Divides, gcd, and lcm

Here is some stuff about the integers $\mathbb{Z}$ that we learn at some point and then eventually forget until it crops up again in surprising ways in abstract algebra.

Definition (divides)**.** If $a, b \in \mathbb{Z}$ with $a \neq 0$, we say that a divides b if there is some other integer $c \in Z$ such that $b = a \cdot c$. If so, we write $a \mid b$; if not, we write $a \nmid b$.

Observations:

- Example: $12 \mid 120$ because $120 = 12 \cdot 10$.
- $3 \nmid 5$ because if I tried to write $5 = 3 \cdot c$, then c would have to be $\frac{5}{3}$, which is not an integer.
- "a divides b" is, annoyingly, synonymous with "b is a multiple of a".
- Every integer divides 0.
- Every integer divides itself.
- 1 divides every integer.

Definition (greatest common divisor, or gcd)**.** If $a, b \in \mathbb{Z} - \{0\}$, then there is a unique integer $d \in \mathbb{Z} - \{0\}$, called the greatest common divisor of a and b, such that:

(a) $d \mid a$ and $d \mid b$ (so d is a "common divisor" of a and b)

(b) if there's some integer $e \in \mathbb{Z}$ such that $e \mid a$ and $e \mid b$, then $e \mid d$ (so d is the "greatest" aka "biggest" of all the common divisors of a and b).

We write $d = \gcd(a, b)$, or, whenever it's clear from context that this isn't an ordered pair or something, $d = (a, b)$.

Definition (relatively prime)**.** If $\gcd(a, b) = 1$, then we say that a and b are relatively prime.

Observations:

- 1 always divides both a and b. If a and b are relatively prime, the point is that *nothing else* divides both a and b.
- If the numbers are smallish, you can decide about their gcd by looking at their prime factorization (but that's hard if the numbers are big). Otherwise, you can repeatedly do long division with remainders – this is called the Euclidean algorithm.
- Example: $\gcd(180, 24) = \gcd(2^2 \cdot 3^2 \cdot 5,\ 2^3 \cdot 3) = 2^2 \cdot 3 = 12$.
- Example: $10 = 2 \cdot 5$ and $21 = 3 \cdot 7$ are relatively prime.
- Any two distinct prime numbers are relatively prime.

Definition (least common multiple, or lcm)**.** If $a, b \in \mathbb{Z} - \{0\}$, then there is a unique integer $\ell \in \mathbb{Z} - \{0\}$, called the least common multiple of a and b (or $\mathrm{lcm}(a, b)$) such that:

(a) $a \mid \ell$ and $b \mid \ell$ (so ℓ is a "common multiple" of a and b)

(b) if there's some integer $m \in \mathbb{Z}$ such that $a \mid m$ and $b \mid m$, then $\ell \mid b$ (so ℓ is the "least" aka "smallest" of all the common multiples of a and b).

Observations:

- I really wish it was called the "smallest common multiple," because "least-common" sounds like it would mean something like "rarest."
- The problem is exactly that it's "least common-multiple," not "least-common multiple," if you see what I mean.
- Example: $\mathrm{lcm}(10, 15) = \mathrm{lcm}(2 \cdot 5, 3 \cdot 5) = 2 \cdot 3 \cdot 5 = 30$. Check that $30 \mid 10 \cdot 15 = 150$.
- ab is certainly a common multiple of a and b, so $\ell \mid ab$.
- $\mathrm{lcm}(a, b) \cdot \gcd(a, b) = ab$. (!!)
- If a and b are relatively prime, then $\mathrm{lcm}(a, b) = ab$.