gcd and lcm, wtf? (What's Their Function)

We need to start with one of them, so let's start with the $\gcd$.

Definition 1. *Let a and b be two positive integers. We define the quantity $\gcd(a, b)$ to be the largest integer d so that $d \mid a$, and $k \mid b$.*

Or, equivalently, remember that the fundamental theorem of arithmetic guarantees that we can write any natural number uniquely as a product of powers of primes. Let a and b be two positive integers and let $p_1, p_2, \ldots, p_n$ be a collection of prime numbers that appear in the factorization of a or b. Then we can write $a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$. We are under the convention that if p_i is a prime factor of a and not a prime factor of b, then $r_i \geq 1$ and $s_1 = 0$. Similarly, if p_j is a prime factor of b but it is not a prime factor of a, then $s_j \geq 1$ and $r_j = 0$. Whoa hoss! Let's look at an example so that you can see what in the world I'm talking about.

Example : Let $a = 729,904,463,220$ and $b = 93,976,850$. Observe that $a = (2^2)(3)(5)(17^3)(19^5)$ and $b = (2)(5^2)(11)(17)(19)(23^2)$ (I know because I started with the prime factorization and multiplied it out). Then we need to list all of the primes that occur in each factorization. I see a 2, a 3, a 5, an 11, a 17, a 19, and a 23. So, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 11$, $p_5 = 17, p_6 = 19, p_7 = 23$

$$\begin{aligned} a &= (2^2)(3^1)(5^1)(11^0)(17^3)(19^5)(23^0) \\ &= p_1^2 \cdot p_2^1 \cdot p_3^1 \cdot p_4^0 \cdot p_5^3 \cdot p_6^5 \cdot p_7^0 \end{aligned}$$

and

$$\begin{aligned} b &= (2^1)(3^0)(5^2)(11^1)(17^1)(19^1)(23^2) \\ &= p_1^1 \cdot p_2^0 \cdot p_3^2 \cdot p_4^1 \cdot p_5^1 \cdot p_6^1 \cdot p_7^2 \end{aligned}$$

Why in heavens name would you want to do that? Because we can write down an actual equation for the $\gcd$.

Definition 2. *Let a, b, p_i, r_i, and s_1 be as above. Then,*

$$\gcd(a, b) = p_1^{\min\{r_1, s_1\}} p_2^{\min\{r_2, s_2\}} \cdots p_n^{\min\{r_n, s_n\}}$$

So, back to our last example. We have the following,

$$\begin{aligned} &\gcd(729904463220, 93976850) \\ &= 2^{\min\{2,1\}} \cdot 3^{\min\{1,0\}} \cdot 5^{\min\{1,2\}} \cdot 11^{\min\{0,1\}} \cdot 17^{\min\{3,1\}} \cdot 19^{\min\{5,1\}} \cdot 23^{\min\{0,2\}} \\ &= 2 \cdot 5 \cdot 17 \cdot 19 \end{aligned}$$

We can now define the least common multiple similarly.

Definition 3. *Let a, b, p_i, r_i, and s_i be as above. Then we define the least common multiple of a and b to be*

$$\operatorname{lcm}(a,b) = p_1^{\max\{r_1,s_1\}} p_2^{\max\{r_2,s_2\}} \cdots p_n^{\max\{r_n,s_n\}}.$$

So, back to our last example,

$$\begin{aligned}
&\operatorname{lcm}(729904463220, 93976850)\\
&= 2^{\max\{2,1\}} \cdot 3^{\max\{1,0\}} \cdot 5^{\max\{1,2\}} \cdot 11^{\max\{0,1\}} \cdot 17^{\max\{3,1\}} \cdot 19^{\max\{5,1\}} \cdot 23^{\max\{0,2\}}\\
&= 2^2 \cdot 3 \cdot 5^2 \cdot 11 \cdot 17^3 \cdot 19^5 \cdot 23^2
\end{aligned}$$

Here's a neat consequence of these ideas.

Theorem 1. *Let $a, b \in \mathbb{N}$. Then $ab = \gcd(a,b) \cdot \operatorname{lcm}(a,b)$.*

Proof. Here's a perfect example of a proof that falls right out of the definitions. We will start on the right side and show that we can get the left side. Suppose that we can write out a and b in terms of their prime factors as we have done previously. That is, suppose

$$\begin{aligned}
a &= p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}\\
b &= p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}
\end{aligned}$$

Remember, some of the r_i's or s_i's may be a zero, depending on whether or not the prime p_i is a factor of a or b respectively. So, from the definitions we know that,

$$\begin{aligned}
&\gcd(a,b) \cdot \operatorname{lcm}(a,b)\\
&= \left(p_1^{\min\{r_1,s_1\}} p_2^{\min\{r_2,s_2\}} \cdots p_n^{\min\{r_n,s_n\}}\right) \left(p_1^{\max\{r_1,s_1\}} p_2^{\max\{r_2,s_2\}} \cdots p_n^{\max\{r_n,s_n\}}\right)\\
&= p_1^{r_1} \cdot p_1^{s_1} \cdot p_2^{r_1} \cdot p_2^{s_2} \cdots p_n^{r_n} \cdot p_n^{s_n}\\
&= \left(p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}\right) \left(p_1^{s_1} \cdot p_2^{s_2} \cdots p_n^{s_n}\right)\\
&= ab
\end{aligned}$$

The idea being that $\min\{r_i, s_i\}$ is either r_i or s_i and the $\max\{r_i, s_i\}$ is either the other one or they are equal. In either case, both p^{r_i} and p^{s_i} show up in the product. $\square$