Computing GCD/GCF and LCM

Terminology:

Greatest Common Divisor (gcd), Greatest Common Factor (gcf) and Highest Common Factor (hcf) are all synonymous . The term Greatest Common Factor (gcf) seems to be universally used in high school text books, but no were else. The term Greatest Common Divisor (gcd) is universally used throughout the math community and, therefore, is the term used in this article.

Greatest Common Divisor (GCD)

As the name suggests, this mathematical operation determines the largest number that evenly divides two or more numbers.

There are three main methods of computing the gcd, only two of which are taught in high school and the one actually used in practice. If these methods are not clearly and properly taught, I find that students become terribly confused by something that is really quite simple. Therefore, this article clearly and properly covers all three methods, with worked examples, pros, and cons.

Complete factorization method

This method requires the input values to be factored into all of their factors, as shown in the example below. This usually requires a trial division by every possible whole number. Note that each division creates two factors. Therefore, the list of factors is constructed from both ends, towards the middle, ending near the square root of the starting value.

Factors of 462: 1, 2, 3, 6, 7, 11, 14, **21**, 22, 33, 42, 66, 77, 154, 231, 462

Factors of 1071: 1, 3, 7, 9, 17, **21**, 51, 63, 119, 153, 357, *1071*

1, Any factors of the larger number greater than the smaller number can be ignored.

2, Starting at the right (greatest) and working toward the left, locate the first (divisor) that appears in both (common) lists.

$$\gcd(1071, 462) = 21$$

Pros: It clearly establishes the concept of what greatest common divisor (gcd) means mathematically.

It scales easily to simultaneous gcd of more than two variables.

Cons: It is practical only for small numbers and can “computationally infeasible” for larger numbers.

Prime factorization method

The fundamental theory of numbers, stated below, is the basis of this method.

All integers, greater than 2, can be expressed as the **product of powers of prime numbers**.

This method requires the input values to be factored into all of their prime factors, as shown in the example below. This usually requires a trial division by every prime number. (If a prime number is not a factor, it can be optionally represented as the prime to the power of zero, since anything to the power of zero is equal to 1.)

$$462 = 2^1 x 3^1 x 7^1 x 11^1$$

$$1071 = 3^2 x 7^1 x 17^1$$

The gcd is computed by selecting the smaller exponent of each corresponding prime factor. If the prime is not a factor, the exponent is zero.

$$gcd\,(1071, 462) = 3^1 x 7^1 = 21$$

Pros: It clearly establishes a useful concept of number theory, reinforcing the concept of what greatest common divisor (gcd) means mathematically.

It scales easily to simultaneous gcd of more than two variables.

Cons: It is practical only for small numbers and can "computationally infeasible" for larger numbers.

Euclidean Algorithm method

This algorithm was first published in the year 300 BC by the Greek mathematician Euclid in volume 7 of his 10 volume text given the named ELEMENTS. Wikipedia provides an exceptionally good explanation of Euclid's algorithm: https://en.wikipedia.org/wiki/Euclidean_algorithm. It is also covered in many math texts.

The main difference between Euclid's original algorithm and what we use today is that Euclid used repeated subtractions, whereas, we use standard division. We use only the remainder of the divisions, not the quotient. Therefore, we describe modular reduction, abbreviated "mod" as follows:

X mod Y = the remainder of Y divided by X.

Note that there are other gcd algorithms and there is also an extended Euclidean algorithm, which is used to compute Bezout coefficients and modular multiplicative inverses. These are beyond the scope of this article.

The following table presents an example of the Euclidean algorithm which uses a simple step that repeats until the smaller number is zero. The larger number is then the gcd. Note that the forth column, X/Y is not necessary, but is included in this example for understanding.

Iteration	**X** **Previous Y**	**Y** **X mod Y**	**X/Y**
0	1071	462	2 R 147
1	462	147	3 R 21
2	147	21	7 R 0
3	**21**	0	

Another example, where gcd(123456, 789) = 3:

Iteration	X Previous Y	Y X mod Y	X/Y
0	123456	789	156 R 372
1	789	372	2 R 45
2	372	45	8 R 12
3	45	12	3 R 9
4	12	9	1 R 3
4	9	3	3 R 0
5	**3**	0	

To demonstrate how simple the Euclidean Algorithm is, the following is an excerpt from a software program used professionally for this computation. This computer language uses the "mod(X, Y)" function to perform the "X mod Y" operation. There are also some special cases and negative number handling that are not shown here.

```
while Y:
   X, Y = Y, mod(X, Y)
return X
```

Pros: It is very computationally infeasible and efficient, even for very large numbers. Cryptographers use this algorithm with numbers of 1,200 decimal digits in length!

Cons: It does not help in understanding the concept of what greatest common divisor (gcd) means mathematically, leaving that to the above methods.

It can be used for only two numbers at a time, but supports more than two numbers by doing pair-wise computations, as follows:

$$\gcd(a, b, c, d) = \gcd(\gcd(a, b), \gcd(c, d))$$

Least Common Multiple (LCM)

As the name suggests, this mathematical operation determines the smallest number that is a multiple of two or more numbers. Stated in another way, the lcm is the smallest number that can be evenly divided by those numbers

There are two methods of computing the lcm, which are related to the prime factorization and Euclidean algorithm methods of computing the gcd. They have the same pros and cons as the gcd methods described above.

Prime factorization method

This method requires the input values to be factored into all of their prime factors, as shown in the example gcd above.

$$462 = 2^1 x 3^1 x 7^1 x 11^1$$

$$1071 = 3^2 x\, 7^1 x\, 17^1$$

The lcm is computed by selecting the larger of the exponents of each corresponding prime.

$$lcm(1071, 462) = 2^1 x\, 3^2 x\, 7^1 x\, 11^1 x\, 1^1 = 23{,}562$$

The pros and cons of this method are the same as those of using this method to compute the gcd.

GCD-based method

Since we have an efficient algorithm for finding the gcd, we need an efficient way to find the lcm. The hint on how to do this lies in the table below.

Mathematical Operation	**Action on Corresponding Exponents of Primes**
Multiplication	Addition
Division	Subtraction
Greatest Common Divisor	Select lowest
Least Common Multiple	Select highest

If we combine the exponents of each corresponding prime (multiplication), then select the smaller exponent (gcd), and subtract (divide) out the smaller exponent (gcd), the following is true. Since the gcd evenly divides both of the original numbers, a small performance improvement can be obtained by doing the division first followed by the multiplication, as shown.

$$lcm(A, B)\, x\, gcd(A, B) = A\, x\, B$$

results in:

$$lcm(A, B) = \frac{A\, x\, B}{gcd(A, B)} = \frac{A}{gcd(A, B)}\, x\, B$$

Therefore:

$$lcm, (1071, 462) = \frac{1071\, x\, 462}{21} = \frac{1071}{21}\, x\, 462 = 23{,}562$$

Applications

Coprime or relatively prime

The term “coprime” or “relatively prime” refers to the case when numbers share no common prime factors, greater than one. Expressed as gcd(X, Y) =1 The numbers 4 and 9 are relatively prime to each other and share no common prime factors, even though neither 4 nor 9 are primes.

Adding fractions

Back in elementary school, we all learned how to add fractions by finding the “least common denominator,” which is simply the least common multiple, used as a denominator.