Proof Methods

- equational reasoning = likhetsresonemang
- inequational reasoning = olikhetsresonemang
- using a lemma = att använda en hjälpsats
- case splitting = falluppdelning
- proof by contradiction = motsägelsebevis
- simple induction = (enkel) induktion / första induktionsprincipen
- strong induction = stark induktion / andra induktionsprincipen

---

- structural induction = strukturell induktion
- proof by analogy = analogibevis

equational reasoning

to prove: $(x+y)(x-y) = x^2 - y^2$

proof:

$(x+y)(x-y)$

$= x^2 - xy + yx - y^2$ [expand]

$= x^2 - y^2$ [cross out -xy against xy]

□

Note: a clear way to show a proof by equational reasoning is to write each term on a separate line, with the reason why you made that step clearly indicated.

inequational reasoning

to prove: $1^1 + 2^2 + 3^3 + \dots + n^n \geq 2^{n+1} - 3$ for $n \geq 1$

proof:

$1^1 + 2^2 + 3^3 + \dots + n^n$

$\geq 1^1 + 2^2 + 2^3 + \dots + 2^n$ [each $a^k \geq 2^k$ for $a \geq 2$]

$= 1 + (2^{n+1} - 1 - 3)$ [geometric sum]

$= 2^{n+1} - 3$

□

Note: Again, put each term on a separate line, which are separated by =, and > and/or ≥, or < and/or ≤.

If all comparisons are = or ≥, you have shown that the first term ≥ the last term.
If all comparisons are = or ≤, you have shown that the first term ≤ the last term.
If all comparisons are = or ≥ and at least one is >, you have shown that the first term > the last term.
If all comparisons are = or ≤ and at least one is <, you have shown that the first term < the last term.
Don't mix ≤, ≥ or <, > in inequational reasoning proofs, because then they become meaningless.

using a lemma

to prove: For every natural number $n \geq 2$, there exists a prime number p such that $p \mid n$.

proof:

1. Every natural number n can be written as a product of prime numbers $p_1 \cdot \ldots \cdot p_k$. (By the Fundamental Theorem of Arithmetic)

2. Since $n \geq 2$, we know that $k \geq 1$.

3. Pick $p = p_1$. We know that $p \mid n$ because $p_1 \mid (p_1 \cdot \ldots \cdot p_k)$

---

case splitting

to prove: n^3 - n is divisable by 3, for all integers n.

proof: by case splitting (on the remainder of dividing n by 3)

case 1: n = 3k

$n^3 - n$

$= (3k)^3 - 3k$

$= 27k^3 - 3k$

$= 3(9k^3 - k)$, which is divisable by 3

case 2: n = 3k+1

$n^3 - n$

$= (3k+1)^3 - (3k+1)$

$= 27k^3 + 27k^2 + 9k + 1 - 3k - 1$

$= 3(9k^3 - 9k^2 + 2k)$, which is divisable by 3

case 3: n = 3k+2

$n^3 - n$

$= (3k+2)^3 - (3k+2)$

$= 27k^3 + 54k^2 + 12k + 8 - 3k - 2$

$= 3(9k^3 - 18k^2 + 3k + 2)$, which is divisable by 3

□

Note: When case splitting, we have to find cases that: (1) are covering all possible cases, (2) should (rather) not overlap. If we prove something in each case, then we have proved that for all cases, and thus it always holds.

proof by contradiction

to prove: $\sqrt{2}$ is not a rational number.

proof: by contradiction. Let's assume that $\sqrt{2}$ is a rational number.

1. Any rational number can be written as a/b, for natural numbers a and b that do not have any common divisors. (So, gcd(a,b) = 1.)

2. So, by our assumption, we have $\sqrt{2} = a/b$ and gcd(a,b) = 1.

3. Now look at:

$$\sqrt{2} = a/b$$

$$\Rightarrow \; 2 = a^2/b^2$$

$$\Rightarrow \; 2b^2 = a^2$$

This means that a is even, so we have a = 2c.

$$\Rightarrow \; 2b^2 = (2c)^2$$

$$\Rightarrow \; 2b^2 = 4c^2$$

$$\Rightarrow \; b^2 = 2c^2$$

This means that b is even.

4. So. a and b are both even, which contradicts that gcd(a,b) = 1!

5. We reached a contradiction, which means that our assumption that $\sqrt{2}$ is a rational number was wrong.

□

Note: Proof by contradiction is often a good idea to use when you are stuck and don't know how to continue. By assuming the negation of what you want to prove, you suddenly know a great deal of things. Now, all you have to do is find something that is "not right".

proof by simple induction

to prove: $1 + 2 + \ldots + n = n(n+1)/2$, for $n \geq 1$

proof: by induction on n

base case: $n = 1$

$1 + 2 + \ldots + n$

$= 1$

$= 1(1+1)/2$

$= n(n+1)/2$

step case: $n = k+1$, $k \geq 1$

1. By the induction hypothesis (I.H.), we know that $1 + 2 + \ldots + k = k(k+1)/2$

2. Now look at:

$1 + 2 + \ldots + n$

$= 1 + 2 + \ldots + k + (k+1)$

$= k(k+1)/2 + (k+1)$ [by the I.H.]

$= k(k+1)/2 + 2(k+1)/2$ [multiply by 2 and divide by 2]

$= (k(k+1) + 2(k+1))/2$

$= (k+2)(k+1)/2$

$= n(n+1)/2$

□

Note: Induction works just like case splitting! In induction, we also have several cases that together cover all cases (here, the base case covers $n=1$ and the step case covers $n \geq 2$).

The only difference is that we can make use of **more information** in the step case: We have the I.H.! The I.H. allows us to make use of earlier instances (for $k < n$) of what we are proving (for n).

In simple induction, we can only make use of **the previous instance**. So, if we are proving something for n ($= k+1$), we can make use of the fact that we have already proved it for $k = n-1$.

In strong induction, we can make use of **all previous instances**. So, if we are proving something for n in the step case, we can make use of the fact that we have already proved it **for all $k < n$**.

proof by strong induction

to prove: Every natural number $n \geq 2$ has some prime factorization.

proof: by strong induction on n.

base case: $n = 2$.

n is already a prime number, so we have a prime factorization.

step case: $n \geq 3$.

1. By the induction hypothesis (I.H.), we know that every natural number $2 \leq k < n$ has a prime factorization.

2. Case split.

    case 1: n is a prime number

    n is already a prime number, so we have a prime factorization.

    case 2: n is not a prime number

    1. In this case, we have $2 \leq a, b < n$ such that $n = a \cdot b$.

    2. By the I.H., we know that a has a prime factorization $p_1 \cdot \ldots \cdot p_k$.

    3. By the I.H., we also know that b has a prime factorization $q_1 \cdot \ldots \cdot q_m$.

    4. So, $$\begin{aligned} n &= a \cdot b \\ &= (p_1 \cdot \ldots \cdot p_k) \cdot (q_1 \cdot \ldots \cdot q_m) \\ &= p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_m \end{aligned}$$

    5. So, n also has a prime factorization

□

Note 1: See notes on simple induction.

Note 2: Many times a base case is actually not needed in strong induction. Look at case 1 in the step case and the base case; they look the same! An alternative, shorter, proof is given below.

proof by strong induction (variant 2)

to prove: Every natural number $n \geq 2$ has some prime factorization.

proof: by strong induction on n.

step case: $n \geq 2$.

1. By the induction hypothesis (I.H.), we know that every natural number $2 \leq k < n$ has a prime factorization. [**Note:** When $n = 2$, we can not use the I.H., because there are no $2 \leq k < n$!]

2. Case split.

case 1: n is a prime number

n is already a prime number, so we have a prime factorization.

case 2: n is not a prime number

1. In this case, we have $2 \leq a, b < n$ such that $n = a \cdot b$.

2. By the I.H., we know that a has a prime factorization $p_1 \cdot \ldots \cdot p_k$.

3. By the I.H., we also know that b has a prime factorization $q_1 \cdot \ldots \cdot q_m$.

4. So,
$$\begin{aligned} n &= a \cdot b \\ &= (p_1 \cdot \ldots \cdot p_k) \cdot (q_1 \cdot \ldots \cdot q_m) \\ &= p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_m \end{aligned}$$

5. So, n also has a prime factorization

□