In this section, we consider more methods and how to find appropriate strategies, when we prove mathematical theorems.

After this section, we will study **Mathematical induction**, which is an extremely useful method for proving statements of the form $\forall n P(n)$, whenever $D = \mathbb{N}$.

1. **Proof by Cases:**
   In order to prove a conditional statement of the form $(p_1 \lor p_2 \lor \cdots \lor p_n) \rightarrow q$, the tautology can be used as a rule of inference
   
   $$(p_1 \lor p_2 \lor \cdots \lor p_n) \rightarrow q \iff (p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \cdots \land (p_n \rightarrow q).$$

   Proving this rule each of the $n$ conditional statements $p_i \rightarrow q$ with $i = 1, 2, \cdots, n$ individually is called proof by cases.

2. **Exhaustive proof:**
   is to prove theorems by examining a relatively small number of examples. This is a special type of proof by cases.
Example 1

1. Use an exhaustive proof to prove that \((n + 1)^3 \geq 4^n\) if \(n\) is a positive integer with \(n \leq 3\).
2. Prove that \(n^2 \geq 2n\) for any integer \(n \geq 2\). Don’t use a proof by exhaustion.
3. Use a proof by cases to show that \(|xy| = |x||y|\).

Note that we can use **without loss of generality (WLOG)** to shorten the proof for #3 in the previous example. When the proof for a case can be easily applied to all others, or that all other cases are equivalent, we can use WLOG.
A proof of a proposition of the form $\exists x \, P(x)$ is called an existence proof.

1. **Constructive:** $\exists x \, P(x)$ is proved by finding an element $a$ called a witness such that $P(a)$ is true.

2. **Nonconstructive:** we do not find a witness $a$ directly. Instead of it, we use proof by contradiction.

---

**Example 2**

1. Show that there is a positive number that can be written as its square.
2. Show that $\exists x \in \mathbb{Q}^c$ and $\exists y \in \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.
3. Show that $\exists x \in \mathbb{Q}$ and $\exists y \in \mathbb{Q}^c$ such that $x^y \in \mathbb{Q}^c$. 

A uniqueness proof consists of two parts:

1. ∃: We show that ∃x with the desired property
2. !: We show that if both x and y have the desired property, x = y. Equivalently, if x ≠ y, they do not have the desired property.

Example3

1. Show that ∃!x such that ax + b = 0 for a ≠ 0, b ∈ ℝ
2. Show that if n is an odd integer, ∃!k ∈ ℤ such that n = (k − 2) + (k + 3).
Theorem

**FERMAT’S LAST THEOREM**

The equation $x^n + y^n = z^n$ has no solutions in integers $x \neq 0, y \neq 0, z \neq 0$, whenever $n$ is an integer with $n > 2$.

- In 17th century, FERMAT established his last theorem without proving. Since then, many mathematicians have tried to prove his last theorem. A correct proof was found by Andrew Wiles’s paper (over hundreds of pages) in the 1990s.

- There are still many open mathematical questions for pure mathematics and applied mathematics.