SRQR: Divisibility (April 1, 2021)

I'm a little confused about the proof for theorem 2.8.

The theorem says that, for positive integers a and b, we have

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

Let me write out the proof in slightly different words.

Notice that the equation says that $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$. In other words, we have a number — namely, the number $ab/\gcd(a, b)$ — and we want to prove that this number is actually the least common multiple of a and b. For notational convenience, we set $d = \gcd(a, b)$ and $m = ab/\gcd(a, b) = ab/d$. In other words, we're trying to prove that m is actually the least common multiple of a and b.

There are two steps to doing this (basically because there are two parts to definition 2.4). The first part is to show that m is actually a common multiple of a and b. The second part is to show that m is the smallest of all positive common multiples.

First, let's show that m is a common multiple of a and b. Since $d \mid a$, we know that there exists an integer r such that $a = dr$. Then

$$m = \frac{ab}{d} = \frac{(dr)b}{d} = rb,$$

which shows us that m is a multiple of b. Similarly, since $d \mid b$, we know that there exists an integer s such that $b = ds$. Then

$$m = \frac{ab}{d} = \frac{a(ds)}{d} = as,$$

which shows us that m is a multiple of a. Thus m is a common multiple of a and b.

The next part is to show that m is the smallest out of all of the positive common multiples of a and b. Suppose c is an arbitrary positive common multiple of a and b. If we can show that c/m is an integer, that would mean that m is a divisor of c so it must be that $m \leqslant c$. In other words, it is sufficient to show that c/m is an integer, since that will imply that m is smaller than c and therefore that m is the smallest of all of the positive common multiples of a and b.

To show that c/m is an integer, we have to introduce some more notation. First, since c is a common multiple of a and b, we know that $c = au$ and $c = bv$ for some integers u and v. Also, by theorem 2.3 (which, incidentally, is also called *Bézout's theorem*), we know that

$d = \gcd(a, b) = ax + by$ for some integers x and y. Now we do some algebra:

$$\begin{aligned}
\frac{c}{m} &= \frac{c}{ab/d} \\
&= \frac{cd}{ab} \\
&= \frac{c(ax + by)}{ab} \\
&= \frac{cax}{ab} + \frac{cby}{ab} \\
&= \frac{cx}{b} + \frac{cy}{a} \\
&= \frac{(bv)x}{b} + \frac{(au)y}{a} \\
&= vx + uy.
\end{aligned}$$

Since u, v, x, y are all integers, this shows that c/m is an integer. As described in the previous paragraph, this means that $m \leqslant c$. In other words, m is the least common multiple of a and b.

> My question relates to Theorems 2.3 and 2.6. I can follow the algebra and technical argument of both proofs, and I understand the result, but is there a more conceptual/intuitive way to understand what's going on in these proofs and why the properties of divisibility and greatest common divisors yield these results?

The proof of theorem 2.6 is mostly just an application of theorem 2.3. Most of the subtlety is in the proof of theorem 2.3. And actually, the book sort of gives us two different proofs of theorem 2.3, though it doesn't say things in this way!

The proof given right after theorem 2.3 is one proof, but it's abstract and non-constructive. It tells you that $\gcd(a, b)$ is the smallest element of this set S, but it gives you no way of actually finding that smallest element!

In fact, the book does also give us a constructive proof of theorem 2.3, though it doesn't state it as such: the "constructive proof" is the Euclidean algorithm of section 2.4! This is an explicit process for *how* to write $\gcd(a, b)$ as a linear combination of a and b. You can work through examples of the Euclidean algorithm by hand, and seeing that this process always works is probably pretty convincing evidence that $\gcd(a, b)$ can in fact be written as a linear combination of a and b.

Generally, constructive proofs are much better at giving you an intuitive understanding. With non-constructive proofs, I think it's fairly normal to feel like you can follow what's going on technically but you don't really understand it. This is why mathematicians often prefer constructive proofs whenever possible.

> I was wondering the difference between a lemma, a corollary, and a theorem. After googling the answers, here is what I got:
> A theorem is a major result that says something definitive. A corollary is a theorem that follows on from another theorem. It can be a reverse proof of a theorem. A lemma is a small result (less important than a theorem). It is a subsidiary proposition assumed to be valid and used to demonstrate a principal proposition.

I will let this "question" stand as it's own response ☺

> I went to search the term "relatively prime integer" and found that it just another way of saying "coprime."

> I was initially confused on the difference between something being divisible by an integer and dividing something by an integer. The formatting of the $a \mid b$ made my brain automatically think a/b, but after some practice with it and plugging in example numbers it made sense that it's rather b being divided into a, if that makes sense.

These concepts (division, divisibility, relatively prime / coprime, . . .) have been around a really long time. That means that terminology and notation related to these concepts have proliferated. Sometimes, we have choices of different words and different grammatical structures that all exactly the same mathematical concept. For example, the following sentences are all completely synonymous:

- a is relatively prime to b
- a is coprime to b
- a and b are relatively prime
- a and b are coprime

Similarly the words "divisor" and "factor" mean exactly the same thing, as do "greatest common divisor" and "highest common factor." This terminological proliferation also leads to notational proliferation. For example, $\gcd(a, b)$ is sometimes denoted $\mathrm{hcf}(a, b)$, where hcf stands for "highest common factor."

And then sometimes we have notation or terminology that is closely related to something else but not exactly the same. For example, the words "divisor" and "multiple" are closely related. The fact that 5 is a divisor of 15 corresponds precisely to 15 being a mulitple of 5. Probably we don't strictly need both of these words around, but it is quite convenient to have words for these "dual" concepts. For example, it's a lot easier to say "the set of multiples of 5" than it is to say "the set of numbers which have 5 as a divisor."

Similar is the relation between the notations "b/a" and "$a|b$." We probably don't strictly *need* the notation "$a|b$," since it's completely equivalent to "b/a is an integer." But it is quite convenient, as you've already begun to see and will continue to see.

We'll continue to see this proliferation going forward. It might feel a bit frustrating to have many words and pieces of notation for the same concept, but it's just a historical fact we have to deal with. You do get used to all of it over time!