3.8 Finding mistakes in proofs

- Correct grammar/syntax in the proof?
- Implications go in the correct direction?
- Each line follows from the previous ones in logical way?
- Uses all hypotheses?
- Work through proof with special values for variables?

4.1 Natural numbers and integers.

Natural numbers are the positive integers, denoted by $\mathbb{N}$. Good intuition about these. The operators $+, \times$: if $n, m \in \mathbb{N}$ then $n+m, n \times m \in \mathbb{N}$. They satisfy useful laws:

$(x+y)+z = x+(y+z)$, $x \times y = y \times x$, $x \times (y+z) = xy + xz$.

There is an order $<$. It satisfies: if $n < m$ and $m < k$ then

$n < k$. Also: if $n < m$ then $kn < km$.

Why go beyond $\mathbb{N}$? In order to solve equations such as $n + 3 = 1$. Introduce for each $n \in \mathbb{N}$ a number $-n$ with the property that $n + (-n) = 0$. Use $\mathbb{Z}$ to denote the integers. The laws for $\mathbb{N}$ hold for $\mathbb{Z}$. Still have an ordering $<$, but we need to take case: if $n < m$ and $k > 0$ then $kn < km$, but if $k < 0$ the $kn > km$.

Still can't solve $3n = 2$, but we'll return to that.

4.2 Divisibility and primes

Work with natural numbers.

Definition (divides). Let $m, n \in \mathbb{N}$. We write $m | n$ and say m divides n if there exists $k \in \mathbb{N}$ such that $mk = n$. If m does not divide n then we write $m \nmid n$.

Examples: $1 | n$, $n | n$ for all $n \in \mathbb{N}$. $3 | 12$, $5 | 30$, $7 \nmid 15$.

Lemma 4.1 Let $a, b, c \in \mathbb{N}$. Then $a | b$ and $b | c \Rightarrow a | c$.

Proof By definition, there exist k, l such that $ak = b$

and $bl = c$. Then multiplying by l: $akl = bl = c$.
Thus, $a | c$. $\boxtimes$

<u>Lemma 4.2</u> Let $a, b, c \in \mathbb{N}$, Suppose $a | b$, $a | c$ and $b < c$.
Then $a | (c-b)$.

<u>Proof</u> By definition, there exist k, l such that $ak = b$ and $al = c$. Then, subtracting, $al - ak = c - b$ or $a(l-k) = c - b$. So $a | (c-b)$. $\boxtimes$