Math 255 - Spring 2022
The least common multiple
15 points

This project will define the notion of the **least common multiple** of two (nonnegative) integers, and invite you to prove some facts about the least common multiple. Please read the text, and answer the questions below for credit.

Let a, b be two integers with $a, b \geq 0$ for simplicity. (As usual, we could consider negative integers as well but it would complicate arguments without adding much insight.) We define their **least common multiple**, often denoted $\text{lcm}(a, b)$, to be the integer $l > 0$ such that

1. a divides l and b divides l (l is a positive common multiple of a and b); and
2. if a divides m and b divides m, and $m > 0$, then $l \leq m$ (l is the *smallest* of the positive common multiples of a and b).

Make sure that you compare this to the definition of greatest common divisor!

Notice that this definition in fact does not work if $a = 0$ or $b = 0$: the least common multiple as defined above does not exist, since in that case there are no positive common multiples of a and b, because the only multiple of 0 is 0.

Just as we could give a slightly different definition of greatest common divisor to handle the case where both a and b are zero, we can also slightly modify the definition of least common multiple to allow a or b to be zero. Let's call this our *second definition of the least common multiple*: This is the integer $l \geq 0$ such that

1. a divides l and b divides l; and
2. if a divides m and b divides m, then l divides m.

Once again, compare this to the second definition of the greatest common divisor. In both cases the "least" or "greatest" part of the definition was replaced with the appropriate divisibility statement. Notice that in this case we also do not need to ensure that $m > 0$.

Now that you know about the least common multiple, please answer the following questions:

1. Prove that the "usual" definition of the least common multiple (the one given first) is equivalent to the second definition of the least common multiple when a and b are not zero.
2. Prove that the greatest common divisor of two positive integers divides their least common multiple.
3. Please prove Theorem 3 of Section 2, which gives the prime-power decomposition of the greatest common divisor of a and b.

4. Please state and prove an analogue of Theorem 3 for the least common multiple of a and b when a and b are not zero. In other words, please describe the prime-power decomposition of $\operatorname{lcm}(a, b)$, just like Theorem 3 gives the prime-power decomposition of $\gcd(a, b)$.

5. Prove that if $a, b \geq 0$ are two integers, then

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