GCD and LCM and Euclidean Algorithm

Aarushi Mehrotra

July 11th, 2022

Contents

1 Introduction

In the topic of Number Theory, any set of two or more integers always have a key property called the **greatest common divisor**, and **least common multiple**.

Definition 1.1 (Greatest Common Divisor)

The **greatest common divisor (or greatest common factor)** of two or more integers is the greatest integer that divides each of the numbers leaving a remainder of 0.

Definition 1.2 (Least Common Multiple)
The **least common multiple** of two or more integers is the least integer that leaves a remainder of 0 when divided by each of the numbers.

The GCD can be thought of as the intersection of two or more numbers and the LCM as the union. For example, the two numbers 8 and 12 have the following factors and multiples:

$$8 : 1, 2, \boxed{4}, \mathbf{8}, 16, \textcircled{24}, 32, \ldots$$
$$12 : 1, 2, 3, \boxed{4}, 6, \mathbf{12}, \textcircled{24}, 36, \ldots$$

From these lists, we can see that the GCD is 4 because it is the greatest factor that exists in both lists, and the LCM is 24 because it is the least multiple that exists in both lists.

Example 1.1
Find the GCD of 51 and 85.

Solution. The factors of 51 are:

$$1, 3, \textcircled{17}, 51$$

and the factors of 85 are

$$1, 5, \textcircled{17}, 85$$

so the GCD of 51 and 85 is 17. †

Example 1.2
Find the LCM of 26 and 39.

Solution. The first few multiples of 26 are:

$$26, 52, \textcircled{78}, 104$$

and the first few multiples of 85 are

$$39, \textcircled{78}, 117, 156$$

so the LCM of 26 and 39 is 78. †

However, listing out the factors and multiples of each number is tedious, so we turn to another method: prime factors.

2 Prime Factorization

Since we want to find the greatest factor that divides each number, each number must contain the prime factorization of the common factor. Using the same example of 8 and 12, their respective prime factorizations are:

$$8 = 2^3$$

$$12 = 2^2 \cdot 3$$

Definition 2.1

The prime factorization of a number is expressing the number as the product of its prime factors to their respective exponents.

We know that the GCD of 8 and 12 is 4, or 2^2. Looking at the prime factorizations of 8 and 12, they do not share a factor of 3, so the largest factor of 2 that they share is 2^2. Finding the LCM is a similar process, their LCM, 24, has a prime factorization of $= 2^3 \cdot 3$. The LCM is the smallest number that contains both the prime factorization of 8 and 12, so it gets 2^3 from 8 and 3 from 12.

Example 2.1

Using the prime factorization method, find the LCM and GCD of 189 and 91.

Solution. $189 = 3^3 \cdot 7$ and $91 = 13 \cdot 7$ so the GCD of 189 and 91 is 7 and the LCM of 189 and 91 is $3^3 \cdot 13 \cdot 7 = 2457$. †

3 The Formula and Interesting Observations

Since the GCD is the intersection of two or more numbers, it is the factor that is in all of the numbers. Using our example of 8 and 12, the only factor in both of these numbers is 2^2. Given two numbers $a = p_0^{e_0} \cdot p_1^{e_1} \cdot p_2^{e_2} \cdots p_m^{e_m}$ and $b = p_0^{f_0} \cdot p_1^{f_1} \cdot p_2^{f_2} \cdots p_m^{f_m}$, where p_i is a prime factor of a and b, with respective exponents e_i and f_i, we can say that

$$\gcd(a,b) = p_0^{\min(e_0,f_0)} \cdot p_1^{\min(e_1,f_1)} \cdot p_2^{\min(e_2,f_2)} \cdots p_m^{\min(e_m,f_m)}.$$

Since the LCM is the union of both numbers, the larger power for each prime factor must be chosen:

$$\operatorname{lcm}(a,b) = p_0^{\max(e_0,f_0)} \cdot p_1^{\max(e_1,f_1)} \cdot p_2^{\max(e_2,f_2)} \cdots p_m^{\max(e_m,f_m)}.$$

Once we take a close look at the GCD and LCM, we can see that if we multiply the GCD and LCM, we get

$$p_0^{\max(e_0,f_0)\cdot\min(e_0,f_0)} \cdot p_1^{\max(e_1,f_1)\cdot\min(e_1,f_1)} \cdots p_m^{\max(e_m,f_m)\cdot\min(e_m,f_m)}.$$

Since for e_i and f_i, both must be factors of $\max(e_i, f_i) \cdot \min(e_i, f_i)$, so $ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$.

Example 3.1

Find $\gcd(10,18)$ and $\operatorname{lcm}(10,18)$.

Solution. We know that $10 = 2 \cdot 5$ and $18 = 2 \cdot 3^2$, so the GCD of 10 and 18 is 2. The LCM is $2 \cdot 5 \cdot 3^2$, we can see this by taking the union of 10 and 18. Now we can see that $2 \cdot 5 \cdot 3^2(\cdot 2) = 10 \cdot 18$.

Is it more clear why $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$? However this rule does **not** work for any more than 2 numbers, as we show with 3.2. †

Example 3.2

Given three numbers a, b, and c, show why

$$\gcd(a,b,c) \cdot \operatorname{lcm}(a,b,c) \neq a \cdot b \cdot c.$$

Solution. Let's try an example by substituting in three numbers for a, b, and c. We plug in $15, 20, 35$ for a, b, and c, respectively.

$$\gcd(a, b, c) = 5 \text{ and } \operatorname{lcm}(a, b, c) = 420$$

$$420 \cdot 5 = 1200 \text{ and } abc = 10500,$$

which are clearly not equal.

Let's now prove this using algebraic terms. Let's call the GCD of a, b, and c g and the quotient of a, b, and c divided by g a_1, b_1, and c_1, respectively.

If we multiply the GCD by the LCM, we get:

$$(g) \cdot (a_1 \cdot b_1 \cdot c_1),$$

which is not equal to abc, unless $\gcd(a, b, c) = 1$.

†

4 Euclidean Algorithm

Definition 4.1

The Euclidean Algorithm is a very efficient way to compute the GCD of two numbers, which also allows us to find the LCM.

The Euclidean algorithm works based off of the statement that the GCD of two numbers is also the GCD of the difference of those two numbers. We can see that this is true: given two numbers $a = kx$ and $b = ky$, where $x > y$, which have GCD k:

$$\gcd(a, b) = \gcd(kx, ky) = \gcd(ky, k(x - y))...$$

We repeat this series of operations until it results in $\gcd(k, 0)$ which is k.

Example 4.1

Find the following values using the Euclidean Algorithm

i. $\gcd(18, 10)$

ii. $\gcd(147, 91)$

Solution.

i. $\gcd(18, 10) = \gcd(10, 8) = \gcd(8, 2) = \gcd(2, 2) = \gcd(2, 0) = 2$.

ii. $\gcd(147, 91) = \gcd(91, 56) = \gcd(56, 35) = \gcd(35, 21) = \gcd(21, 14) = \gcd(14, 7) = \gcd(7, 0) = 7$.

†

Theorem 4.1

From the work in Example 4.1, we can see that:
$\gcd(x, 1) = 1$ and
$\gcd(x, ax) = x$

5 Practice Problems

Exercise 5.1. (AMC 8 2013) What is the ratio of the least common multiple of 180 and 594 to the greatest common factor of 180 and 594?

Exercise 5.2. (AMC 10B 2018) How many ordered pairs (a, b) of positive integers satisfy the equation

$$a \cdot b + 63 = 20 \cdot \text{lcm}(a, b) + 12 \cdot \gcd(a, b)?$$

Exercise 5.3. (AIME 1987) Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples (a, b, c) of positive integers for which $[a, b] = 1000$, $[b, c] = 2000$, and $[c, a] = 2000$.

Exercise 5.4. (AIME 1985) The numbers in the sequence 101, 104, 109, 116,... are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$ For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

Exercise 5.5. (AMC 10A 2018) Let a, b, c, and d be positive integers such that $\gcd(a, b) = 24$, $\gcd(b, c) = 36$, $\gcd(c, d) = 54$, and $70 < \gcd(d, a) < 100$. Which of the following must be a divisor of a?