The Euclidean Algorithm

by Richard Born
Associate Professor Emeritus
Northern Illinois University
rborn2@niu.edu

Introduction

The *greatest common divisor* (GCD) of a pair of positive integers is the largest positive integer that divides both integers without a remainder. For example, the GCD of 18 and 12 is 6. Other terms that mean the same thing as GCD include, but are not limited to, greatest common factor (GCF) and highest common divisor (HCD).

The concept of GCD is central to the mathematical study of number theory. However, there are other applications of GCD. One of the most common is simplifying fractions, though you may ***not*** have made use of the GCD ***concept*** while simplifying fractions. For example, 12/18 reduces to 2/3 by dividing both the numerator and denominator by 6, their GCD. Another classic example involves tiling a floor. If you have a space that is 12" x 18", you might want to know the largest square tiles that could be used to cover the space exactly. No problem—simply use square tiles that are 6" on a side.

Although there are several ways to compute the GCD of a pair of numbers, a very efficient way dates back to the ancient Greek mathematician Euclid. His technique for computing the GCD is known as the Euclidean algorithm and appeared in his book *Elements*. Figure 1 shows how to use the Euclidean algorithm to compute the GCD of 18 and 12. The Euclidean algorithm is iterative. In the first iteration of the example, 18 is divided by 12, giving a quotient of 1 and a remainder of 6. In the second iteration, the previous divisor becomes the new dividend, and the previous remainder becomes the new divisor. 12 is divided by 6, giving a quotient of 2 and a remainder of 0. When the remainder is 0, the iterations stop and the current divisor is the GCD. Equivalently, we could say that the GCD is the previous iteration's remainder.

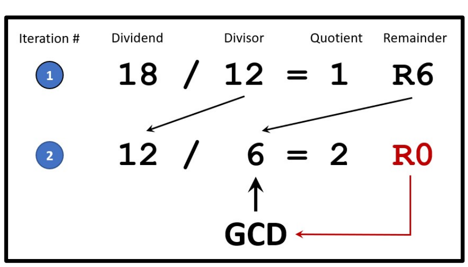

Figure 1

Evo: The Euclidean Algorithm Tutor

In this lesson, Evo is the teacher's helper. Evo demonstrates how to compute the GCD of any pair of positive integers up to 99. Evo accomplishes this via a provided OzoBlockly program that makes use of the Ozomap shown in Figure 2. Larger copies suitable for student use can be obtained by printing the document entitled *Ozomap for GCD Demo.pdf*.

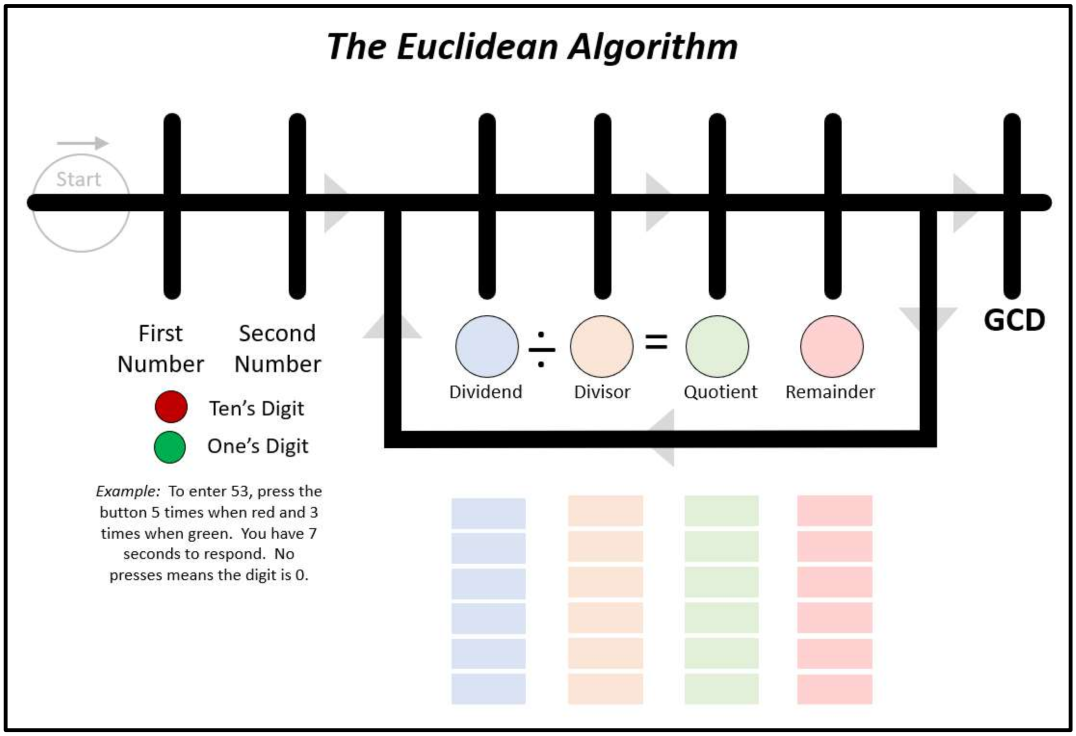

Figure 2

After loading the OzoBlockly program *TheEuclideanAlgorithm.ozocode* into Evo, Evo is placed on the start location facing the direction of the arrow. The program is started, Evo's top light turns white, and Evo moves to the "First Number" location. As indicated in the Ozomap, the light will be red for 7 seconds, giving the student time to enter the ten's digit of the first number. The light then turns green for 7 seconds, giving the student time to enter the one's digit of the first number. No presses indicate that the digit is zero. Evo then moves to the "Second Number" location, where the student similarly enters the value for the second number. Evo then goes through the first iteration in the Euclidean algorithm. He stops and speaks the value of the dividend, divisor, quotient, and remainder. The colored rectangles are provided for the student to pencil in the values as Evo speaks them. Pencil is recommended so the values can be erased when the GCD of another pair of numbers is to be computed. If the remainder is not zero, then Evo will loop back for another iteration. When the remainder is zero, Evo knows that the GCD has been found, stops at the GCD intersection, and speaks the value of the GCD.

An Example

Figure 3 shows the results for an example in which the first number is 99 and the second number is 56. Equivalently, the first number could be 56 and the second number 99, since the algorithm will always take the larger of the two numbers as the original dividend. The student can easily uncover the pattern by which the Euclidean algorithm works to find the GCD. The dividend for an iteration is the same as the previous iteration's divisor. The divisor for an iteration is the previous iteration's remainder. When the remainder is 0, the GCD is the current iteration's divisor. Equivalently, you could say that the GCD is the previous iteration's remainder.

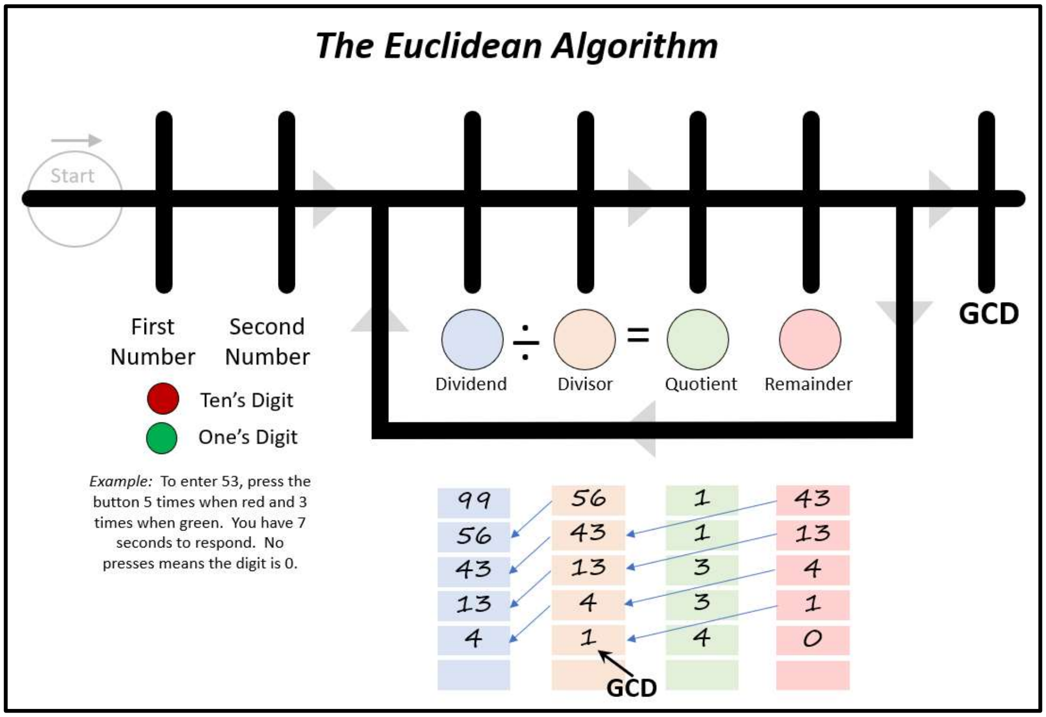

Figure 3

Note that the example if Figure 3 tells us that the numbers 99 and 56 are relatively prime. Two numbers are said to be *relatively prime* if there is no integer greater than 1 that divides them both.