Last time: we studied the interaction between negation and quantifiers.

<u>Example</u> For all x: if x is a Snark then x is a Boojum.

Negation. There exists x such that x is a Snark and x is not a Boojum.

<u>Example</u> n is an integer.

For all n there exists an m such that $m > n$. (No largest number)

There exists n s.t. for all m: $m \leq n$. (There exists largest number.)

In general:

- Go left to right.
- Flip quantifiers "for all" $\leftrightarrow$ "exists"
- Flip operators "and" $\leftrightarrow$ "or"
- Negate atomic statements.

2.8 Converse and contrapositive

Given an implication $P \Rightarrow Q$, there are two related implications:

$$Q \Rightarrow P \qquad\qquad (\text{not } Q) \Rightarrow (\text{not } P)$$

converse $\qquad\qquad$ contrapositive.

The converse is in general <u>not</u> equivalent to the original implication

E.g. $\quad (x=2) \Rightarrow (x^2=4)$ ⊛ $\quad$ true

Converse $\quad (x^2=4) \Rightarrow (x=2) \quad$ false $\quad$ (could be that $x=-2$)

Very often a theorem has the form $(P \Rightarrow Q)$ and $(Q \Rightarrow P)$. In other words P and Q are equivalent, or $P \Leftrightarrow Q$, or P if and only if Q, P iff Q. Generally we need to prove $P \Rightarrow Q$ and $Q \Rightarrow P$ separately.

In contrast, the contrapositive is equivalent to the original implication. E.g. contrapositive of ⊛ is

$$(x^2 \neq 4) \Rightarrow (x \neq 2) \quad \text{true.}$$

Let's check the equivalence of the contrapositive by truth table:

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
F	F	T	T	T	T
F	T	T	F	T	T
T	F	F	T	F	F
T	T	F	F	T	T

Equal so • and • are equivalent.

Final example:

If rain is forecast, I carry an unbrella.

Contrapositive

If I am not carrying an umbrella then rain is not forecast

Quiz. n, a, b are all positive integers.

Composite(n) : there exist a, b s.t. $(n = ab)$ and $(a \neq 1)$ and $(b \neq 1)$

Negate Composite(n):

Prime(n) : for all a, b, $(n \neq ab)$ or $(a = 1)$ or $(b = 1)$

For all n, there exists m s.t. $(m > n)$ and Prime(m) and Prime($m+2$)

3.1 What is proof?

Premises/hypotheses ⇝ logical argument ⇝ conclusion.

Simple example

Theorem 3.1 Let n be a positive integer. If n is divisible by 3, then n^2 is divisible by 3.

Proof Let n be a positive integer divisible by 3. (Premise)

Write n as $n = 3k$ for some integer k.

Then $n^2 = (3k)^2 = 3(3k^2)$.

(Logical argument.)

So n^2 is divisible by 3

(Conclusion)

3.2 The logic of proof

Three kinds of theorem statements:

- For all ______ . Typical but hardest
- There exists ______ . Easier.
- Equivalence $P \Leftrightarrow Q$. Requires proving $P \Rightarrow Q$ and $Q \Rightarrow P$.

3.3 Proofs with several parts

- One argument works in one situation and another in a second.
- Format: "We consider two cases:"

  "First suppose ______ ..." (argument)

  "Next suppose ______ ..." (argument)

  "The cases are exhaustive, so the conclusion is ______"

Example:

Theorem 3.2 Suppose n is not divisible by 3. Then n^2+2 is divisible by 3.

Proof Write n as $n = 3k+j$ where $j=1$ or $j=2$.

Then $n^2+2 = (3k+j)^2 + 2 = 9k^2 + 6kj + j^2 + 2$

$$= 3(3k^2 + 2kj) + j^2 + 2$$

There are two cases:

$j = 1$: $\quad n^2 + 2 = 3(3k^2 + 2kj) + 3 = 3(3k^2 + 2kj + 1)$ ✓

$j = 2$: $\quad n^2 + 2 = 3(3k^2 + 2kj) + 6 = 3(3k^2 + 2kj + 2)$ ✓

These cases are exhaustive, and in both cases $n^2 + 2$ is divisible by 3. $\boxtimes$

3.4 Disproving a statement

Assuming the statement is "for all ...", this is generally easy — we just have to find one counterexample.

"Theorem" 3.3. Every prime is odd. False — 2 is prime.

"Theorem" 3.4. If p is a prime the $2^p - 1$ is a prime.

Try:

$p = 2$. $\quad 2^2 - 1 = 3$ prime ✓

$p = 3$. $\quad 2^3 - 1 = 7$ prime ✓

$p = 5$. $\quad 2^5 - 1 = 31$ prime ✓

$p = 7$ $\quad 2^7 - 1 = 127$ prime ✓

$p = 11$ $\quad 2^{11} - 1 = 2047 = 23 \times 89$. composite ✗

3-5 Special technique 1: proving the contrapositive.

We are asked to prove $P \Rightarrow Q$. Maybe hard.

It may be easier to prove $(\text{not } Q) \Rightarrow (\text{not } P)$.