Proof Structure

- State theorem to be proved in symbolic form.
- Mark beginning with word "**Proof**:"
- Introduce initial variables and explain
  - what kind of objects they are (i.e. which set they belong to)
  - what other properties they have
- Proof body
  - start from assumptions (i.e. what is already known)
  - work step by step towards conclusion
  - justify every step with either an assumption, a previously derived step, an axiom, an already proved theorem, or a valid argument form.
- Conclusion - Mark end with **Q.E.D** (quod erat demonstrandum) or ∵

Cases with simple proofs

Proving Existential Statements of the form $\exists x \in D, P(x)$

1. **Find an example**

   E.g. Some prime is a sum of 2 other primes (use 7=5+2)

2. **Construct an example**.

   E.g. proof of the infinitude of $\mathbb{N}$ i.e. There is no largest natural number.

Proving Universal Statements of the Form $\forall x \in D, P(x)$

1. If **D** = ∅ then the statement is **vacuously true** (its negation, $\exists x \in \varnothing, \sim P(x)$, is false)

2. If D is a small set, you can use the **method of exhaustion**: prove that property is true for each element of the set one by one.

   E.g. every even integer between 4 and 20 can be written as the sum of two primes

Domain Change

Proving Universal Statements of the Form $\forall x \in D, P(x) \Rightarrow Q(x)$

Note that by domain change, this is the same as $\forall x \in \{y \in D \mid P(y)\}\ Q(x)$. Therefore, you can simply start your proof by assuming that x has the property P, and then prove that it also has the property Q.

General Proof Methods

1. **Direct proofs**: deduce conclusion from assumptions, axioms, lemmas, theorems and valid argument rules.

   E.g.: | is transitive.

2. **Proofs by division into cases**: if it is simpler to think of the whole problem as a collection of separate cases, prove the theorem in each of the cases, and conclude that it is true by the *division into cases*: $p \vee q,\ p \rightarrow r,\ q \rightarrow r\ \therefore\ r$.

   E.g. any two consecutive integers have opposite parity

3. **Proofs by contradiction**: assume that the theorem is false and show that it leads to a contradiction; conclude that the theorem must be true by the *rule of contradiction:* $\sim p \rightarrow c\ \therefore\ p$.

   E.g. If the square of an integer is even, then so is that integer.

4. **Proof by contraposition:** Note that an implication is equivalent to its contrapositive. Sometimes it is easier to prove the contrapositive.

   E.g. If the square of an integer is even, then so is that integer.

5. **Proofs by Induction**: see separate handout.

<u>Note that you may use more than one method in a proof.</u>

E.g. $\forall n,m \in \mathbb{N},\ m.n = 1 \Rightarrow m=1 \wedge n=1$ (contraposition and division into cases)

Methods for Disproving Statements

<u>Disproving Existential Statements of the form $\exists x \in D, P(x)$</u>

1. **Trivial case**: If $\mathbf{D = \varnothing}$ then the statement is **false**

2. The negation of an existential statement is a universal statement: disproving $\exists x \in D, P(x)$ is the same as proving $\forall x \in D, \sim P(x)$. Use techniques for proving universal statements.

<u>Disproving Universal Statements of the form $\forall x \in D, P(x)$</u>

The negation of a universal statement is an existential statement. Disproving $\forall x \in D, P(x)$ is the same as proving $\exists x \in D, \sim P(x)$.

Use techniques for proving existential statements. If you find an example of the negation of P(x) it is called a <u>counterexample</u>.

E.g. $\forall m,n \in \mathbb{Z},\ n^2 = m^2 \Rightarrow m=n$ has a counterexample of n=1, m=-1