Direct Proof

Direct Proof

From page 122 of the text

Proposition If $a, b, c \in \mathbb{N}$, then $\text{lcm}(ca, cb) = c \cdot \text{lcm}(a, b)$.

Proof. Assume $a, b, c \in \mathbb{N}$. Let $m = \text{lcm}(ca, cb)$ and $n = c \cdot \text{lcm}(a, b)$. We will show $m = n$. By definition, $\text{lcm}(a, b)$ is a positive multiple of both a and b, so $\text{lcm}(a, b) = ax = by$ for some $x, y \in \mathbb{N}$. From this we see that $n = c \cdot \text{lcm}(a, b) = cax = cby$ is a positive multiple of both ca and cb. But $m = \text{lcm}(ca, cb)$ is the *smallest* positive multiple of both ca and cb. Thus $m \leq n$.

On the other hand, as $m = \text{lcm}(ca, cb)$ is a multiple of both ca and cb, we have $m = cax = cby$ for some $x, y \in \mathbb{Z}$. Then $\frac{1}{c}m = ax = by$ is a multiple of both a and b. Therefore $\text{lcm}(a, b) \leq \frac{1}{c}m$, so $c \cdot \text{lcm}(a, b) \leq m$, that is, $n \leq m$.

We've shown $m \leq n$ and $n \leq m$, so $m = n$. The proof is complete. ■

Figure 1: lcm proposition

The hidden part - check the definitions

Definition: Let a and b be positive integers. Then the least common multiple $\mathrm{lcm}(a, b)$ is the smallest positive integer m such that $a|m$ and $b|m$.

Definition: if a, m are natural numbers, then $a|m$ means there exists a natural number y such that $m = ay$.

Example: $2|6$ $\quad 6 = 2 \cdot 3$

m a y

$\nmid$ $\quad 5 \nmid 7$ means there is no $y \in \mathbb{N}$ for which $7 = 5y$

$\nmid$ = does not divide

For all $y \in \mathbb{N}$, $5y \neq 7$

Since $7 = 5 \cdot 1 + 2$ by the division alg $5 \nmid 7$

q r $0 \leq r < 5$

$a = 12 \qquad b = 9$

$a \cdot b = 108$

$12 \mid 108 \qquad 9 \mid 108$

$108 = 12(9) \qquad 108 = 9(12)$

$12 \mid 36$? $\qquad 9 \mid 36$?

yes $36 = 3 \cdot 12 \qquad 36 = 9y \quad y \in \mathbb{N}$?

$36 = 9 \cdot 4$

$72 = 36 \cdot 2$

$12 \mid 72 \qquad 9 \mid 72$

$72 = 6 \cdot 12 \qquad 72 = 9 \cdot 8$

$\text{lcm}(12, 9) = 36$

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

The hidden part II

Second, make sure the claim is clear. Look at some examples.

$$lcm(ca, cb) = c\, lcm(a, b)$$

$a = 2 \quad b = 3 \quad c = 4$

$ca = 8 \quad c \cdot b = 12$

$$lcm(8, 12) = 4\, lcm(2, 3)$$

$$= 24$$

$8 = 2^3 \cdot 3^0$

$12 = 2^2 \cdot 3$

$lcm(8, 12) = 2^3 \cdot 3$

$= 24$

$a = 8 \quad b = 9 \quad c = 10$

$$lcm(80, 90) = 10\, lcm(9, 9)$$

$2^4 \cdot 5 \quad 2 \cdot 3^2 \cdot 5 \quad 720$

$2^4 \cdot 5 \cdot 3^2 \quad 16 \cdot 5 \cdot 9 = 80 \cdot 9 = 720$

The hidden part continued III - interpret the definition

Three ways of saying the same thing:

- m is the smallest positive integer such that $a|m$ and $b|m$
- If x is a positive integer so that $a|x$ and $b|x$, then $x \geq \mathrm{lcm}(a, b)$.
- If x is a positive integer so that $a|x$ and $b|x$, then $\mathrm{lcm}(a, b) \leq x$.

The hidden part IV

Read the proof to understand it's structure, without worrying about the details.

Take the proof of the proposition apart

- Assume $a, b, c \in \mathbb{N}$.
- Let $m = \mathrm{lcm}(ca, cb)$ and $n = c\,\mathrm{lcm}(a, b)$. We will show that $m = n$.
- By definition, $\mathrm{lcm}(a, b)$ is a positive multiple of both a and b, so $\mathrm{lcm}(a, b) = ax = by$ for some x and y in $\mathbb{N}$.
- From this we see that $n = c\,\mathrm{lcm}(a, b) = cax = cby$ is a positive multiple of both ca and cb. Thus $m \leq n$.

$n = (ca)x = (cb)y$

$\Rightarrow$ n is a common multiple of ca and cb

$\therefore \quad n \geq \mathrm{lcm}(ca, cb)$

Taking the proof apart

- On the other hand, as $m = \mathrm{lcm}(ca, cb)$ is a multiple of both ca and cb, we have $m = cax = cby$ for some $x, y \in \mathbb{Z}$.
- Then $\frac{1}{c}m = ax = by$ is a multiple of both a and b.
- Therefore $\mathrm{lcm}(a, b) \leq \frac{1}{c}m$ so $c\,\mathrm{lcm}(a, b) \leq m$, that is $n \leq m$.
- Since $m \leq n$ and $n \leq m$, we have $m = n$. The proof is complete.

$\frac{m}{c} = ax = by$ are in $\mathbb{N}$

$\frac{m}{c}$ is a common multiple of a, b.

Suppose a, b, c are integers, $a, b \neq 0$

Show: If $a|b$ and $b|c$ then $a|c$.

Remember: $a|b$ means there exists $k \in \mathbb{Z}$ so that $b = ka$

① $a|b$ so there is a k with $b = ak$

② $b|c$ so there is a k' with $c = bk'$

③ $c = (ak)k' = a(kk')$

Therefore $a|c$ since kk' is an integer and $c = a(kk')$

$3|6$ $\quad$ $6|24$

$6 = 3 \cdot 2$ $\quad$ $24 = 6 \cdot 4$

$24 = (3 \cdot 2)(4) = 3 \cdot 8$

so $3|24$

$b = ak$

$c = bk'$

$c = akk'$ ✓