Lesson 4

Three proof methods. Examples.

Def: a in $\mathbb{Z}$ is even iff $\exists k$ in $\mathbb{Z}$ $a = 2k$.

a in $\mathbb{Z}$ is odd iff $\exists k$ in $\mathbb{Z}$ $a = 2k+1$

Given a, b in $\mathbb{Z}$ a divides b iff
b is a multiple of a
$\exists k$ in $\mathbb{Z}$ $b = a \cdot k$.

Th: Being a multiple of 4 is sufficient for being even. This means

$\forall x$ in $\mathbb{Z}$ $\underbrace{x \text{ is a multiple of } 4}_{P(x)} \Rightarrow \underbrace{x \text{ is even}}_{Q(x)}$

is True

Proof: suppose x is a multiple of 4,
that is $x = 4k$ for some k in $\mathbb{Z}$,
then $x = 2(2k)$ and $2k$ is in $\mathbb{Z}$
therefore x is even

This is an example of a direct proof.

Th: the square of an even integer is even.

This means

$\forall x$ in $\mathbb{Z}$ $\underbrace{x \text{ is even}}_{P(x)} \Rightarrow \underbrace{x^2 \text{ is even}}_{Q(x)}$

Proof: assume x is in $\mathbb{Z}$ and x is even then $x = 2k$ for some k in $\mathbb{Z}$ and therefore $x^2 = 4k^2 = 2(2k^2)$ so x^2 is even.

Th: x is even is a necessary condition for x^2 to be even.

This means prove that

$\forall x$ in $\mathbb{Z}$ $\underbrace{x^2 \text{ is even}}_{P(x)} \Rightarrow \underbrace{x \text{ is even}}_{Q(x)}$

Proof: try a direct proof, what happens?

proof by contraposition: assume x is odd, then $x = 2k+1$ for some k in $\mathbb{Z}$ and therefore $x^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Therefore x^2 is odd.

Division th: given integers a and b, with $b > 0$ there are unique integers q and r such that $a = bq + r$ and $0 \le r < b$

Note: a is divisible by $b \iff r = 0$.

We will not prove this theorem at the moment, but you can use it from now on.

Th: $\forall n$ in $\mathbb{Z}$ $\underbrace{6 \text{ divides } n}_{P} \iff \underbrace{((2 \text{ divides } n) \wedge (3 \text{ divides } n))}_{Q}$

choose a generic n in $\mathbb{Z}$ and show

$\forall n$ in $\mathbb{Z}$ 6 divides $n \iff ((2 \text{ divides } n) \wedge (3 \text{ divides } n))$

Recall that $P \iff Q$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ therefore

First we will prove that

$\forall n$ in $\mathbb{Z}$ 6 divides $n \Rightarrow ((2 \text{ divides } n) \wedge (3 \text{ divides } n))$

assume 6 divides n, then $n = 6k$ for some k in $\mathbb{Z}$, therefore $n = 2(3k)$ and $n = 3(2k)$ so 2 divides n and 3 divides n.

Now we need to prove

$\left(\underbrace{(2 \text{ divides } n) \wedge (3 \text{ divides } n)}_{A}\right) \Rightarrow \underbrace{6 \text{ divides } n}_{B}$:

Proof 1:

assume 2 divides n and 3 divides n, then $n = 2k$ and $n = 3h$ for some k h in $\mathbb{Z}$

the fore $2k = 3h$ so $3h$ is even and therefore h must be even, that is $h = 2t$ for some t in $\mathbb{Z}$, so

$n = 3h = 3 \cdot 2\,t = 6t$ so 6 divides n

Proof 2: assume by contreposition that 6 does not divide n, therefore $n = 6q + r$ with $0 < r < 6$.

Assume also that 2 divides n (can I assume this?), therefore $n = 2k$ for some k in $\mathbb{Z}$, so we have $n = 2k = 6q + r$

so $r = 2(k - 3q)$ is even so $r = 2$ or 4.

If $r = 2$ $n = 6q + 2 = 3(2q) + 2$ so if $r = 2$ 3 does not divide n.

If $r = 4$ $n = 6q + 4 = 6q + 3 + 1 = 3(2q + 1)$

so when $r = 4$ 3 does not divide n. Since in both cases ($r = 2$ or $r = 4$) 3 does not divide n we have shown that if 6 does divide n and 2 divides n then 3 does not divide n.

Are we done?

Statement to prove had the form

$(P \wedge Q) \Rightarrow R$

P is 2 div n
Q is 3 div n
R is 6 div n

Contrapositive is

$\neg R \Rightarrow \neg(P \wedge Q)$ that is $\neg R \Rightarrow (\neg P \vee \neg Q)$ S_1

We proved $(\neg R \wedge P) \Rightarrow \neg Q$ S_2 is this ok ?

yes $\neg R \Rightarrow (\neg P \vee \neg Q)$ and $(\neg R \wedge P) \Rightarrow \neg Q$ are equivalent as the truth table below shows

P	Q	R	$\neg P \vee \neg Q$	$\neg R \wedge P$	S1	S2
T	T	T	F	F	T	T
T	T	F	F	T	F	F
T	F	T	T	F	T	T
F	T	T	T	F	T	T
T	F	F	T	T	T	T
F	T	F	T	F	T	T
F	F	T	T	F	T	T
F	F	F	T	F	T	T