on the assumptions of difficulty of calculating divisors of large numbers. So, people have been thinking of divisors of numbers for a very, very long time and calculating these actually has significant import in the modern day world. A very related and even more basic notion is the notion of multiples of quantities. One very natural way to compare quantities is to "measure" how many times do 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 one a sense of how the two lengths compare without actually knowing the two lengths. Unfortunately, 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, for the larger quantity we will have to use a greater number of parts than the smaller quantity. For example, when comparing two weights, one might observe that 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 us a sense of how big the first weight is to the second one. 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 we 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 relative magnitudes of the two weights. However, having smaller numbers like 7 and 5 to describe relative magnitudes seems intuitively and practically more appealing as opposed to 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. It turns out that this is a question that was given some thought by Greek mathematicians more than 2000 years ago. An important figure in (Greek) mathematics by the name of Euclid was one of the first to compile 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 the 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 or just the first to record it in writing.

1.1 Who was Euclid?

One of the most influential mathematicians of ancient Greece, Euclid, lived around 300 B.C.E. Very little is known about his life. It is generally believed that he was educated at Plato's academy in Athens, Greece. 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. By all accounts, it seems that he was a kind, fair, patient man. 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 that 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 mathemati-

cian 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 like (*Data, On Divisions of Figures, Phaenomena, Optics*, and the lost books *Conics* and *Porisms*), but *Elements* remains his best known compilation. The first "book" 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 geometry people studied until the Renaissance). This book has the definitions of basic geometric objects like points and lines along with the basic postulates or axioms. These axioms are then used by Euclid to establish many other truths (*Theorems*) of geometry. *Elements* is considered one of the greatest works of mathematics. 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 GCD. As such, he seems to be relating numbers to geometry which is quite different from present day treatment of number theory.

Today, erroneously, many different methods are called Euclid's algorithm to compute the greatest common divisor(GCD) of two numbers. By reading the original writings of Euclid you will discover the real Euclid's 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 [1] :

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

2 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 for "x divides y". We denote by $divisors(x)$ the set of all the numbers y such

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

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 2.1. What is the set of divisors of the number 315?

Exercise 2.2. 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 2.3. Calculate $divisors(3456)$.

Exercise 2.4. Calculate $cd(3456, 4563)$.

Exercise 2.5. 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 2.6. 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 quite as easy as finding the smallest common divisor.

3 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 [2]. 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.

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

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.

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

Exercise 3.2. What is likely meant when Euclid states that a number "measures" another number? Express Euclid's notion of "measures" in modern mathematical notation.

Exercise 3.3. Does the number 4 measure number 72? Does 5 measure 72? Briefly justify your answer.

Exercise 3.4. 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 3.5. 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 3.6. According to Euclid's definitions, are the numbers 21 and 55 composite to one another? Justify your answer.

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

[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.

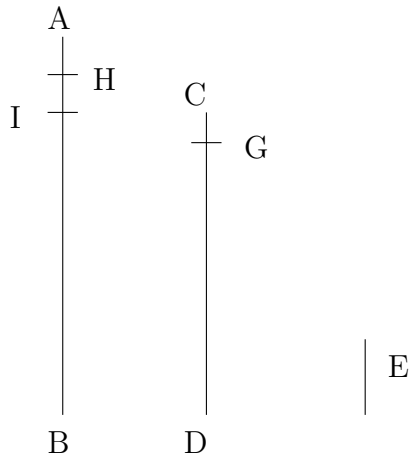
PROPOSITION 1.

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 3.7. 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 3.8. 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 3.9. 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) ?

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]

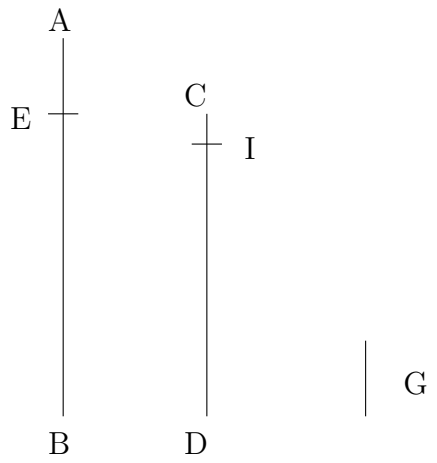
For a unit will not be left; otherwise AB, CD will be prime to one another [VII, I], which is contrary to the hypothesis.

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

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,

[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.



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 3.10. 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 3.11. 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 3.12. 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, …, a_{n+1} and a sequence of (positive) integer multipliers q_1, q_2, q_3, …, 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 3.13. 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 3.14. In the modern description of the Euclidean algorithm in Exercise (3.12), 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 3.15. 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) $a_1 = 216$, $a_2 = 288$.

References

[1] Knuth, D.E., *The Art of Computer Programming*, Volume 1, 1968.

[2] Heath T.L., *Euclid The Thirteen Books of the Elements*, Volume 2, Second Edition, Dover Publications, New York, 1956.