Topic: proof techniques

3.1 (Counterexamples)**.** Using a counterexample, show that each of the following statements is False.

(a) Every natural number can be written as the sum of two perfect squares.

(b) Every quadrilateral with perpendicular diagonals has equal sides.

(c) If $f : \mathbf{R} \longrightarrow \mathbf{R}$ is continuous at $x = 0$, then f is differentiable at $x = 0$.

Note: a correct solution requires a **specific** counterexample for each statement.

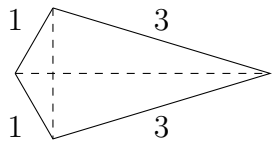
Solution.

(a) The natural number $n = 3$ cannot be expressed as a sum of two perfect squares: since perfect squares are non-negative integers, we look at all the possible ways of writing 3 as a sum of two non-negative integers:

$$3 = 3 + 0 = 2 + 1.$$

In the first one 3 is not a perfect square, and in the second one 2 is not a perfect square. Therefore 3 cannot be expressed as the sum of two perfect squares.

(b) Consider the quadrilateral



Since this quadrilateral has perpendicular diagonals but unequal sides, the claim is False. This quadrilateral is called a kite. In general, a *kite* is a quadrilateral with the following properties:

i. It has two pairs of adjacent sides that are equal, i.e., $AB = AD$ and $BC = CD$, where the equal sides are next to each other.

ii. Its diagonals are perpendicular, i.e., $AC \perp BD$.

iii. One of the diagonals acts as a line of symmetry, dividing the kite into two congruent triangles.

(c) $f(x) = |x|$ is continuous, but not differentiable at $x = 0$. Therefore the claim is False. □

3.2 (Existence proofs)**.** Express each of the following in the language of formal logic. Then provide a proof for each statement.

(a) Some integer q satisfies $2q^2 - 9q = 5$.

(b) There is a natural number one more than a perfect square and one less than a perfect cube.

Note: a correct solution requires a **specific** example for each statement.

Solution.

(a) $(\exists q \in \mathbf{Z})\ 2q^2 - 9q = 5$ is True when $q = 5$.

(b) $(\exists p, q, r \in \mathbf{N})\ p = q^2 + 1 \wedge p = r^3 - 1$ is True when $p = 26$ $(q = 5, r = 3)$. □

3.3 (An integer is even if and only if its square is even)**.** In Theorem 1.36 we proved:

"Let x be an integer. If x is even, then x^2 is even."

(a) Write out the converse of the above statement.

(b) Write out the contrapositive of your statement from (a).

(c) Prove your statement from (b) with a direct proof.

(d) Using your work from parts (a)–(c) and the fact that

$$(p \Leftrightarrow q) \equiv [(p \Rightarrow q) \wedge (\neg p \Rightarrow \neg q)],$$

convince yourselves that the following statement is True

"An integer x is even if and only if x^2 is even."

Solution.

(a) Let x be an integer. If x^2 is even, then x is even.

(b) Let x be an integer. If x is odd, then x^2 is odd.

(c) Assume x is odd. Then there exists $k \in \mathbf{Z}$ so that $x = 2k + 1$. Squaring we find

$$x^2 = 4k^2 + 4k + 1 = 2(2k^2 + k) + 1.$$

Therefore x^2 is odd.

(d) Let $r(x)$ be the condition "x is even". Let $s(x)$ be the condition "x^2 is even".

From Theorem 1.36 we know that $r(x) \Rightarrow s(x)$ is True. From part (c) we have $\neg r(x) \Rightarrow \neg s(x)$. Since $(p \Leftrightarrow q) \equiv [(p \Rightarrow q) \wedge (\neg p \Rightarrow \neg q)]$ it follows that $r(x) \Leftrightarrow s(x)$ is True for every $x \in \mathbf{Z}$. □

3.4 (The square root of 2 is irrational)**.** We want to prove that $\sqrt{2} \notin \mathbf{Q}$. As this is stated, it supposes that we know what $\sqrt{2}$ is and where it belongs, namely the real numbers $\mathbf{R}$. Of course we do know this, but we have not yet proved it in this subject.

To avoid this issue, we can rewrite our statement as: "$(\forall x \in \mathbf{Q}) x^2 \neq 2$." This is what we prove now.

(a) Fill in the blanks in the proof below. When you are done, have one group member read the sentences aloud one at a time. Do not proceed to the next sentence until every group member can explain why the sentence is true.

Claim: $(\forall x \in \mathbf{Q}) x^2 \neq 2$.

Proof: We proceed by contradiction. That is, we assume _____

In other words, there exist $a, b \in \mathbf{Z}$, so that $x = a/b$ with a/b a fraction in lowest terms, and $2 = x^2 = \frac{a^2}{b^2}$.

Rearranging, we have $a^2 = 2b^2$. Therefore a^2 is even. By _____, it then follows a is even.

Since a is even, there exists $k \in \mathbf{Z}$ so that _____. Therefore $a^2 = 4k^2$. Since $a^2 = 2b^2$, it then follows that $b^2 = 2k^2$. Therefore b^2 is even.

By Tutorial Question 3.3, it then follows that b is _____. Since a and b are both even, a/b is **not** _____. This contradicts our assumption that _____.

(b) One can use the method above to prove $\sqrt{p}$ is irrational for any prime number p. If you were to do so, what result would you first have to prove? [**Hint**: Trying re-writing the proof above for $\sqrt{3}$ instead of $\sqrt{2}$ and see what needs to change.]

Solution.

(a) We proceed by contradiction. That is, we assume $(\exists x \in \mathbf{Q}) x^2 = 2$.

In other words, there exist $a, b \in \mathbf{Z}$, so that $x = a/b$ with a/b a fraction in lowest terms, and $2 = x^2 = \frac{a^2}{b^2}$.

Rearranging, we have $a^2 = 2b^2$. Therefore a^2 is even. By Tutorial Question 3.3, it then follows a is even.

Since a is even, there exists $k \in \mathbf{Z}$ so that $a = 2k$. Therefore $a^2 = 4k^2$. Since $a^2 = 2b^2$, it then follows that $b^2 = 2k^2$. Therefore b^2 is even.

By Tutorial Question 3.3, it then follows that b is even. Since a and b are both even, a/b is **not** a fraction in lowest terms. This contradicts our assumption that a/b is a fraction in lowest terms.

(b) One would need to prove the following statement:

"Let p be a prime number and x be an integer. If x^2 is divisible by p, then x is divisible by p." □

3.5 (Peirce's Law and Curry's Paradox)**.** We look at a simple identity due to philosopher Charles Peirce (1839–1914). An odd consequence is Curry's Paradox, discovered by logician Haskell Curry (1900–1982). This paradox arises when we allow **self-reference**.

Before we start: *modus ponens* is a rule of deduction that says "if $p \Rightarrow q$ is True and p is True then q is True". (You can check that this is valid by staring at the truth table for $\Rightarrow$.)

You may find modus ponens useful in the following questions.

(a) Using truth tables, show that *Peirce's Law*

$$[(p \Rightarrow q) \Rightarrow p] \Rightarrow p$$

is a tautology.

(b) Suppose that $(p \Rightarrow q) \Leftrightarrow p$ is True. Use part (a) to deduce that q is True.

(c) Argue informally that, for any statement q, the self-referential statement

$$p: \text{ "If } p \text{ is True, then } p \text{ implies } q\text{"}$$

satisfies $(p \Rightarrow q) \Leftrightarrow p$.

(d) Use (b) and (c) to conclude that anything is True. What has gone wrong?

Solution.

(a) Here is the truth table:

p	q	$p \Rightarrow q$	$(p \Rightarrow q) \Rightarrow p$	$[(p \Rightarrow q) \Rightarrow p] \Rightarrow p$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	F	T

Since all entries in the last column of the truth table are T, the formula is a tautology.

(b) If $(p \Rightarrow q) \Leftrightarrow p$ is True, then in particular $(p \Rightarrow q) \Rightarrow p$ is True. Applying modus ponens to the tautology in (a), we obtain that p is True. Now, $(p \Rightarrow q) \Leftrightarrow p$ being True also implies that $p \Rightarrow (p \Rightarrow q)$ is True. Since p is True, using modus ponens twice gives q.

(c) Note that the given statement p is saying "$p \Rightarrow (p \Rightarrow q)$". We want to prove that $(p \Rightarrow q) \Leftrightarrow p$.

In one direction, suppose p is True. Therefore $p \Rightarrow (p \Rightarrow q)$ is True, and by modus ponens we have that $p \Rightarrow q$ is True, which is what we wanted to prove.

In the other direction, suppose $p \Rightarrow q$ is True. Then $p \Rightarrow (p \Rightarrow q)$ is True. But this is precisely the definition of p, so p is True, which is what we wanted to prove.

(d) It follows immediately from (b) and (c) that q is True for any statement q! If q is a falsehood (e.g. $1 = 0$), we clearly have a paradox. The problem is the self-reference in p. Since statements in propositional logic must be built out of simpler (primitive) statements, they cannot refer to themselves, thereby preventing Curry's paradox. □

Topic: proofs by mathematical induction

3.6 (Proof reading)**.** Consider the following claim and the following proof.

Claim: The largest natural number is 1.

Proof. Let N be the largest natural number.

Therefore for every $n \in \mathbf{N}$ we have $N \geqslant n$. Since $1 \in \mathbf{N}$, we know $N \geqslant 1$. And since $N^2 \in \mathbf{N}$, we know $N \geqslant N^2$. Therefore $N^2 - N \leqslant 0$. So $N(N-1) \leqslant 0$. Thus $N - 1 \leqslant 0$, meaning that $N \leqslant 1$. We conclude that $N = 1$. □

The claim is False, but all of the logical steps in the proof seem to be reasonable? Explain.

Solution. Let p be the statement "There is a largest integer."

Let q be the statement "The largest integer is 1."

The proof shows that the statement $p \Rightarrow q$ is True. Unfortunately, knowing that $p \Rightarrow q$ is True tells us nothing about the truth values of the individual statements p and q. In this case, both p and q are False.

The first line of the proof pre-supposes the existence of a largest integer, a False statement. □

3.7 (Mathematical induction)**.** Using proofs by induction, prove the following statements:

(a) $(\forall n \in \mathbf{N}) \quad 0^3 + 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$;

(b) $n^2 \leqslant n!$ whenever $n \geqslant 4$.

Solution.

(a) Let $p(n)$ be the condition

$$0^3 + 1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2.$$

We prove that $(\forall n \in \mathrm{N})p(n)$ by induction on $n \geqslant 0$.

Base case: Show that $p(0)$ is True.

For $n = 0$, both sides of the equation are zero, as $0^3 = \frac{1}{4}0^2(0+1)^2$.

Induction step: Show that for each $k \in \mathbf{N}$, $p(k) \Rightarrow p(k+1)$.

Fix $k \in \mathbf{N}$ and suppose that $p(k)$ is True, in other words

$$0^3 + 1^3 + 2^3 + \cdots + k^3 = \frac{1}{4}k^2(k+1)^2.$$

Algebraically we manipulate:

$$\begin{aligned} 0^3 + 1^3 + 2^3 + \cdots + k^3 + (k+1)^3 &= \frac{1}{4}k^2(k+1)^2 + (k+1)^3 \qquad \text{(since } p(k) \text{ is True)} \\ &= \frac{1}{4}(k+1)^2(k^2+4k+4) \\ &= \frac{1}{4}(k+1)^2(k+2)^2 \\ &= \frac{1}{4}(k+1)^2\big((k+1)+1\big)^2. \end{aligned}$$

Therefore, $p(k+1)$ is True.

By the Principle of Mathematical Induction, $p(n)$ is True for all $n \in \mathbf{N}$.

(b) Let $p(n)$ be the condition: $n^2 \leqslant n!$. We prove that $(\forall n \geqslant 4)p(n)$ by induction on $n \geqslant 4$.

Base case: Show that $p(4)$ is True.

For $n = 4$, we have $4^2 = 16 < 24 = 4!$. Thus, $p(4)$ is True.

Induction step: Show that for each $k \geqslant 4$, $p(k) \Rightarrow p(k+1)$.

Fix an integer $k \geqslant 4$ and suppose that $p(k)$ is True, that is $k^2 \leqslant k!$.

Algebraically we manipulate (using $k \geqslant 4$):

$$\begin{aligned}(k+1)! = (k+1)k! &\geqslant (k+1)k^2 && \text{(since } p(k) \text{ is True and } k+1 > 0)\\ &\geqslant (k+1)2k = (k+1)(k+k)\\ &\geqslant (k+1)(k+1) = (k+1)^2.\end{aligned}$$

Therefore $p(k+1)$ is True.

By the Principle of Mathematical Induction, $p(n)$ is True for all $n \geqslant 4$. □

3.8 (Powers of i)**.** Using the fact that $i^2 = -1$ and a proof by induction, show that for all $n \geqslant 0$ we have

$$\begin{aligned}i^{4n+1} &= i\\ i^{4n+2} &= -1\\ i^{4n+3} &= -i\\ i^{4n+4} &= 1.\end{aligned}$$

Solution. Let $p(n)$ be the condition

$$(i^{4n+1} = i) \quad \wedge \quad (i^{4n+2} = -1) \quad \wedge \quad (i^{4n+3} = -i) \quad \wedge \quad (i^{4n+4} = 1).$$

We prove that $(\forall n \in \mathbf{N})p(n)$ by induction on $n \geqslant 0$.

Base case: Show that $p(0)$ is true.

We compute

$$\begin{aligned}i^{4(0)+1} &= i\\ i^{4(0)+2} &= i^2 = -1\\ i^{4(0)+3} &= i^3 = i^2 \cdot i = -i\\ i^{4(0)+4} &= i^2 \cdot i^2 = 1.\end{aligned}$$

Therefore $p(0)$ is True.

Induction step: Show that for each $k \in \mathbf{N}$, $p(k) \Rightarrow p(k+1)$.

Let $k \in \mathbf{N}$ and suppose that $p(k)$ is True. That is, assume the following equalities hold:

$$\begin{aligned}i^{4k+1} &= i\\ i^{4k+2} &= -1\\ i^{4k+3} &= -i\\ i^{4k+4} &= 1.\end{aligned}$$

By algebraic manipulation we get:

$$\begin{aligned}i^{4(k+1)+1} &= i^{4k+1+4} = i^{4k+1}i^4 = i \cdot 1 = i\\ i^{4(k+1)+2} &= i^{4k+2+4} = i^{4k+2}i^4 = -1 \cdot 1 = -1\\ i^{4(k+1)+3} &= i^{4k+3+4} = i^{4k+3}i^4 = -i \cdot 1 = i\\ i^{4(k+1)+4} &= i^{4k+4+4} = i^{4k+4}i^4 = 1 \cdot 1 = 1.\end{aligned}$$

Therefore $p(k+1)$ is True.

By the Principle of Mathematical Induction, $p(n)$ is True for all $n \in \mathbf{N}$. □

3.9 (Fibonacci numbers)**.** The *Fibonacci sequence* starts with 0 and 1 and proceeds so that each subsequent number is the sum of the previous two:

$$0, 1, 1, 2, 3, 5, 8, 13, 21 \ldots$$

The elements of this sequence are called *Fibonacci numbers*.

The sequence is named after the Italian mathematician Leonardo Bonacci, who included it as an example in his 1202 textbook **Liber Abaci** (**Book of Calculation**). Among other things, the book popularised the use of the Indo-Arabic numeral system in the Western world.

However, Fibonacci was certainly not the first to study the above sequence of numbers. References to it appear as far back as India in 200 BCE, when an Indian author named Pingala used these numbers to count the number of fixed-length music patterns that could be made using short and long syllables. Pingala's work on short and long syllable sequences can be seen as an early form of binary notation. Unfortunately, as is very often the case in mathematics, the name commonly attached to an object is that of a person who rediscovered or popularised it, rather than those who studied it earlier.

For $n \geqslant 0$, let f_n denote the n-th Fibonacci number: $f_0 = 0, f_1 = f_2 = 1, f_3 = 2, \ldots$. By definition we have $f_n = f_{n-1} + f_{n-2}$ for all $n \geqslant 2$.

Using a proof by strong induction prove that

$$f_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n$$

for all $n \geqslant 0$.

Solution. For any $n \geqslant 0$, let

$$g_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2} \right)^n.$$

Let $p(n)$ be the condition: $f_n = g_n$.

We prove that $p(n)$ is True for all $n \in \mathbf{N}$ by strong induction on $n \geqslant 0$.

Base case: Show that $p(0)$ is True.

We compute

$$f_0 = 0 = g_0$$
$$f_1 = 1 = g_1.$$

Induction step: Show that for each $k \in \mathbf{N}$, $p(k) \Rightarrow p(k+1)$.

Let $k \in \mathbf{N}$ and suppose that for all $\ell \in \{0, 1, \ldots, k\}$ we have $f_\ell = g_\ell$.

By definition of the Fibonacci numbers we have

$$f_{k+1} = f_{k-1} + f_k.$$

Since $k, k-1 \in \{0, 1, 2, \ldots, k\}$, the induction hypothesis gives $f_{k-1} = g_{k-1}$ and $f_k = g_k$.

Algebraically, we get that

$$\begin{aligned} f_{k+1} &= f_{k-1} + f_k = g_{k-1} + g_k \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1} + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k} \\ &= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k+1} = g_{k+1}, \end{aligned}$$

where we made use of

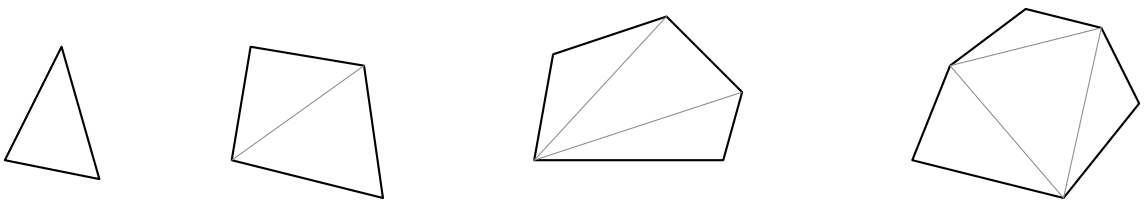
$$1 + \frac{1+\sqrt{5}}{2} = \frac{3+\sqrt{5}}{2} = \left(\frac{1+\sqrt{5}}{2}\right)^2 \quad \text{and} \quad 1 + \frac{1-\sqrt{5}}{2} = \frac{3-\sqrt{5}}{2} = \left(\frac{1-\sqrt{5}}{2}\right)^2.$$

Therefore $f_{k+1} = g_{k+1}$.

The result now follows from the Principle of Strong Mathematical Induction. □

3.10 (Dividing polygons)**.** Let $n \geqslant 3$ be an integer.

Consider the process of *triangulating* a convex polygon with n sides, that is dividing it fully into triangular regions by means of non-intersecting lines from vertex to non-adjacent vertex. For example here are some triangulated convex polygons with $n = 3, 4, 5, 6$ sides:



(Can't remember what a *convex* polygon is? Google it...)

(a) Looking at the above examples (and working out a few more if you need them), guess a formula for the number of regions in a triangulated convex polygon with n sides.

(b) Prove that your formula is correct using a proof by induction. You may use without proof the fact that a single line splits a convex polygon into two convex polygons (with fewer sides).

(c) (highly optional)

Explore what happens if we drop the convexity condition and allow polygons that are concave. First note that not all choices of lines will give you triangulations (some lines may be passing on the outside of the polygon, so they are not actually dividing the polygon).

Does your proof in (b) still work in this setting?

If not, does your formula in (a) still work in this setting?

(Can you see why these two questions could have different answers?)

Solution.

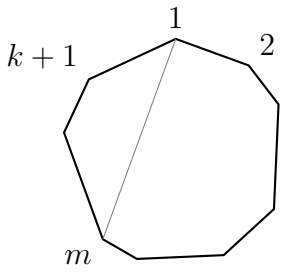
(a) Staring at the examples given, one could guess that the number R_n of regions in a triangulated convex n-gon is $R_n = n - 2$.

(b) We use strong induction to prove the statement: for all $n \geqslant 3$, any triangulated convex polygon with n sides has $n-2$ regions.

Base case: $n = 3$. This is a trivial case as there are no pairs of non-adjacent vertices; the polygon is already triangulated, and there is a single region, the polygon itself.

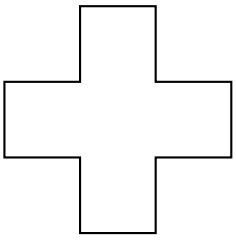
Induction step: Fix $k \geqslant 3$ and assume that the formula holds for all triangulated convex polygons with ℓ sides, where $3 \leqslant \ell \leqslant k$.

Consider a triangulated convex polygon with $k+1$ sides. Choose any line in the triangulation; it joins two non-adjacent vertices. Label one of these vertices 1, then label all the other vertices of the polygon consecutively from here, say clockwise. The other vertex on the line we picked has a label m, where $3 \leqslant m \leqslant k$.



The line therefore cuts our $(k+1)$-gon into an m-gon and a $(k+3-m)$-gon. Both are convex by the fact we were told to assume. Since $3 \leqslant m \leqslant k$ and $3 \leqslant k+3-m \leqslant k$, the induction hypothesis tells us that the number of regions in the m-gon is $m-2$, and the number of regions in the $(k+3-m)$-gon is $k+1-m$. Therefore the number of regions in our $(k+1)$-gon is the sum of these: $m-2+k+1-m = (k+1)-2$, as claimed.

(c) Here is a good example of wacky behaviour. Consider the concave polygon that appears on the Swiss flag:



Find a triangulation of this polygon that has 10 regions (hint: first break it into the 5 obvious squares, then cut each square diagonally), and another triangulation with 8 regions (hint: pick one of the four vertices where the interior angle is $3\pi/2$ and draw interior lines from it to all the vertices you see).

The conclusion is that the formula in part (a) does not hold (since it only depends on the number of sides, not on the triangulation itself). Therefore the proof in part (b) cannot be valid.

Revision: This actually just shows that we do not have the correct definition of triangulation – it works fine for a convex polygon, but is not well-behaved for a non-convex polygon, as the example above shows.

Numerically, the triangulation with 10 regions satisfies the formula we found in the convex case, and the one with 8 regions does not. If you stare at the one with 8

regions, you notice that it is not *maximal*: it is possible to draw a couple more interior non-intersecting lines between non-adjacent vertices.

This suggests that the correct general definition of a triangulation should insist on maximality: a triangulation is a division of the polygon into triangular regions by means of non-intersecting interior lines from vertex to non-adjacent vertex, in such a way that no further such lines can be added.

Using this definition, the number of regions for an n-gon (whether convex or not) is $n-2$. The proof is identical to the proof in part (b), except that we can ignore convexity altogether. □