Proof techniques:

- Direct proof
- Disproof by counterexample
- Proof by contradiction
- Proof by contrapositive
- Biconditional proof
- Proof by induction

YESTERDAY

TODAY

NEXT WEEK

Book: Chapter 1.5

Proof by contradiction

- You want to prove "p".
- You assume that p is false (not p)
- You deduce something absurd (false).
- Thus, the assumption "not p" cannot be true. Therefore, p needs to be true.

Example: there is no largest real number strictly smaller than 1.

negation: there is an $x \in \mathbb{R}$, $x<1$, that is the largest real number smaller than 1.

$\rightarrow$ Let's call this number M

$\rightarrow$ $M < 1$

$\forall x \in \mathbb{R}, x < 1 : x \leq M$

Consider $y = \frac{M+1}{2}$. Then $M<1 \Rightarrow M+M < 1+M$

$\Rightarrow M < \frac{1+M}{2}$

$M<1 \Rightarrow 1+M < 1+1$

$\Rightarrow \frac{1+M}{2} < 1$

So $M < y < 1$. Contradiction: M is not the largest number <1, since y is larger! $\lightning$ $\perp$

Proof by contrapositive

- You want to prove "if p, then q"
- Remember: $p \rightarrow q$ and $\neg q \rightarrow \neg p$ are equivalent.
- Instead, you prove "if not q, then not p"

Example: all prime numbers larger than 2 are odd

$(\forall x \in \mathbb{N}, x > 2)$: x prime $\rightarrow$ x is odd $\qquad p \rightarrow q$

$(\forall x \in \mathbb{N}, x > 2)$: x even $\rightarrow$ x is not prime $\qquad \neg q \rightarrow \neg p$

Proof : $\begin{cases} x > 2 \\ x \text{ even} \end{cases} \Rightarrow x = 2k,\ k \in \mathbb{N},\ k > 1$

$\hookrightarrow$ x has more than 2 divisors, namely 1, 2k, 2, k, ...

$\Rightarrow$ x is not prime QED $\blacksquare$

Example: $(\forall x,y \in \mathbb{R})(x,y > 0)(x^2+y^2 > 1 \Rightarrow x+y > 1)$

contrapositive: $(\forall x,y \in \mathbb{R})(x,y > 0)(x+y \leq 1 \Rightarrow x^2+y^2 \leq 1)$

Let $x,y \in \mathbb{R}$, $x,y > 0$

$$x+y \leq 1 \qquad \downarrow^{2}$$

$$\Rightarrow (x+y)^2 \leq 1^2$$

$$\Rightarrow x^2 + 2xy + y^2 \leq 1$$

$$\Rightarrow x^2 + \cancel{2xy} + y^2 - \cancel{2xy} \leq 1 - 2xy$$

$$\Rightarrow x^2 + y^2 \leq 1 - 2xy \quad \wedge \quad 1 - 2xy \leq 1$$

$$a \leq b \qquad\qquad 2xy \geqslant 0$$

$$b \leq c$$

$$\Rightarrow x^2+y^2 \leq 1$$

QED

Biconditional proof

- To prove "if and only if" theorems
- Recall: $p \leftrightarrow q$ is short for $(p \to q) \wedge (q \to p)$
- We prove "if p, then q" AND "if q, then p"

Example: $\forall x \in \mathbb{Z}$: x^2 is a multiple of 3 $\Leftrightarrow$ x is a multiple of 3

$\underline{\Leftarrow|}$ $\forall x \in \mathbb{Z}$: x is a multiple of 3 $\Rightarrow$ x^2 is a multiple of 3

x is a multiple of 3. Then $x = 3k$, for some $k \in \mathbb{Z}$

Then $x^2 = (3k)^2 = 9k^2 = 3(3k^2)$

(we write x^2 as $3 \cdot \underbrace{\text{something}}_{\in \mathbb{Z}}$)

$\Rightarrow$ x^2 is a multiple of 3

$\underline{\Rightarrow|}$ $\forall x \in \mathbb{Z}$: x^2 is a multiple of 3 $\Rightarrow$ x is a multiple of 3

contrapositive : $\forall x \in \mathbb{Z}$: x is NOT a multiple of 3 $\Rightarrow$ x^2 is NOT a multiple of 3

1	$1+3k$
2	$2+3k$
3	$3k$
4	$1+3k$
5	$2+3k$
6	$3k$
7	
$\vdots$	

$(k=0)$

Let $x \in \mathbb{Z}$, x is NOT a multiple of 3

then $x = 3k+1 \ \lor \ x = 3k+2$

- if $x = 3k+1$, then

$$x^2 = (3k+1)^2 = 9k^2 + 6k + 1$$
$$= 3(3k^2+2k) + 1$$

$\Rightarrow x^2$ is NOT a multiple of 3

- if $x = 3k+2$, then

$$x^2 = (3k+2)^2 = 9k^2 + 12k + 4$$
$$= 9k^2 + 12k + 3 + 1$$
$$= 3\underbrace{(3k^2+4k+1)}_{\in \mathbb{Z}} + 1$$

$\Rightarrow x^2$ is NOT a multiple of 3

$\hookrightarrow$ x is NOT a multiple of 3 $\Rightarrow$ x^2 is not a multiple of 3 $\blacksquare$

$\forall m \in \mathbb{N}, \forall n \in \mathbb{N} : m \cdot n$ is odd $\Longleftrightarrow$ m and n are odd

$\Leftarrow)$ $\forall m, n \in \mathbb{N} : m, n$ odd $\Rightarrow m \cdot n$ odd

Let $m, n \in \mathbb{N}$

$m = 2k+1$, then $m \cdot n = (2k+1)(2\ell+1) = \underbrace{4k\ell + 2k + 2\ell}_{2 \cdot \text{something} \in \mathbb{Z}} + 1$
$n = 2\ell+1$

$\Rightarrow m \cdot n$ is odd

$\Rightarrow)$ $\forall m, n \in \mathbb{N} : m \cdot n$ odd $\Rightarrow m$ and n odd

contrapositive : $\forall m, n \in \mathbb{N}$: m or n is even $\Rightarrow m \cdot n$ even

Let $m, n \in \mathbb{N}$

without loss of generality, assume $m = 2k$, $k \in \mathbb{Z}$.

Then $m \cdot n = 2kn$ is even. $\blacksquare$

Checklist (proofs)

- Do you understand why, if asked to prove something for all elements of a set, it is sufficient to start the proof by picking an arbitrary element?
- Do you understand why it is sufficient to disprove a "for all" statement to find a single counter-example?
- Are you comfortable proving statements of the form "if p, then q", by assuming p that is true, and showing that q follows?
- Do you know that to prove p <-> q, you need to prove both p->q and q->p?
- Are you comfortable using the different proof techniques (contrapositive, contradiction, disproof by counterexample, direct proof, biconditional)?