19 Basic proof techniques

19.1 Proofs by contradiction

Example 150. $\sqrt{5}$ is not rational.

Proof. Assume (for contradiction) that we can write $\sqrt{5} = \frac{n}{m}$ with $n, m \in \mathbb{N}$. By canceling common factors, we can ensure that this fraction is reduced.
Then $5m^2 = n^2$, from which we conclude that n is divisible by 5. Write $n = 5k$ for some $k \in \mathbb{N}$. Then $5m^2 = (5k)^2$ implies that $m^2 = 5k^2$. Hence, m is also divisible by 5. This contradicts the fact that the fraction n/m is reduced. Hence, our initial assumption must have been wrong. □

Variations. Does the same proof apply to, say, $\sqrt{7}$? Which step of the proof fails for $\sqrt{4}$?

19.2 A famous example of a direct proof

Example 151. (Gauss) $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$

Proof. Write $s(n) = 1 + 2 + \ldots + n$.
$2s(n) = (1 + 2 + \ldots + n) + (n + (n-1) + \ldots + 1) = (1+n) + (2+n-1) + \ldots + (n+1) = n \cdot (n+1)$. Done! □

Anecdote. 9 year old Gauss (1777-1855) and his classmates were tasked to add the numbers 1 to 100 (and not bother their teacher while doing so). Gauss was not writing much on his slate... just the final answer: 5050.

19.3 Proofs by induction

(induction) To prove that $\mathrm{CLAIM}(n)$ is true for all integers $n \geqslant n_0$, it suffices to show:

- **(base case)** $\mathrm{CLAIM}(n_0)$ is true.
- **(induction step)** If $\mathrm{CLAIM}(n)$ is true for some n, then $\mathrm{CLAIM}(n+1)$ is true as well.
  [We may even assume that $\mathrm{CLAIM}(n_0), \mathrm{CLAIM}(n_0+1), \ldots, \mathrm{CLAIM}(n)$ are all true.]

Why does this work? By the base case, $\mathrm{CLAIM}(n_0)$ is true. Thus, by the induction step, $\mathrm{CLAIM}(n_0+1)$ is true. Applying the induction step again shows that $\mathrm{CLAIM}(n_0+2)$ is true, ...

Example 152. (Gauss, again) For all integers $n \geqslant 1$, $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Proof. Again, write $s(n) = 1 + 2 + \ldots + n$.
$\mathrm{CLAIM}(n)$ is that $s(n) = \frac{n(n+1)}{2}$.

- **(base case)** $\mathrm{CLAIM}(1)$ is that $s(1) = \frac{1(1+1)}{2} = 1$. That's true.
- **(induction step)** Assume that $\mathrm{CLAIM}(n)$ is true (the **induction hypothesis**).

$$s(n+1) = s(n) + (n+1) = \underbrace{\frac{n(n+1)}{2}}_{\substack{\text{this is where we use} \\ \text{the induction hypothesis}}} + (n+1) = \frac{(n+1)(n+2)}{2}$$

This shows that $\mathrm{CLAIM}(n+1)$ is true as well.

By induction, the formula is therefore true for all integers $n \geqslant 1$. □

Comment. The claim is also true for $n = 0$ (if we interpret the left-hand side correctly).

Example 153. Induction is not only a proof technique but also a common way to define things.

- The **factorial** $n!$ can be defined inductively (i.e. recursively) by

$$0! = 1, \quad (n+1)! = n! \cdot (n+1).$$

Comment. This may not seem impressive, because we can "spell out" $n! = 1 \cdot 2 \cdot 3 \cdots (n-1)n$ directly.

- The **Fibonacci numbers** F_n are defined inductively (i.e. recursively) by

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+1} = F_n + F_{n-1}.$$

Getting a feeling. $F_2 = F_1 + F_0 = 1$, $F_3 = F_2 + F_1 = 2$, $F_4 = 3$, $F_5 = 5$, $F_6 = 8$, $F_7 = 13$, ...

Comment. Though not at all obvious, there is a way to compute F_n directly. Let $\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618$. Then $F_n = \lfloor \varphi^n / \sqrt{5} \rfloor$. Try it! For instance, $\varphi^{10}/\sqrt{5} \approx 55.0036$. That seems like magic at first. But it is the beginning of a general theory (look up, for instance, Binet's formula and C-finite sequences). Also, recall that we observed that F_{n+1}/F_n are the convergents of the continued fraction for φ.

Example 154. Let us prove that $F_n < 2^n$ for all integers $n \geqslant 0$.

Getting a feeling. $0 < 1$, $1 < 2$, $1 < 4$, $2 < 8$, $3 < 16$, $5 < 32$, $8 < 64$ (seems like the claim is "very" true)

Note that our observation from continued fractions implies that $\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \varphi \approx 1.618$.
In other words, F_n is indeed growing exponentially (but $1.618 < 2$)!
(In particular, say, $F_n > n^{1000}$ for large enough n, so we should be careful only looking at the first few cases.)

Proof.

- base cases: $F_0 = 0 < 2^0 = 1$, $F_1 = 1 < 2^1 = 2$.
- induction step: suppose that $F_m < 2^m$ for all integers $m \in \{1, 2, ..., n\}$. (strong induction!)
  We need to show that $F_{n+1} < 2^{n+1}$.
  $F_{n+1} = F_n + F_{n-1} <^{(\mathrm{IH})} 2^n + 2^{n-1} < 2^n + 2^n = 2^{n+1}$ □

Important note. Why was it necessary to consider two base cases?

Example 155. (sum of squares) For all integers $n \geqslant 1$, $1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Proof. Write $t(n) = 1^2 + 2^2 + ... + n^2$.
We use induction on the claim $t(n) = \frac{n(n+1)(2n+1)}{6}$.

- The base case $(n = 1)$ is that $t(1) = 1$. That's true.
- For the inductive step, assume the formula holds for some value of n.
  We need to show the formula also holds for $n+1$.

$$\begin{aligned} t(n+1) &= t(n) + (n+1)^2 \\ \text{(using the induction hypothesis)} &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n+1)}{6}[2n^2 + n + 6n + 6] \\ &= \frac{(n+1)}{6}(n+2)(2n+3) \end{aligned}$$

  This shows that the formula also holds for $n+1$.

By induction, the formula is true for all integers $n \geqslant 1$. □

Example 156. Observe the following connection with our sums and integrals from calculus:

- $\int_0^n x\mathrm{d}x = \frac{n^2}{2}$ versus $\sum_{x=0}^{n} x = 1+2+\ldots+n = \frac{n(n+1)}{2} = \frac{n^2}{2} + \text{lower order terms}$
- $\int_0^n x^2\mathrm{d}x = \frac{n^3}{3}$ versus $\sum_{x=0}^{n} x^2 = 1^2+2^2+\ldots+n^2 = \frac{n(n+1)(2n+1)}{6} = \frac{n^3}{3} + \text{lower order terms}$
- $\int_0^n x^3\mathrm{d}x = \frac{n^4}{4}$ versus $\sum_{x=0}^{n} x^3 = 1^3+2^3+\ldots+n^3 = \left[\frac{n(n+1)}{2}\right]^2 = \frac{n^4}{4} + \text{lower order terms}$

The connection makes sense: the integrals give areas below curves, and the sums are approximations to these areas (rectangles of width 1).

Example 157. There are irrational numbers x and y such that x^y is rational.

Proof. Let $x=\sqrt{2}$ and $y=\sqrt{2}$ (which are both irrational). There is two possibilities:

- $\sqrt{2}^{\sqrt{2}}$ is rational. In that case, we can take $x=\sqrt{2}$ and $y=\sqrt{2}$, and are done.
- $\sqrt{2}^{\sqrt{2}}$ is irrational. In that case, we can take $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$.
  (Note that $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$ is rational.) □

Note. We have proved that there are irrational numbers x and y such that x^y is rational. Yet, in our argument, we have not produced a single example that we are sure about!
Logically, we used the **law of the excluded middle**.

In fact, $\sqrt{2}^{\sqrt{2}}$ is irrational (even transcendental) but this is much harder to prove.

See, for instance: http://math.stackexchange.com/questions/446647/irrationality-of-sqrt2-sqrt2

Example 158. ("all horses have the same color") We will prove that all horses are the same color.

"Proof". We will prove by induction that, in any group of n horses, they all have the same color.

- The base case $(n=1)$ of groups of 1 horse is trivially true.
- For the induction step, we assume that (for fixed n), in any group of n horses, they all have the same color. We will show that, in any group of $n+1$ horses, they also all have the same color.
  Line up your $n+1$ horses. The first n horses all have the same color by the induction hypothesis.
  Also, the last n horses all have the same color by the induction hypothesis.
  So, the first horse has the same color as the horses in the middle, and these have the same color as the last horse. Hence, all $n+1$ of them have the same color.

What's wrong? We are talking about "horses in the middle". This is no problem for $\geqslant 3$ many horses, but there is no middle horses for 2 horses. The induction step argument does not apply if $n=1$.

Comment. There is a wikipedia entry with the title "all horses have the same color". Using that language, this "paradox" is due to George Pólya.