Recap

- Definition: prime, composite.
- Lemma: Every $n \in \mathbb{N}$, $n \geq 2$, has a prime factor.

  This implies every $n \in \mathbb{N}$, $n \geq 2$ can be factored into primes.

  The Fundamental Theorem of Arithmetic says this factorisation is unique. (Proof omitted.)
- Theorem: There are infinitely many primes.
- Definition: greatest common divisor, $\gcd(a,b)$.
- Lemma: For all $a, b \in \mathbb{N}$ there exist q, r such that $a = qb + r$, where $0 \leq r < b$.
- Lemma: With a, b, q, r as above: if $r > 0$ then $\gcd(a,b) = \gcd(b,r)$
- Euclid's algorithm for computing the gcd repeats this reduction until $r = 0$.

Definition Let $a, b \in \mathbb{N}$. Then the lowest common multiple of a and b, $\mathrm{lcm}(a,b)$ is the smallest number m such that $a \mid m$ and $b \mid m$.

Examples $\mathrm{lcm}(15,35) = 105 = 7 \times 15 = 3 \times 35$

$\mathrm{lcm}(24,30) = 120 = 5 \times 24 = 4 \times 30$.

Lemma 4.7 Suppose $a, b, n \in \mathbb{N}$ and let $m = \mathrm{lcm}(a,b)$. If $a \mid n$ and $b \mid n$ then $m \mid n$.

Proof By Lemma 4.5 we can write n as $n = qm + r$ where $0 \le r < m$. If $r = 0$, then $n = qm$ and we are done. Now suppose $r > 0$. Rearranging, $r \overset{(*)}{=} n - qm > 0$. Since $a \mid n$ and $a \mid b$, we see that a divides the r.h.s. of $(*)$ and hence it divides r : $a \mid r$. Similarly, $b \mid r$. Thus r is a common multiple of a and b, and so $r \ge m$. Contradiction. $\boxtimes$

<u>Experiment</u> Let $a = 15$, $b = 35$. Then $\mathrm{lcm}(a,b) = 105$, and $\gcd(a,b) = 5$. Now $\mathrm{lcm}(a,b) \times \gcd(a,b) = 105 \times 5 = 525$, and $a \times b = 15 \times 35 = 525$.

<u>Theorem 4.8</u> Suppose $a, b \in \mathbb{N}$. Then $\gcd(a,b)\,\mathrm{lcm}(a,b) = ab$.

<u>Proof</u> Let $g = \gcd(a,b)$ and $m = \mathrm{lcm}(a,b)$. Let's consider $\frac{ab}{g}$, which is an integer. Moreover, $a \mid \frac{ab}{g}$ and $b \mid \frac{ab}{g}$. Hence, $\frac{ab}{g}$ is a common multiple of a, b. Thus $\frac{ab}{g} \geq m$. Equivalently, $ab \geq mg$ (+).

Let's now consider $\frac{ab}{m}$. Note that ab is a common multiple of a and b. By Lemma 4.7, $\mathrm{lcm}(a,b) = m \mid ab$. So $\frac{ab}{m}$ is an integer. Now $a \mid m \Rightarrow ab \mid mb \Rightarrow \frac{ab}{m} \mid b$.

an integer!

Similarly, $\frac{ab}{m} \mid a$. Thus $\frac{ab}{m}$ is a common divisor of a and b, and hence is no bigger that the greatest common divisor, g. We have $\frac{ab}{m} \leq g$, or $ab \leq gm$. (††) Putting (†) and (††) together, we get $ab = gm$. $\boxtimes$