Introduction

The Euclidean algorithm is a unique method for finding the greatest common divisor of two integers. It builds upon the idea that if any number divides two integers, it also divides their greatest common divisor. A process using this concept can be repeated until one singular greatest common divisor is found. First introduced over two-thousand years ago, it has had a hand in the development of many other mathematical concepts including the unique factorization theorem and the linear Diophantine equations. Today, the algorithm is still relevant and proves to be applicable in several fields of mathematics.

Historical Background

The Euclidean algorithm was first introduced in 300 B.C.E. by Greek mathematician Euclid, in Book VII of his *Elements*. *Elements* was a collection of books traditionally divided into three main parts: Plane Geometry, Arithmetic, and Solid Geometry, (Artmann, 1991). It is not certain however, that Euclid was the one to discover the algorithm, as many of the mathematical concepts in his books were based on books written by earlier mathematicians. Supposedly, many of the ideas presented throughout his book were based to a large extent on the mathematical discoveries made in the school of Pythagoras. "Euclid's whole thirteen books were devoted to explaining the five 'divine solids of Plato,' first investigated by Pythagoras" (Gould, 1943). Euclid's contributions to developing the algorithm should not go unnoticed however, as his version in *Elements* is widely known and has been instrumental in the formation of countless other mathematical concepts since that time.

Algorithm Description

The basis for the Euclidean algorithm is deeply rooted in many of the ideas introduced in *Elements* and is proved by Euclid's extensive work with number theory. In Book VII, after describing how the algorithm works, he presents an algebraic property: "If a number divides two numbers, then it divides their greatest common divisor" from which "the common divisors of a and b are exactly the common divisors of a and r" (Pengelley & Richman, 2006) is considered true. Both of these ideas are essential to the implementation of the algorithm, as equations involving three integers and a remainder will be formed an indefinite number of times until the greatest common divisor is found.

To start, two integers, *a* and *b,* are chosen. To find (*a, b*)*,* or the greatest common divisor of *a* and *b*, they are written in the form:

$$b = aq_1 + r_1$$

where q_1 and r_1 are also integers and $b > a$. In this equation, the larger of the two integers *b* is dividing *a* to yield the quotient q_1 with a remainder of r_1. This notation is critical, as it will set up the next equation, for which we're now finding (a, r_1):

$$a = r_1q_2 + r_2$$

The equation is in line with the idea mentioned above, which explains how any common divisor of *a* and *b* will also be a common divisor of *a* and *r*, and this includes the greatest common divisor of the two integers. The next equation will find ($r_{1,}\ r_2$):

$$r_1 = r_2q_3 + r_3$$

By rewriting the equation using r_1 and r_2, we're able to use smaller integers which means we're narrowing down on the greatest common divisor. The process is stopped when we reach an equation with a remainder of zero, for which the remainder from the previous equation is the greatest common divisor of *a* and *b*. The algorithm can be much better understood using a real example of how it works. In this example, we're finding (630, 132):

630 = 132(4) + 102

132 = 102(1) + 30

102 = 30(3) + 12

30 = 12(2) + **<u>6</u>**

12 = 6(2) + 0

The algorithm shows that (630, 132) = 6. The process described above repeats until a remainder of zero is reached, so the remainder from the previous equation is taken as our greatest common divisor. The answer 6 is bolded and underlined. In this next example, we'll find (4784, 7245):

7245 = 4784(1) + 2461

4784 = 2461(1) + 2323

2461 = 2323(1) + 138

2323 = 138 (16) + 115

138 = 115(1) + **<u>23</u>**

115 = 23 (5) + 0

The process shows how each step is independent of what comes before it, as the greatest common divisor of the pair of integers in each equation is the same:

(4784, 7245) = (4784, 2461) = (2461, 2323) = (2323, 138) = (138, 115) = (115, 23) = 23.

In the case either *a* or *b* or both are negative integers, their greatest common divisor remains unchanged, so (12, 16) = (-12,16) = (12, -16) = (-12, -16) = 4. This is because 12 and 16 will always divide 4 evenly regardless of whether they're negative or positive- their quotient will just have a different sign.

The Euclidean algorithm can also be demonstrated using matrices. Doing this provides a more visual representation of how the algorithm works, but is more difficult to implement. We find (630, 132) again using matrix form:

$$\begin{pmatrix} 1 & 0 & 630 \\ 0 & 1 & 132 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & -4 & 102 \\ 0 & 1 & 132 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 1 & -4 & 102 \\ -1 & 5 & 30 \end{pmatrix} \rightarrow \begin{pmatrix} 4 & -19 & 12 \\ -1 & 5 & 30 \end{pmatrix}$$

$$\rightarrow \begin{pmatrix} 4 & -19 & 12 \\ -9 & 43 & 6 \end{pmatrix} \rightarrow \begin{pmatrix} 22 & -105 & 0 \\ -9 & 43 & \textcircled{6} \end{pmatrix}$$

The first matrix includes the identity matrix on the left side and puts the larger of the two integers, 630, on top. 132 goes into 630 four times, so we will subtract R1 (row 1) by 4 * R2 and replace R1 with the resulting vector keeping R2 the same. Next, we see that 102 goes into 132 one time, so we will subtract R2 by 1 * R1 and replace R2 with the resulting vector keeping R1 the same. The process for which the vector with the larger rightmost value is subtracted by the other vector multiplied by an integer is repeated until one of them has zero as its rightmost value, which is shown in the last matrix (Ibrahim & Gucker, 1972). The greatest common divisor, 6, is circled. It is important to note that 630 * (-9) + 132 * (43) = 6. This is an example of Bezout's equation where gcd(a, b) = $sa + tb$ for some integers s and t: one of the many applications of the Euclidean algorithm (Pengelley & Richman, 2006).

Applications

The applications for the Euclidean algorithm are innumerable, as its purpose, finding the greatest common divisor of two integers, is trivial, but proves to be fundamental to many other mathematical concepts in number theory and algebra "as it is susceptible to great generalization" (Clair, 1954).

The algorithm has many applications related to fractions alone, one of the less complex being its use in simplifying them. Given a numerator and a denominator, one can use the algorithm to find the greatest common divisor of the two integers. With their greatest common divisor, the fraction can then be simplified. For example, if a fraction is 34/119, solving for (34,119) results in 17. Dividing both the numerator and denominator by this number gives an equivalent and simplified fraction of 2/7. The algorithm saves time, especially with larger integers as the guess and check method is often used instead. Another application involving fractions is the approximation of complicated numbers, irrational or rational, using rational numbers. Clair (1954) gives an example using the fraction 29/73. When divided, the repeating decimal 0.39726 is the quotient. By using the Euclidean algorithm in matrix form to find (29, 73), the resulting vector gives the equation 73 * (2) - 29 * (5) = 1. Here (29, 73) = 1, and the fraction 2/5 is a great approximation for 29/73 since 2 divided by 5 is 0.4. The Euclidean algorithm can also be used to decompose fractions into partial fractions. Clair (1954) gives an example using the fraction 7/30. We can start by finding two factors of 30, say 5 and 6, and then finding their greatest common divisor. We found (5, 6) = 1 and 1 * 6 - 1 * 5 = 1. By dividing both sides by 30, we now have 1/5 - 1/6 = 1/30. By repeating the process with 1/6, we have the equation 1/6 = 1/2 - 1/3. Plugging this back into the original equation, we write out 1/30 = 1/5 - 1/2 + 1/3. The rest of the partial fraction is found below:

7/30 = 7/5 - 7/2 + 7/30 = 1 2/5 - 3 1/2 + 2 1/3 = 2/5 - 1/2 + 1/3.

The algorithm's relation to partial fractions opens up a new field of applications, as this same process can also be used with polynomials to break them down into their linear combinations (Clair, 1954).

There are other significant applications of the algorithm, like its use in proving the unique factorization theorem, also called the fundamental theorem of arithmetic. The theorem states that "Every counting number other than 1 is either itself a prime or it can be factored uniquely as a product of primes" (Greenleaf & Wisner, 1959). Some more applications include the algorithm's use in solving linear Diophantine equations as well as its use in relation to Gaussian integers (Clair, 1954). These applications are much more complex than the ones introduced before, but they show the usefulness of the Euclidean algorithm and the influence it has had on many mathematical concepts.

References

Artmann, B. (1991). Euclid's "Elements" and its Prehistory. *Apeiron: A Journal for Ancient Philosophy and Science*, *24*(4), 1–47. http://www.jstor.org/stable/40913670

Beardon, A. F. (2000). 84.40 Reflections on Euclid's Algorithm. *The Mathematical Gazette*, *84*(500), 294–296. https://doi.org/10.2307/3621668

Clair, H. S. (1954). Euclid's Algorithm and Its Applications. *Mathematics Magazine*, *28*(2), 71–82. https://doi.org/10.2307/3029367

Gould, S. H. (1943). Euclid and Pythagoras. *The Classical Weekly*, *36*(10), 112–113. https://doi.org/10.2307/4341603

GREENLEAF, N., & WISNER, R. J. (1959). The unique factorization theorem. *The Mathematics Teacher*, *52*(8), 600–603. http://www.jstor.org/stable/27956028

IBRAHIM, A., & GUCKER, E. (1972). THE EUCLIDEAN ALGORITHM as a MATRIX TRANSFORMATION. *The Mathematics Teacher*, *65*(3), 228–229. http://www.jstor.org/stable/27958796

Pengelley, D., & Richman, F. (2006). Did Euclid Need the Euclidean Algorithm to Prove Unique Factorization? *The American Mathematical Monthly*, *113*(3), 196–205. https://doi.org/10.2307/27641888