Math From Scratch Lesson 18: The Euclidean Algorithm

W. Blaine Dowler

December 27, 2011

Contents

This content was originally written as a standalone teaching tidbit for Bureau 42.

1 The Algorithm

When students are first introduced to the concept of greatest common factors, they are not always entirely comfortable with division. The usual means of calculating the greatest common factor between two numbers involves listing all of the possible factors for both numbers, and then checking the lists for numbers that appear on both. This methodology works, but has two drawbacks:

1. The student must be comfortable with division.
2. The student must be able to recognize any and all factors of a number.

This method may work well for finding the greatest common factor shared by 12 and 18, but how well does it work for finding the greatest common factor between 221 and 351?

Euclid developed an alternative algorithm[1] over 2000 years ago, and the only operation students need apply is subtraction. You begin with your original

[1] The algorithm is called the Euclidean algorithm, for reasons that should now be obvious.

numbers, say 24 and 60, and subtract the smaller from the larger:

$$60 - 24 = 36$$

The two smallest numbers in this set are 24 and 36. Again, we subtract the smaller from the larger:

$$36 - 24 = 12$$

And again:

$$24 - 12 = 12$$

And again, until we get down to 0 for an answer:

$$12 - 12 = 0$$

Once we got to 0, the number we subtracted from itself (12) is our greatest common factor: $24 = 2 \times 12$ and $60 = 5 \times 12$.

For our more detailed example, we do exactly the same thing:

$$\begin{aligned} 351 - 221 &= 130 \\ 221 - 130 &= 91 \\ 130 - 91 &= 39 \\ 91 - 39 &= 52 \\ 52 - 39 &= 13 \\ 39 - 13 &= 26 \\ 26 - 13 &= 13 \\ 13 - 13 &= 0 \end{aligned}$$

Our greatest common factor is 13: $221 = 13 \times 17$, $351 = 13 \times 27$.

Astute readers may recognize the process of repeated subtraction as longhand division, just as repeated addition is longhand multiplication. If a student is comfortable with division, this can actually be done more efficiently by using the remainders of divisions instead, as follows:

$$\begin{aligned} 351 \div 221 &= 1R130 \\ 221 \div 130 &= 1R91 \\ 130 \div 91 &= 1R39 \\ 91 \div 39 &= 2R13 \\ 39 \div 13 &= 3R0 \end{aligned}$$

In this formulation, it is the divisor when the remainder equals 0 that is our greatest common factor.

This method is no more or less valid than those usually taught in school. It does, however, have the advantages of allowing students not comfortable with division to resort to the more familiar subtraction, and of allowing students to find the greatest common factors whether they recognize the prime factors in the original numbers or not.

2 Why It Works

To prove the algorithm works, we'll use both the subtraction and the division formulation of the algorithm. We need to show a few things to prove that our candidate (the final non-zero remainder r_k) is the greatest common factor g:

1. Both a and b are divisible by r_k, proving that r_k is one of the common factors.
2. r_k is the greatest number that divides into both a and b.

We are looking to find g, the greatest common factor of two numbers a and b, which are not both 0. Let us assume that $b \neq 0$. We can do this because the decision of which variable to label as which is entirely arbitrary. We can find $a \div b = q_1 R r_1$, where q_i is the quotient for that step of the algorithm, and r_1 is the remainder from that step of the algorithm. By the rules of remainders and division, $b > r_1$. We now find $b \div r_1 = q_2 R r_2$, so our inequality builds to $b > r_1 > r_2$. We continue the process until we get $r_{k-1} \div r_k = q_{k+1} R 0$, making r_k our final non-zero remainder. If all goes as planned, then $r_k = g$.

By the nature of division, $a \div b = q_1 R r_1$ means $a = b \times q_1 + r_1$. We can manipulate this to find $r_1 = a - b \times q_1$. Now, if a and b have any common factor d, such that $a = kd$ and $b = ld$, then we can say $r_1 = kd - ldq_1 = d\,(k - lq_1)$. In other words, the entire right hand side is divisible by d, so therefore r_1 must also be divisible by d. Similar arguments show that $r_2, r_3, \ldots, r_k$ are also all divisible by d.

In our final step, we have no remainder: $r_{k-1} = r_k \times q_{k+1}$. This proves that r_{k-1} is divisible by r_k. We can back that up, step by step, as in $r_{k-2} = r_{k-1} \times q_k + r_k$ (in which the entire right hand side is divisible by r_k, and therefore the left must be also) to show that every previous remainder, a and b are all divisible by r_k. This satisfies our first criterion to see if $r_k = g$: r_k divides evenly into both a and b. Therefore, $r_k \leq g$: we'll call this Result A for future reference.

We use the subtraction model for the second half of the proof.[2] Our first remainder is found by subtracting the larger number from the smaller between a and b. Again, we can arbitrarily decide that $a > b$ for the purposes of notation: the pedantic reader can reproduce the entire argument for the other case if he or she so chooses. To get to our first remainder r_1, we subtract b from a some number q_1 times, so that $a - q_1 b = r_1$. Thus, whatever the greatest common factor of a and b is, the left hand side is divisible by that number g, and therefore, so is the right hand side, which is r_1. In other words, the first remainder is guaranteed to be a multiple of the greatest common factor g.

The second remainder is formed by dividing b by r_1, which is equivalent to subtracting q_2 multiples of r_1 from b, or $b - q_2 r_1 = r_2$. Both b and r_1 are multiples of g, so the left hand side is divisible by g, and so the right hand side r_2 is also divisible by g. When r_3 is found from $r_1 - q_3 r_2$ we apply the same logic, and so forth, so that r_i is divisible by g for any i such that $1 < i < k$. This is what we need: it means that $g \leq r_i$ for all meaningful values of i, which means that $g \leq r_k$, which we call Result B.

Now we combine Result A with Result B: $r_k \leq g \leq r_k$. If either of those statements needed the inequality rather than the equality, we'd have the nonsensical $r_k < r_k$. Therefore, that can't be the case, and we must use the equality: $r_k = g$. Thus we have proven that the Euclidean algorithm does, indeed, produce the greatest common factor g as its last nonzero result.

[2]Remember that the subtraction and division appearances are entirely equivalent; I'm switching notation between the two in order to make the steps easier to write down, but a result in one notation is just as valid as a result in the other notation.