The Euclidean and Bezoutian Algorithms

Jack Chen
Old Scona Academic High School

There is a systematic method of finding the greatest common divisor of two positive integers. It is called the **Euclidean Algorithm** after the ancient Greek mathematician Euclid, famous for his treatise *The Elements*, which is the premiere publication on the subject of geometry.

The calculations required are mechanical, and can be summarized as follows.

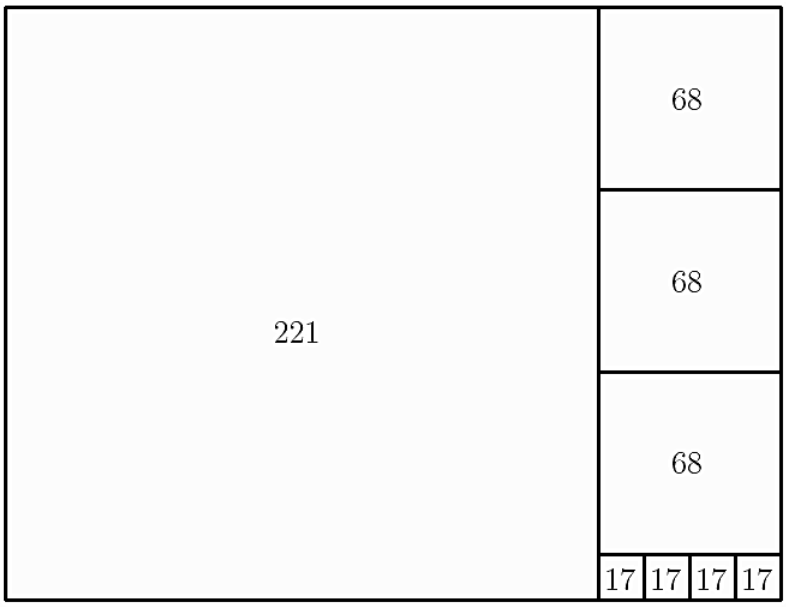
(1) Put the larger of the two given numbers into box A and the smaller one into box B.
(2) Divide the number in box A by the number in box B.
(3) If the division is exact, go to Step (5). If not, move the number in box B to box A and put the remainder obtained from the division into box B.
(4) Return to Step (2).
(5) The number in box B is the greatest common divisor we seek, and the Algorithm is terminated.

As a numerical example, let us find the greatest common divisor of 289 and 221.

Box A	Box B	Division
289	221	$221 \overline{)\ 289}$ $\quad 221$ $\quad 68$
221	68	$68 \overline{)\ 221}$ $\quad 204$ $\quad 17$
68	**17**	$17 \overline{)\ 68}$ $\quad 68$ $\quad\ \ 0$

The algorithm was first described in Euclid's *The Elements*, though Euclid himself –who complied previous mathematical results in his treatise– may not have discovered it (B. L. van der Waerden has argued that the algorithm originated from the school of Pythagoras). As Euclid is most famous for his geometric work, a natural question, then, is why the geometer Euclid has this number-theoretic algorithm named after him. It turns out that in ancient Greece, arithmetic was visualized in geometric means. For instance, the addition 3 + 4 was visualized as the construction of a line segment whose length is equal to the total length of two given segments of lengths 3 and 4. Furthermore, Greek numerals were clumsy and quickly became long as numbers became large. They could not be added conveniently and as a result, the Greeks turned to geometry. Indeed, in ancient Greece, the development of number theory pales in comparison to the development of geometry. However, of note is that fact that books VII, VIII, and IX of *The Elements* are all about number theory, so perhaps it isn't all too surprising that a number theory algorithm was named after Euclid.

How then can the Euclidean Algorithm be visualized? Let us continue with the example above, that of finding the greatest common divisor of 289 and 221. We start with a 221 × 289 rectangle. At each stage, we cut off the largest possible square and discard it. We continue until the residual rectangle is a square. The side length of this final square will be the desired greatest common divisor.



The steps in the geometric construction correspond exactly with the steps in the numerical computation before.

It should be emphasized that the geometric construction always terminates since the integral dimensions of the resulting rectangles continue to diminish. From a 221×289 rectangle, we downsize to a 68 × 221 rectangle and then a 17×68 rectangle. After cutting off 17 × 17 squares, we are left with a single 17×17, signifying that 17 is the desired greatest common divisor.

It is easy to see why this geometric form of the Euclidean Algorithm always produces the correct answer. In our example, the final step shows that 17 divides 68. Since 221 is a combination of 68 and 17, 17 also divides 221. Similarly, since 289 is a combination of 221 and 68, 17 divides 289 too. Hence 17 is indeed a common divisor of 289 and 221. Moreover, it must be the greatest common divisor. If there is a greater one, it would have appear before we come to the 17 × 17 square.

Note that we used a rectangle in our geometric representation, and not another figure such as a line segment or triangle. A rectangle allows us to make the numbers 289 and 221 into the figure's side length. Following the steps above, we obtain a resulting square whose side length is the greatest common divisor. A rectangle is a two-dimensional figure that allows us to represent both 289 and 221 in tandem. A representation of the Euclidean Algorithm could be made with two separate line segments, but the rectangular representation is both neater and more elegant.

The symbol $\triangle$ is used in this paper to represent the operation of finding the greatest common divisor of two positive integers. The companion operation of finding the least (positive) common multiple of two positive integers is symbolized by $\bigtriangledown$. The benefit of using these symbols in this context is twofold. One, it allows for neater presentation less parentheses are needed (parentheses are traditionally used to represent the greatest common divisor operation). Two, it emphasizes the fact that the process of calculating a greatest common divisor is a binary operation, similar to addition or multiplication.

Placing a symbol between two elements makes the greatest common divisor operation appear visually to be a binary operation, and is thus a more accurate representation.

For positive integers a, b and c, we have

(1) $a\triangle a = a\bigtriangledown a = a$;

(2) $a\triangle b = b\triangle a$ and $a\bigtriangledown b = b\bigtriangledown a$;

(3) $a\triangle(b\triangle c) = (a\triangle b)\triangle c$ and $a\bigtriangledown(b\bigtriangledown c) = (a\bigtriangledown b)\bigtriangledown c$;

(4) $a\triangle(b\bigtriangledown c) = (a\triangle b)\bigtriangledown(a\triangle c)$ and $a\bigtriangledown(b\triangle c) = (a\bigtriangledown b)\triangle(a\bigtriangledown c)$.

What we have proved above is that $289\triangle 221 = 221\triangle 68 = 68\triangle 17 = 17$.

A linear combination of two positive integers, say 289 and 221, is an expression of the form $289x + 221y$ where x and y are integers, obviously one positive and one non-positive. An important property of the greatest common divisor of two positive integers is that it is always expressible as a linear combination of them. This can be proved theoretically using the Well-Ordering Principle, but there is a method which produces explicit values for x and y. This is known as the **Bezoutian Algorithm**, named after Bezout, an eighteenth century French mathematician.

The Bezoutian Algorithm is closely tied to the Euclidean Algorithm. In fact, it may be regarded as an extended Bezoutian Algorithm. Whereas the Euclidean Algorithm finds us the greatest common divisor, the Bezoutian Algorithm extends the process and finds us the greatest common divisor as a linear combination of the two original numbers. The Bezoutian Algorithm, in a sense, reverses the Euclidean Algorithm by finding combinations of numbers that result in a given greatest common divisor. Additionally, both algorithms have similar applications. For example, they are both widely used in cryptography and public-key encryption. The Bezoutian Algorithm consists of two steps.

(1) For each remainder obtained in the Euclidean Algorithm, starting with the smallest, write down an equation showing how this remainder is obtained. In our introductory example, these equations are:

$$17 = 221 – 3\,(68)\,,$$
$$68 = 289 – 221\,.$$

(2) Combine the equations obtained in Step (1), starting with the equation for the greatest common divisor. Substitute into this equation the one for the second smallest remainder, and then simplify by combining like terms. Continue until all intermediate numbers generated by the Euclidean Algorithm have been eliminated, and the original two numbers have been reached. Continuing with the example in Step (1), we have

$$\begin{aligned} 17 &= 221 – 3\,(68) \\ &= 4\,(221) – 3\,(289) \end{aligned}$$

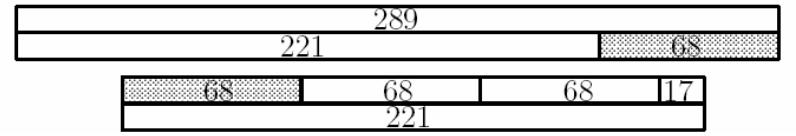
This yields the linear combination $289\,(–3) + 221(4) = 17$.

The Bezoutian Algorithm, though straightforward, is quite cumbersome. It is also counter intuitive since we usually simplify things rather than blowing them up. Sometimes, halfway through the computations, we start simplifying too far, and end up with a trivial statement such as $1 = 1$. On the other hand, if we have made some errors, there is a very good way to find out where it is. With no errors, each line must have the greatest common divisor as its value. So the first line where the value is no longer the same is obtained erroneously from the previous line.

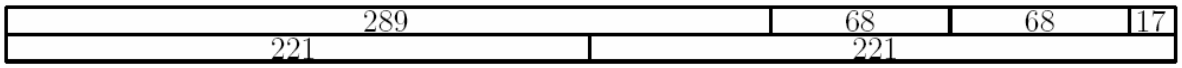
The Bezoutian Algorithm was not featured in *The Elements*, but as an extension of the Euclidean Algorithm, it could have been. It would not be unreasonable for the Bezoutian Algorithm to be featured in Book 14 of *The Elements*, which would be an extension of the number theory presented in Book 7. If the Bezoutian Algorithm were featured in *The Elements*, there would be several implications. It may have led to a quicker development of Euclid's Lemma and The Chinese Remainder Theorem, both of which resulted from the Bezoutian Algorithm. Additionally, ancient Greece and the mathematical world as a whole would have a greater understanding of number theory and modular

arithmetic, potentially leading to a faster development of mathematics.

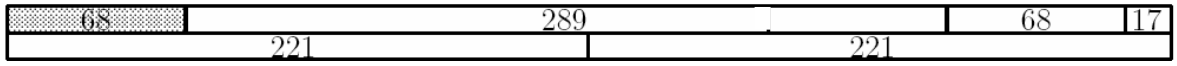
To visualize it geometrically, let us extract from the earlier diagram for the Euclidean Algorithm two significant portions.



We can combine the two diagrams above by removing the shaded parts, as shown below.



We are down from three copies of 68 to two. To continue its elimination, we first modify the last diagram by moving one copy of 68 to the left, as shown below.



Combine this with the first diagram to eliminate the second copy of 68. After the third copy of 68 has been eliminated in the same way, we will have four copies of 221 on the bottom row and three copies of 289 plus the lone copy of 17 on the top row.

Author's e-mail: jackchen5@hotmail.com

《數學數育》第 38 期勘誤表 Errata – EduMath 38			
頁碼	章節/位置	原文	修正為
70	• Method 2	$MK^2 = \sqrt{2}x$ cm	$MK = \sqrt{2}x$ cm
71	• Method 3 (b) (i)	Express *AE*, *DE* and *AE* in terms of *x* respectively.	Express *AK*, *KE* and *AE* in terms of *x* respectively.
72	4. Concluding Remarks	… also help our students to figure out that by …	… also help our students to figure out that *KE*=*ME* by …
72	4. Concluding Remarks	In fact, students can also find by …	In fact, students can also find *CE* by …