In Favour of the Euclidean Algorithm

By **Colin Foster**

Mathematics teachers often talk as though algorithms are boring – we prefer to call our methods ‘procedures’ or ‘processes’, because ‘algorithms’ sound like rote learning, and something we should shun. But algorithms are often beautiful (see Fry, 2018), and the *Euclidean Algorithm* is a good example of this. I am not sure why it is not taught more frequently in schools, and why, when it is, it tends (at least in my experience) to be introduced as an ‘extension’ for higher attainers. It is often a very efficient method.

Consider this question:

What is the highest common factor (HCF) (Note 1) of 1240 and 1241?

How would you approach this? I think that students and teachers often have broadly two methods for finding the HCF:

1. *If the given numbers are small and familiar, find all of the factors of both numbers and pull out the highest common one by inspection.*

For example, if the two numbers were 12 and 40, we might list (perhaps mentally) the factors of 12 (12, 6, 4, 3, 2, 1), since 12 has fewer factors than 40 does, and, starting with the highest factor, check to see whether each factor of 12 is also a factor of 40. We note that 12 and 6 are not factors of 40, but 4 is, so the HCF must be 4.

2. *If the numbers are large and less familiar, find and use their prime factorisations.*

Here, if the two numbers were 120 and 72, we might write these as products of powers of prime numbers:

$120 = 4 \times 3 \times 10 = 2^2 \times 3 \times (2 \times 5) = 2^3 \times 3 \times 5$

$72 = 8 \times 9 = 2^3 \times 3^2$

Then, by pulling out the smaller power of each, prime number, and multiplying them together, the largest factor the two numbers have in common would be $2^3 \times 3 = 24$.

However, I don’t think that either of these methods is particularly convenient for big numbers. In the question I gave above, with 1240 and 1241, Method 2 would involve worrying about whether 1241 is prime or not, which is not obvious, and figuring out the factorisation of 1240, which is not particularly easy. By contrast, the Euclidean Algorithm enables us to see immediately that the numbers are co-prime (i.e., that their HCF is 1).

The key insight of the Euclidean Algorithm is that HCF(a, b), where $a > b$, is equal to HCF($a - b$, b) (Note 2). In other words, we can replace the larger of the two numbers by the difference, and the HCF is unchanged. Indeed, we can do this as many times as we wish, so, if $a - b$ is *still* greater than b, then we can subtract *another* b, and so on. We could write HCF(a, b) = HCF($a - nb$, b), where n is any integer such that $a - nb > 0$. Another way to say this is that HCF(a, b) = HCF(r, b), where r is the *remainder* after dividing a by b.

Subtracting multiples of the smaller number will always give us an easier HCF problem to solve. In the example I posed above, HCF(1241, 1240) must be equal to HCF(1241 − 1240, 1240) = HCF(1, 1240), and this must be equal to 1, because the only factor of 1 is 1. In general,

$$\text{HCF}(a + 1, a) = \text{HCF}(1, a) = 1, \text{ for all } a,$$

meaning that pairs of consecutive positive integers *always* have a HCF of 1. I find that this is one of those facts that seems simple but people are often surprised that they didn’t know.

So, *why* is it true that HCF(a, b) = HCF ($a - b$, b), for all $a > b$?

If HCF(a, b) = k, then this means that $nk = a$ and $mk = b$, for integers n and m, and that there is *no* $k' > k$ such that $n'k' = a$ and $m'k' = b$ for integers n' and m'. The quantity $a - b = nk - mk = (n - m)k$, so k must be a factor of $a - b$, and there cannot be a *higher* factor of $a - b$ that is *also* a factor of b, since, if there were, it would *also* be a factor of a, and therefore k would *not* be the *highest* common factor of a and b. So k must be the HCF of $a - b$ and b. This is an argument that sounds more complicated than it is! For a really nice visual approach to this, see Vicky Neale’s, LUMEN video (Neale, n.d.). Removing the largest possible squares from rectangles is a great way to see what the Euclidean Algorithm is doing.

Repeated applications of the Euclidean Algorithm quickly reduce large numbers down to size. Our example above with 120 and 72 becomes:

$$\begin{aligned}&\text{HCF}(120, 72)\\&= \text{HCF}(120 - 72, 72) = \text{HCF}(48, 72)\\&= \text{HCF}(48, 72 - 48) = \text{HCF}(48, 24)\\&= \text{HCF}(48 - 24, 24) = \text{HCF}(24, 24)\\&= 24.\end{aligned}$$

Surely *subtracting* numbers in this kind of way should be an easier process for students than finding prime factorisations and then juggling them to obtain the HCF? So why isn't this commonly taught as the standard method?

I can think of two possible objections to teaching this as the principal method for students to use:

1. *What about when you need to find the HCF of 3 or more numbers; for example, HCF(120, 72, 40)?*

With the prime factorisation method, we would write:

$$\begin{aligned}120 &= 12 \times 10 = (4 \times 3) \times (2 \times 5) = 2^3 \times 3 \times 5,\\72 &= 8 \times 9 = 2^3 \times 3^2,\\40 &= 8 \times 5 = 2^3 \times 5.\end{aligned}$$

And then we would pull out the largest common factor, which would be $2^3 = 8$. However, any tiny error in any of the indices will lead to disaster. So too will any confusion caused by uncertainty over which powers of the 3s or 5s should be included. I have sometimes found that the easiest way to avoid this problem is to use the fact that $a^0 = 1$ for all $a \neq 0$ to write the numbers as products of powers of *each* prime number, including zeroth powers where necessary, explicitly as:

$$\begin{aligned}120 &= 2^3 \times 3^1 \times 5^1,\\72 &= 2^3 \times 3^2 \times 5^0,\\40 &= 2^3 \times 3^0 \times 5^1.\end{aligned}$$

Then, it may be clearer that the *highest common factor* is going to be $2^3 \times 3^0 \times 5^0 = 8$, because this is just the product of the lowest power of each prime number, and this avoids mistakenly including any higher powers of 3 or 5.

However, with the Euclidean Algorithm, you can just subtract multiples of *any* of the three numbers from *any* of the other numbers, provided that you always ensure that you remain within the positive integers, so in a sense this is even easier than with two numbers, as you have more possibilities to reduce the complexity quickly. For example,

$$\begin{aligned}&\text{HCF}(120, 72, 40)\\&= \text{HCF}(120 - 2 \times 40, 72 - 40, 40)\\&\text{or HCF}(40, 32, 40)\\&= \text{HCF}(40 - 32, 32)\\&\text{or HCF}(8, 32) = 8.\end{aligned}$$

So, even here, the Euclidean Algorithm seems much easier than juggling prime factors, as it just involves repeated subtraction.

2. *What about when you need to find the lowest common multiple (Note 3)? If you need to teach the prime factorisation method for that, then the saving associated with teaching the Euclidean Algorithm for the HCF is much less substantial.*

As Morgan (2019) has pointed out, one option for finding the LCM is to calculate it from the HCF using the formula (Foster, 2012):

$$\text{LCM}(a, b) = \frac{ab}{\text{HCF}(a, b)}.$$

It makes intuitive sense that the LCM is simply the *product* of the two numbers, provided that they are co-prime. If they are *not* co-prime, we just have to divide out the HCF > 1 that *prevents* them from being co-prime. So, why not simply use the Euclidean Algorithm to find the HCF, and then divide the product by this to obtain the LCM (Note 4)?

Many of the problems students have with finding HCF and LCM arise from the business of finding the prime factorisations, followed by remembering/understanding how to manipulate these expressions to obtain the HCF and LCM. The processes are similar but different, and so easily confused. To find the HCF, we pull out the *lowest* power of each prime number, and multiply them together; to find the LCM, we pull out the *highest* power of each prime number and multiply them together. Highest goes with lowest, and lowest goes with highest, which is surely a recipe for confusion. There are various representations, such as tables and Venn diagrams, to help students do this, but none of them seems as straightforward as using the Euclidean Algorithm. So, why not just teach the Euclidean Algorithm method for finding the HCF, and then the LCM can be obtained in one simple step from this?

Notes

1. For mysterious historical reasons, in the UK (at least in schools), we tend to say 'highest common factor' (HCF), rather than 'greatest common divisor' (GCD), which seems to be the norm elsewhere.
2. Throughout this article, I assume that all numbers are positive integers (see Foster, 2022).
3. 'Lowest common multiple' (LCM) is elsewhere known as 'least common multiple'.
4. The LCM of *three* numbers is slightly more problematic. The easiest approach would be to treat it in two steps, as
$$\text{LCM}(a, b, c) = \text{LCM}(a, \text{LCM}(b, c)).$$
This would be much simpler than using the complicated formula:
$$LCM(a, b, c) = \frac{abc\ HCF(a, b, c)}{HCF(a, b)HCF(b, c)HCF(a, c)},$$
where the numerator is not at all straight-forward to see (see Foster, 2012).

References

Foster, C. (2022, November 24). 'Fractions as factors' [blogpost]. https//:blog.foster77.co.uk/2022/10/fractions-as-factors.html

Foster, C. (2012). 'HCF and LCM – Beyond procedures', *Mathematics in School,* 41(3), pp. 30–32.

Fry, H. (2018). *Hello world: How to be human in the age of the machine*. Transworld Digital.

Morgan, J. (2019). *A Compendium of Mathematical Methods: A handbook for School Teachers*. John Catt Educational Ltd.

Neale, V. (n.d.). *A Visualisation in Number Theory* [video]. www.lboro.ac.uk/services/lumen/professional-development/visualisation-in-number-theory/

Keywords: Euclidean Algorithm, Greatest common divisor, Highest common factor, Lowest common multiple, Prime factorisation.

Author: Colin Foster, Department of Mathematics Education, Schofield Building, Loughborough University, Loughborough LE11 3TU.

Email: **c@foster77.co.uk**

website: **www.foster77.co.uk**

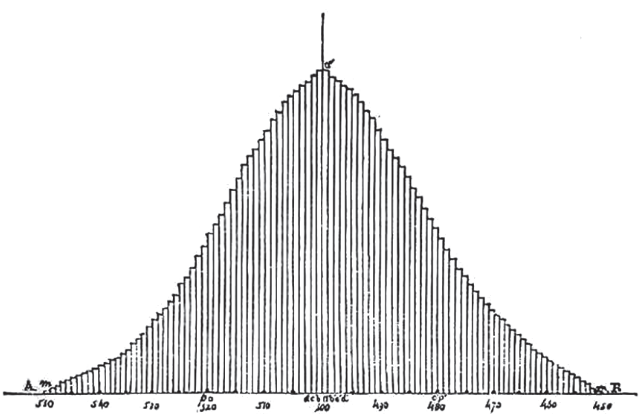
blog: **https://blog.foster77.co.uk/**

Great Mathematical Figures from Great Mathematical Figures

Quetelet's Normal 'Curve'

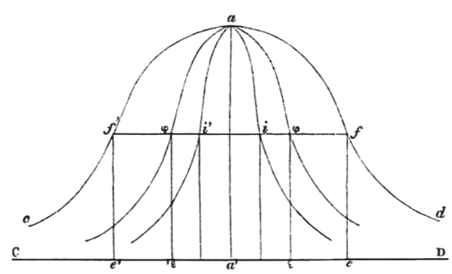
By **Chris Pritchard**

In the early history of statistics there are few more influential men than Adolphe Quetelet (1796–1874), whose data sets on the chest girths of Scots militiamen and the heights of French conscripts were used to establish the 'law of frequency of error' (later the normal distribution) as a model of the variability in human physical dimensions. It would pave the way for the work of Francis Galton and others in the second half of the nineteenth century.



But Quetelet would not have reached this point without taking the earlier step of recognising the normal curve as the limiting form of the binomial. Now this in itself was not new in the mid-1840s because Abraham de Moivre had already made use of Stirling's formula to give the result without recourse to a diagram in a pamphlet of 1733, and Christian Kramp (1760–1826) had produced tables of the normal integral in 1799 in relation to his optical researches. Quetelet produced the figure above to depict for the first time the binomial distribution behaving like the normal, asymptotically, i.e. for a large number of trials.

It appeared in *Lettres ... sur la Théorie des Probabilités*, published in 1846, though the arguments had been rehearsed in a monograph two years earlier. Quetelet considered making 999 draws from an urn holding a vast number of white and black balls in equal proportions. The probabilities were given in a table beginning with the most likely result of 499 white and 500 black balls and finishing with 420 whites and 579 blacks. These results were displayed in a diagram of a symmetric binomial distribution, with its 'ligne brisée' (broken line), but also generalised to give a continuous 'courbe de possibilité'.



Born in Ghent, Quetelet established a significant reputation as an astronomer and founded the Brussels Observatory, but in applying the normal curve to human dimensions he also founded the science of anthropometry.

Keywords: Quetelet; Binomial distribution; Normal curve

Author: Dr Chris Pritchard, contact details on p1.