GCD and LCM

Tony Lu

July 22, 2021

Contents

1 Introduction

Two very important functions in number theory are the GCD function and the LCM function. These two functions work with the prime factorization of numbers and help us manipulate numbers in interesting ways.

A few notes on the structure of this handout: we will begin with a purely theoretical section, first outlining the definitions of GCD and LCM and how we use them in contests and the Euclidean Algorithm. We will finish with a section consisting of example problems and walkthroughs. The reader is encouraged to do all the examples before reading the solution.

2 Basic Definitions and Examples

You should know the definitions of GCD and LCM already, but we restate them here for completeness.

Greatest Common Divisor
The *Greatest Common Divisor*, abbreviated *GCD*, of two positive integers a, b is the greatest positive integer n such that n is both a factor of a and b.

Least Common Multiple
The *Least Common Multiple*, abbreviated *LCM*, of two positive integers a, b is the least positive integer n such that n is both a multiple of a and b.

This is all terrific, but given two numbers, how do we even compute their GCD or LCM? We can use the following proposition to compute the GCD or LCM.

Proposition 2.1 (Alternative GCD/LCM Definition)
For any two positive integers $x = a_1^{m_1} a_2^{m_2} a_3^{m_3} \cdots a_n^{m_n}$ and $y = b_1^{n_1} b_2^{m_2} b_3^{m_3} \cdots b_n^{m_n}$ for a_i, b_i prime, their GCD is given by

$$\gcd(x, y) = \prod_{p_i \in \{a_1, a_2, a_3, \cdots, a_n\} \cap \{b_1, b_2, b_3, \cdots, b_n\}} p_i^{\min(m_i, n_i)},$$

and their LCM is given by

$$\operatorname{lcm}(x, y) = \prod_{p_i \in \{a_1, a_2, a_3, \cdots, a_n\} \cup \{b_1, b_2, b_3, \cdots, b_n\}} p_i^{\max(m_i, n_i)}.$$

This may seem complicated, but this comes naturally from our original definition of GCD and LCM. Notice that for any prime p that divides both x, y, its smaller exponent among x, y will divide both numbers (and is the largest exponent of p that does so.) Then we can multiply through all primes p by dividing at least one of x, y. To illustrate this, let's look at an example:

Example 2.2
Find the GCD and LCM of 1536 and 1764.

Solution. First we factor the two integers:

$$1536 = 2^9 \cdot 3$$
$$1764 = 2^2 \cdot 3^2 \cdot 7^2.$$

We can look at each prime factor separately. For example, for the prime factor 2 which is common to both numbers, we take the smaller exponent (i.e. 2). The prime factor 3 is also common to both numbers, and the smaller exponent is 1. Therefore, their GCD is just $2^2 \cdot 3 = 12$.

To find their LCM, we can use a similar technique; this time, the prime factor 2 we take to the larger exponent (9), the prime factor 3 we take to the exponent 2, while the prime factor 7 we also take to the exponent 2. Therefore, their LCM is then

$$2^9 \cdot 3^2 \cdot 7^2 = 225792.$$

It's that simple! □

Notice that our GCD and LCM definition can also be generalized to multiple variables – the proof is identical to the two-variable case.

Before moving on, we also introduce a bit of terminology.

Relatively Prime

Two integers a, b are known as ***relatively prime*** if and only if $\gcd(a, b) = 1$. In particular, every positive integer is relatively prime to 1.

It turns out that two integers are also relatively prime if and only if they share no common prime factors.

Suppose m, n are relative prime integers. By the definition of relatively prime, no prime number can divide both m, n, so if the prime factorizations are

$$\prod_{i=1}^{\infty} p_i^{m_i} \text{ and } \prod_{i=1}^{\infty} p_i^{n_i}$$

respectively, then one of m_i, n_i is 0 for each i. Actually, it turns out that this is sufficient, since

$$\gcd(m, n) = \prod_{i=1}^{\infty} p_i^{\min(m_i, n_i)} = \prod_{i=1}^{\infty} p_i^0 = 1.$$

Exercise 2.3. Prove Proposition 2.1.

Exercise 2.4. What is the GCD and LCM of 2016 and 1728?

Exercise 2.5. What is the GCD and LCM of 256 and 773?

2.1 GCD and LCM Properties

Evaluate the product of the GCD and LCM of say, 12 and 20. Does this number look familiar? Indeed, this is just the product of 12 and 20! We can state this in a more general way as follows:

Theorem 2.6
For any two positive integers a, b,

$$\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab.$$

Proof. Follows easily from the original definition of GCD and LCM. Just notice that $\min(x,y) + \max(x,y) = x + y$. □

There is also a nice property of GCD and LCM that is very obvious but useful in some problems:

Proposition 2.7 (Factoring)
For any two positive integers a, b and for some $k \mid a, b$, we have

$$\gcd(a,b) = k \gcd\left(\frac{a}{k}, \frac{b}{k}\right).$$

Again, the proof is very simple and left as an exercise to the reader.

Using this method, we can simplify many GCD calculations by "extracting" obvious factors, as shown below:

Example 2.8
Find all positive integers k such that there exists at least one positive integer n satisfying

$$\gcd(3n^3 - 8n^2 + 3n + 2, 3n^3 - 7n^2 + 4) = k.$$

Solution. At first we're unsure how to approach this problem. First, we are motivated to factor the two polynomials that we are given, which might give us something useful:

$$3n^3 - 8n^2 + 3n + 2 = (3n+1)(n-1)(n-2),$$

while

$$3n^3 - 7n^2 + 4 = (3n+2)(n-1)(n-2).$$

Then, we have that the GCD just equals

$$\gcd((3n+1)(n-1)(n-2), (3n+2)(n-1)(n-2)).$$

Using Proposition 2.7, this can be rewritten as

$$(n-1)(n-2)\gcd(3n+1, 3n+2) = (n-1)(n-2),$$

because $\gcd(3n+1, 3n+2)$ equals 1 for all positive integers n! Therefore, the positive integer $k = \boxed{(n-1)(n-2)}$ for some positive integer n. □

There was a small observation that we noted in this problem that is also useful in some cases; we state it below.

Fact 2.9. Two consecutive numbers are always relatively prime.

Exercise 2.10. How many ordered pairs (m, n) with $1 \le m, n \le 100$ are there such that $\gcd(m, n) = 5$?

We finish this section off with an application of Theorem 2.6.

Example 2.11
Find all pairs of positive integers (m, n) such that the LCM of m and n is exactly three times the GCD of m and n.

Solution. Rewrite the condition as

$$\operatorname{lcm}(m, n) = 3\gcd(m, n).$$

This is the kind of situation where Theorem 2.6 is helpful; we can get rid of the lcm using it, yielding

$$\frac{mn}{\gcd(m, n)} = 3\gcd(m, n) \implies 3\gcd(m, n)^2 = mn.$$

Now what next? In many problems where you have a multiplicative GCD expression like this, it often helps considering prime factors separately! This turns our "multiplication" into addition due to exponent rules.

Therefore, say we have some prime factor p of $\gcd(m, n)$. Say it seems p_m times in m and p_n times in n. Then, it seems $p_m + p_n$ times in mn (see how we were talking about turning multiplication into addition earlier?). In particular, if p is not 3, then it also appears $\min(p_m, p_n)$ times in the GCD.

Thus, we have the equation

$$2\min(p_m, p_n) = p_m + p_n$$

since the GCD is squared. It is easy to see by inspection that we must have $p_m = p_n$ in this case! This is a lot of progress – now we only have to look at the prime factor $p = 3$.

Say that 3 appears a times in m and b times in n. Then, it appears $a + b$ times in $m + n$ and $2\min(a, b) + 1$ times in the other side. Then

$$2\min(a, b) + 1 = a + b.$$

WLOG set $a \le b$; then

$$2a + 1 = a + b \implies b - a = 1.$$

Now we're done! We can sum up our restrictions as follows: we must have

1. $v_p(m) = v_p(n)$ for all $p \neq 3$;
2. $|v_3(m) - v_3(n)| = 1$.

(If you haven't seen it before, $v_p(n)$ is the several times the prime factor p appears in the prime factorization of n. We are in a way adopting this notation prematurely because v notation is usually used in ***Lifting the Exponent***, which is altogether a different topic than this handout!) □

Exercise 2.12. Generalize the above example to arbitrary constants. In particular, if

$$\operatorname{lcm}(m,n) = k\gcd(m,n)$$

for some constant k, what does this imply about m, n?

3 The Euclidean Algorithm

In this section, we introduce a powerful tool for working with the GCD – The Euclidean Algorithm. We present it directly:

Proposition 3.1 (Euclidean Algorithm)
For any positive integers m, n,

$$\gcd(m,n) = \gcd(m,|m-n|) = \gcd(n,|m-n|).$$

Proof. WLOG $m > n$. Then say some prime p divides both m and n, so let $m = pm'$ and $n = pn'$ for positive integers m', n'. But we have

$$p \mid p(m'-n') \implies p \mid m-n,$$

which means that any prime factor that divides both m, n divides $m-n$. Next we show that we cannot have $\gcd(m,m-n) > \gcd(m,n)$. This is trivial, because we have $\gcd(m,m-n) \mid m$ by Proposition 2.7. Assume that $p = \gcd(m,n)$; however, m' and n' are relatively prime, which means that m' and n' contains no prime factors in m or n. Hence, we must have

$$\gcd(m,m-n) = p \implies \gcd(m,m-n) = \gcd(m,n).$$

The case for n is similar. □

Now, why do we call this an "algorithm"? How is it even useful to solve number theory problems? Consider the following example.

Example 3.2
Find the GCD of 169344 and 169792.

Solution. Factoring these two numbers would be needlessly bashy. However, by Proposition 3.1, we do have

$$\gcd(169344, 169792) = \gcd(169344, 169792 - 169344) = \gcd(169334, 448).$$

What next? Well, we can *repeatedly* apply the Euclidean Algorithm on 169334 and 448:

$$\gcd(169334, 448) = \gcd(169334 - 448, 448) = \gcd(169334 - 2 \cdot 448, 448) = \cdots,$$

– we can subtract any number of multiples of 448 that we want! In particular, let's see specifically how many multiples we can subtract. We have $\frac{169344}{448} = 378$ – oh wait, this is an integer! Therefore, since 169334 is a multiple of 448, the GCD must be $\boxed{448}$. □

In this problem, we found a generalized version of the Euclidean Algorithm:

Theorem 3.3 (Genearlized Euclidean Algorithm)
For any positive integers m, n,

$$\gcd(m, n) = \gcd(m, m - kn)$$

for any integer constant k.

Exercise 3.4. Prove Theorem 3.3 in a similar way that we proved Proposition 3.1.

Exercise 3.5. Find the GCD of 10944 and 11520 using the Euclidean Algorithm.

Exercise 3.6. Find the GCD of 2587 and 3184 using the Euclidean Algorithm.

Exercise 3.7. Find the LCM of 2750 and 3250 using the Euclidean Algorithm. **Hints**: 18

Now, don't think that the Euclidean Algorithm is just practical as a shortcut for evaluating numerical GCD's – it is much more powerful. The key is that we can also use it for arbitrary variables, unlike our original definition or observations of GCD. Let's look at an example of how this is useful.

Example 3.8
For any positive integer $n \geq 2$, show that $n^2 - 3$ and $n + 2$ are always relatively prime.

Proof. The problem simply wants us to show that

$$\gcd(n^2 - 3, n + 2) = 1.$$

Let's apply Theorem 3.3! First of all, $n^2 - 5$ looks like a difference of squares – indeed, we can write $n^2 - 3 = (n + 2)(n - 2) + 1$. Therefore, we can write

$$\gcd(n^2 - 3, n + 2) = \gcd(n + 2, n^2 - 3 - (n - 2)(n + 2)) = \gcd(n + 2, 1) = 1.$$

This finishes the problem. □

Some commentary: Indeed, in this problem, the Euclidean Algorithm was just really an extension of your common sense – since $n^2 - 4$ is a multiple of $n + 2$, $n^2 - 3$ clearly can't share any prime factors with $n + 2$. Indeed, the Euclidean Algorithm is just your divisibility intuition, stated algebraically! Nonetheless, it is handy in a wide variety of problems. You'll get to see much more of these algebraic applications in the next section.

4 A Few Examples

In this next section, we will cover the applications of GCD and LCM in contest problems. I have noticed that many problems in contests using these topics also invoke the Euclidean Algorithm; we will provide a few examples of these uses below.

We begin with a relatively famous problem that demonstrates a conventional application of the Euclidean Algorithm.

Example 4.1 (1959 IMO/1)
Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n.

Proof. First of all, we should rephrase the "irreducible" condition in terms of GCD's. We just need to show that

$$\gcd(21n+4, 14n+3) = 1$$

for all natural numbers n. Now, as we learned in the previous section, we can use the Euclidean Algorithm with variables:

$$\begin{aligned}\gcd(21n+4, 14n+3) &= \gcd(14n+3, 21n+4-14n-3) = \gcd(14n+3, 7n+1) \\ &= \gcd(7n+1, 14n+3-7n-1) = \gcd(7n-1, 7n-2) = 1\end{aligned}$$

because of Fact 2.9. Alternatively, we could apply the algorithm again to get

$$\gcd(7n-1, 7n-2) = \gcd(1, 7n-1) = 1,$$

which finishes the problem. □

Next, we present a more complicated problem using the same ideas regarding the Euclidean Algorithm.

Example 4.2 (1986 AIME/5)
What is that largest positive integer n for which $n^3 + 100$ is divisible by $n + 10$?

At first, we don't see anything in this problem that relates to GCDs or LCMs. So how could we apply the concepts that we've learned before here? Recall by Proposition 2.? that we can rewrite the given condition $n + 10 \mid n^3 + 100$ as

$$\gcd(n^3 + 100, n + 10) = n + 10.$$

Now, we can use the Euclidean Algorithm as we did before!

Solution. The problem is equivalent to finding the greatest n such that

$$\gcd(n^3 + 100, n + 10) = n + 10.$$

Before we blindly start applying the Euclidean algorithm, $n^3 + 100$ looks quite familiar. It is *almost* a sum of cubes; in particular, we can write

$$n^3 + 100 = n^3 + 1000 - 900.$$

However, we know by the sum of cubes factorization that $n + 10 \mid n^3 + 1000$! This allows us to skip a lot of tedious steps in the Euclidean Algorithm.

Hence, we can write

$$\begin{aligned}\gcd(n^3 + 100, n + 10) &= \gcd((n+10)(n^2 + 10n + 100) - 900, n + 10) \\ &= \gcd(-900, n + 10) = \gcd(900, n + 10)\end{aligned}$$

after we subtract $n^2 + 10n + 100$ times the second term $n + 10$ from the first term $n^3 + 100$.

Now, we need the largest integer n such that $n + 10$ is a factor of 900. The largest such n is clearly $\boxed{890}$. □

Remark 4.3. Notice that in the end, we didn't directly use the concept of "GCD", only the concept of divisibility. However, our Euclidean Algorithm manipulations with the GCD also apply to divisibility problems like this one. This just goes to show that ***intuition behind Euclidean Algorithm manipulations is more important than knowing how to use the algorithm!***

Next, we formalize a piece of "intuition" regarding when to use the Euclidean Algorithm in the upcoming problem.

Example 4.4 (1995 AIME/8)
For how many ordered pairs of positive integers (x, y), with $y < x \leq 100$, are both $\frac{x}{y}$ and $\frac{x+1}{y+1}$ integers?

How are the concepts of the Euclidean Algorithm correlated to this problem? Well, to count all the pairs of positive integers (x, y), we want only one restriction on x, y. That makes it easy to sum over the possible values of x and see which possible values of y satisfy the condition for some x. Unfortunately, the problem has two conditions that we can't link together directly.

Solution. Let's write the two given conditions as GCD's. We can write $\gcd(x, y) = y$ and $\gcd(x+1, y+1) = y+1$ are equivalent to the given conditions, because $y < x$. Now we want to manipulate this expression in some way such that we obtain two restrictions on ***one term.*** Thinking about creating equal terms in the gcd expressions, we observe

$$x - y = (x+1) - (y+1).$$

Therefore, using the Euclidean Algorithm, the two conditions can be rewritten as

$$\gcd(x-y, y) = y \text{ and } \gcd(x-y, y+1) = y+1.$$

This attains our goal of creating only one restriction; the two conditions are then equivalent to

$$y \mid x-y, y+1 \mid x-y \implies y(y+1) \mid x-y.$$

Now the possible (x, y) are easy to count; notice that we only have to consider $y \leq 9$, since after that $y(y+1) > 100 > x - y$. It follows that there are $\left\lfloor \frac{100-y}{y(y+1)} \right\rfloor$ values of x for each y. (Why?) Summing over $y = 1$ to 9, we obtain

$$\sum_{y=1}^{9} \left\lfloor \frac{100-y}{y(y+1)} \right\rfloor = 49 + 16 + 8 + 4 + 3 + 2 + 1 + 1 + 1 = \boxed{85}$$

such pairs (x, y) exist. □

Collapsing many different restrictions into one restriction on a term is commonly fruitful for problems asking you to count the number of ordered pairs satisfying conditions $a_1, a_2, \cdots, a_n$.

In the next problem, we shift gears a bit, instead of looking at how we can integrate LCM and GCD definitions into counting problems.

Example 4.5 (1987 AIME/8)
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 $[c,a] = 2000$.

Solution. First as with any number theory problem, we factor the numbers given:

$$1000 = 2^3 \cdot 5^3$$
$$2000 = 2^4 \cdot 5^3.$$

From this, we immediately find that 2 and 5 are the only prime factors of a, b, c. Thus we can let

$$a = 2^{x_1} \cdot 5^{y_1}$$
$$b = 2^{x_2} \cdot 5^{y_2}$$
$$c = 2^{x_3} \cdot 5^{y_3}.$$

Then by the definition of LCM, we then have

$$\max(x_1, x_2) = 3, \max(x_1, x_3) = 4, \max(x_2, x_3) = 4.$$

At this point, we could use some logic. We must have $x_3 = 4$, since otherwise both of x_1, x_2 must be 4 which is impossible.

Now, we simply need one of x_1, x_2 to be 3. To count the possibilities is simple casework; if one of x_1, x_2 is 3, then we have 2 ways to choose the $x_i = 3$ and 3 ways to choose the other x_i; if they were both 3, we have 1 extra way. This gives 7 ways to choose the x_i.

We can repeat for the y_i. This time, two or more of the y_i must be 3 (why?). If exactly two are 3, there are $\binom{3}{2} \cdot 3 = 9$ ways to choose the y_i; there is 1 way when they are all 3. Adding these gives us 10 ways to choose the y_i.

Finally, since choosing the x_i and y_i are independent, there are $10 \cdot 7 = \boxed{70}$ such ordered triples. □

Some commentary: the above problem was arguably more combinatorics-weighted than number theory weighted. However, to solve many problems like this, you will need a deep fundamental intuition about how LCM and GCD behave – especially important to note is that ***when we take the LCM or GCD, we can regard the prime factors independently from each other.*** It seems obvious, but it's very important! You'll see a similar problem in the problem set.

Example 4.6 (2016 PUMaC NT A5)
Let $K = 2^6 \cdot 3^5 \cdot 5^2 \cdot 7^3 \cdot 53$. Let S be the sum of $\frac{\gcd(m,n)}{\text{lcm}(m,n)}$ over all ordered pairs of positive integers (m,n) where $mn = K$. If S can be written in simplest form as $\frac{r}{s}$, compute $r+s$.

Solution. What makes this expression hard to sum is that it is very hard to handle GCD and LCM together with each other. Moreover, we have a lot of fractions, which make

evaluating directly very ugly. So how can we alter the expression? We can use the fact that

$$\text{lcm}(m,n) = \frac{mn}{\gcd(m,n)}!$$

In particular, we can write

$$\frac{\gcd(m,n)}{\text{lcm}(m,n)} = \frac{\gcd(m,n)}{\frac{K}{\gcd(m,n)}} = \frac{\gcd^2(m,n)}{K},$$

because $mn = k$ as given. Now we have a constant denominator when we sum, which is an improvement.

Okay, so how do we sum $\gcd^2(m,n)$ now? We can use an idea similar to how we sum the divisors of a positive integer – consider prime factor by prime factor! A tipoff to do this is because $\gcd(m,n)$ either takes the value of m or n; this makes it behave similar to the sum of divisors function.

> This is so important we say it again – in many number theory problems where you have to sum something, usually relating to prime factors, try splitting the sum into prime factors or considering prime factor by prime factor.

Let's try to do so in this problem. Think about some $m \mid -K$. Our first claim is

Claim — For any prime factor p of m, the exponent of p, which we will call k, satisfies

$$k \leq \frac{r}{2},$$

if r is the exponent of p in K.

This is quite easy to show; if $k > \frac{r}{2}$, then $n = \frac{K}{m}$ contains $r - k < \frac{r}{2}$ factors of p, which is a contradiction, since in this case, we would take the minimum exponent from n instead of m!

Since *any* number of the form

$$2^{2k_1}3^{2k_2}5^{2k_3}7^{2k_4}53^{2k_5}$$

can be represented that satisfies the above conditions, we can think of adding each new term as "choosing" an exponent from each prime. Since we can choose the prime factors independently, and we ultimately sum them, we can ***add the possible prime exponents for each prime***, then ***multiply the sum of these together***.

Exercise 4.7. Verify that indeed, summing like this covers every single possible factor.

For example, the possible choices of the factors of 2 are $1, 2^2, 2^4, 2^6$ (recall that we have GCD ***squared***, and otherwise all $k_i \leq 3$.)

Before we are ready to sum through, we have to consider one more subtlety. (m,n) is a *ordered* pair; therefore, there will always be ***two ways*** to assign the smallest prime

exponent to m, n unless this exponent equals exactly $\frac{r}{2}$ – in this case, the two exponents are identical, and we don't care about order. Therefore, our sum is just

$$(1+2^2+2^4+2^6+2^4+2^2+1)(1+3^2+3^4+3^4+3^2+1)(1+5^2+1)(1+7^2+7^2+1)(1+1).$$

This evaluates to $106 \cdot 182 \cdot 27 \cdot 100 \cdot 2$, so putting this over the denominator K,

$$\frac{106 \cdot 182 \cdot 27 \cdot 100 \cdot 2}{2^6 \cdot 3^5 \cdot 5^2 \cdot 7^3 \cdot 53} = \frac{2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13 \cdot 53}{2^6 \cdot 3^5 \cdot 5^2 \cdot 7^3 \cdot 53} = \frac{13}{2 \cdot 3^2 \cdot 7^2} = \frac{13}{882},$$

which yields an answer of $\boxed{895}$. □

Remark 4.8. The key idea highlighted in the past few problems is that when we sum prime factors or choose prime factors, ***we can consider all prime factors independent of each other.*** This is why we can multiply the sums of prime exponents together to create the sum of all possible terms.

5 Walkthroughs

In this section, we present some more difficult, nonconventional problems that use the concepts we have learned in interesting and insightful ways. The reader is encouraged to try the problems on their own, and write up their solution from the walkthrough steps. Complete solutions will be provided to the walkthroughs in the solutions packet.

Example 5.1 (1996 AIME/14)
A $150 \times 324 \times 375$ rectangular solid is made by gluing together $1 \times 1 \times 1$ cubes. An internal diagonal of this solid passes through the interiors of how many of the $1 \times 1 \times 1$ cubes?

At first glance, this problem looks nothing like a number theory problem. Indeed, it uses more combinatorics concepts than number theory concepts, but we nonetheless include it because it illustrates an application of the ideas of GCD and how it pops up in all sorts of problems.

Walkthrough. The key idea is that our internal diagonal enters a new cube every time it goes through a lattice plane of the x, y, or z dimensions.

1. Count the total number of cubes by considering how many times space diagonal passes into a new cube through the x, y, z dimensions, respectively. Why does this initial count overcount the cubes?
2. Find the number of times where space diagonal enters one cube through two dimensions at the same time, and where it enters one cube through three dimensions. How are GCD's involved here?
3. Use the ***Principle of Inclusion-Exclusion*** to finish.

Example 5.2 (2018 AMC 10A/22)
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?

(A) 5 **(B)** 7 **(C)** 11 **(D)** 13 **(E)** 17

Walkthrough. This problem has many different approaches in the sense that there isn't a single, totally rigorous solution – we just have to prove one case works and find contradictions to the other ones.

1. Notice that a, b, c, d must all be multiples of 6. Then, substitute $a' = \frac{a}{6}$ and similar. How should we reduce the last condition concerning this substitution?
2. Next, eliminate possible values of $\gcd(a', d')$ by looking at the factors of a.
3. You should be left with only one possible value of $\gcd(a', d')$, from where you can extract the answer.

Before we move on, a bit of commentary: it is often useful to reduce variables with gcd conditions. For example, if $\gcd(a, b) = k$ for some given k is a condition in the problem, we can substitute $a' = \frac{a}{k}$ and $b' = \frac{b}{k}$ into the problem.

Notice that this manipulation both introduces useful facts into the problem and reduces our condition; we now only need $\gcd(a', b') = 1$ which is much easier to handle.

Example 5.3 (2018 PUMaC NT A4)
Let n be a positive integer. Let $f(n)$ be the probability that, if divisors a, b, c of n are selected uniformly at random with replacement, then $\gcd(a, \text{lcm}(b, c)) = \text{lcm}(a, \gcd(b, c))$. Let $s(n)$ be the sum of the distinct prime divisors of n. If $f(n) < \frac{1}{2018}$, compute the smallest possible value of $s(n)$.

Walkthrough. This is another example of lifting the GCD and LCM conditions to minimum/maximum conditions in the exponent.

1. Consider any prime factor p, and let x, y, z be the exponents of p in a, b, c respectively. Convert the given condition to one on a, b, c.
2. Let the expression you obtained be $A = B$. Can you find an expression S such that $A \le S \le B$ for all x, y, z?
3. Manipulate the equality case of the expression to find a very simple restriction on x, y, z.
4. Find the probability that this restriction holds for some p.
5. Stemming from the last step, find the minimum number of prime factors that n must-have.
6. We don't care about the specific values of the prime factors. Thus, if the number you obtained in the last step was k, sum the first k primes.

A hint if you're stuck at step 4: remember that we can let n be anything – the exponents of primes in n can be arbitrarily large. Consider what happens when the exponent of p in n, is arbitrarily large. Also, note that the inequality is strict.

Again, this problem exhibits a key problem-solving idea with GCD and LCMs: ***the prime factors are independent of each other!*** In many GCD and LCM problems with little constants, often the values of the prime factors themselves don't matter – only their exponent matters.

Next up is a token application of the Euclidean Algorithm.

Example 5.4 (2012 PUMaC NT B6)
Let $f_n(x) = n + x^2$. Evaluate the product

$$\gcd\{f_{2001}(2002), f_{2001}(2003)\} \times \gcd\{f_{2011}(2012), f_{2011}(2013)\} \times \gcd\{f_{2021}(2022), f_{2021}(2023)\},$$

where $\gcd\{x, y\}$ is the greatest common divisor of x and y.

Walkthrough. This problem is quite straightforward with the Euclidean Algorithm.

1. What is the relation between 2003 and 2002? Between 2013 and 2012, and so on? Can you find a general form of the GCD's that we are trying to evaluate?
2. Use the Euclidean Algorithm to reduce that GCD.
3. You should still end up with an x^2 term somewhere. How can you reduce that term? (Hint: Complete the square.)
4. After reducing the GCD, multiply to finish.

6 Problems

Minimum is [27 ♟]. Problems denoted with ♜ are required. (They still count towards the point total.)

[2 ♜] **Problem 1 (2019 PUMaC NT/A1).** The least common multiple of two positive integers a, b is $2^5 \cdot 3^5$. How many such ordered pairs (a, b) are there? **Hints**: 14

[2 ♟] **Problem 2 (2016 AMC 10A/25, 2016 AMC 12A/22).** How many ordered triples (x, y, z) of positive integers satisfy $\text{lcm}(x, y) = 72, \text{lcm}(x, z) = 600$ and $\text{lcm}(y, z) = 900$? **Hints**: 7

[3 ♟] **Problem 3 (2015 PUMaC NT A2).** What is the sum of all positive integers n such that $\text{lcm}(2n, n^2) = 14n - 24$? **Hints**: 6

[4 ♟] **Problem 4 (2018 AMC 10B/23).** How many ordered pairs (a, b) of positive integers satisfy the equation

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

where $\gcd(a, b)$ denotes the greatest common divisor of a and b, and $\text{lcm}(a, b)$ denotes their least common multiple? **Hints**: 21 19

[4 ♟] **Problem 5 (2020 AMC 10A/24).** Let n be the least positive integer greater than 1000 for which

$$\gcd(63, n + 120) = 21 \quad \text{and} \quad \gcd(n + 63, 120) = 60.$$

What is the sum of the digits of n? **Hints**: 20 24 23

[5 ♜] **Problem 6 (2017 CMIMC NT/2).** Determine all possible values of $m + n$, where m and n are positive integers satisfying

$$\text{lcm}(m, n) - \gcd(m, n) = 103.$$

Hints: 10 1 9

[5 ♟] **Problem 7 (2017 PUMaC NT/2).** The sequence of positive integers $a_1, a_2, \ldots$ has the property that $\gcd(a_m, a_n) > 1$ if and only if $|m - n| = 1$. Find the sum of the four smallest possible values of a_2. **Hints**: 4 16

[5 ♟] **Problem 8 (2020 AMC 12A/21).** How many positive integers n are there such that n is a multiple of 5, and the least common multiple of 5! and n equals 5 times the greatest common divisor of 10! and n? **Hints**: 27 13

[6 ♟] **Problem 9 (1985 AIME/13).** 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. **Hints**: 12

[6 ♟] **Problem 10 (2017 CMIMC NT/5).** One can define the greatest common divisor of two positive rational numbers as follows: for a, b, c, and d positive integers with $\gcd(a, b) = \gcd(c, d) = 1$, write

$$\gcd\left(\frac{a}{b}, \frac{c}{d}\right) = \frac{\gcd(ad, bc)}{bd}.$$

For all positive integers K, let $f(K)$ denote the number of ordered pairs of positive rational numbers (m, n) with $m < 1$ and $n < 1$ such that

$$\gcd(m, n) = \frac{1}{K}.$$

What is $f(2017) - f(2016)$? **Hints**: 17 8 25

[7 ♟] Problem 11 (2020 PUMaC NT/A4). Given two positive integers $a \neq b$, let $f(a, b)$ be the smallest integer that divides exactly one of a, b, but not both. Determine the number of pairs of positive integers (x, y), where $x \neq y$,$1 \leq x, y, \leq 100$ and $\gcd(f(x, y), \gcd(x, y)) = 2$. **Hints**: 22 3 2 28

[8 ♜] Problem 12 (2021 AIME I/10). Consider the sequence $(a_k)_{k\geq 1}$ of positive rational numbers defined by $a_1 = \frac{2020}{2021}$ and for $k \geq 1$, if $a_k = \frac{m}{n}$ for relatively prime positive integers m and n, then

$$a_{k+1} = \frac{m + 18}{n + 19}.$$

Determine the sum of all positive integers j such that the rational number a_j can be written in the form $\frac{t}{t+1}$ for some positive integer t. **Hints**: 26 15 11 5

7 Hints

1. Let $\text{lcm}(m,n) = k\gcd(m,n)$ for some k.
2. WLOG $\nu_2(x) > \nu_2(y)$. Then $\nu_2(y) = 1$.
3. Combine this with the GCD condition. What do you obtain?
4. Every a_n must have one prime factor in common with a_{n-1} and one in common with a_{n-2}.
5. You should reach a point when all fractions after some given one will be in simplest form.
6. We can compute $\text{lcm}(2n, n^2)$ explicitly.
7. This is basically just Example 4.5, but with different numbers.
8. Why does it suffice to consider pairs of positive rational numbers (m', n') with $\gcd(m', n') = 1$?
9. Consider cases to finish. Notice that 103 is prime.
10. Recall that the LCM of two numbers is always a multiple of the GCD of the two numbers.
11. When you find an unsimplified fraction, simpify it and repeat.
12. Use the Euclidean Algorithm.
13. Notice that the power of 5 in n must be 3. Can you finish similarly?
14. Using the definition of LCM, convert the condition to one concerning the exponents of primes.
15. Use the Euclidean Algorithm.
16. The smallest such a_2 are of the form cp^aq^b for some constant c.
17. This definition of GCD is multiplicative.
18. How are GCD and LCM related?
19. Set $\gcd(a,b) = x$ and $\text{lcm}(a,b) = y$. Then use Simon's Favorite Factoring Trick. (If you don't know what this is, consult Section 7.
20. The first condition can be rewritten as $n + 120$ is a multiple of 21, but not 63.
21. Recall that $\gcd(a,b) \cdot \text{lcm}(a,b) = ab$.
22. $f(x,y)$ is always a power of a prime.
23. Finally, eliminate the cases where $n + 120$ is a multiple of 63 and similarly for the other GCD condition to finish.
24. First ignore the not-multiple-of-63 condition and solve a system of modular congruences.
25. m', n' must be relatively prime positive integers.
26. The raw, unsimplified form of a_n is in simplest form most times. Can you figure out when it isn't?
27. Look at the exponents of primes separately.
28. Either x and y are all multiples of 3, or they both aren't.