

# Problematic Proofs

Kevin Buzzard, Imperial College London

Mechanisation and Mathematical Research, Leiden, 16/9/25

## Before I start

Thank you very much to the organisers for giving me this opportunity to speak.

I was asked to “talk about proof” (although I’m not an expert).

I will tell you my perception of what proofs currently are in practice, and then speak about my vision of what they could be.

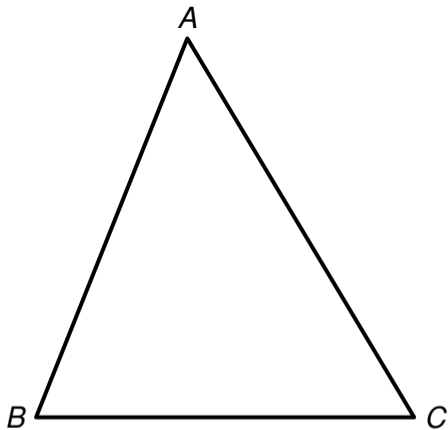
Thanks to Emily for setting the scene yesterday.

# Introduction to proof

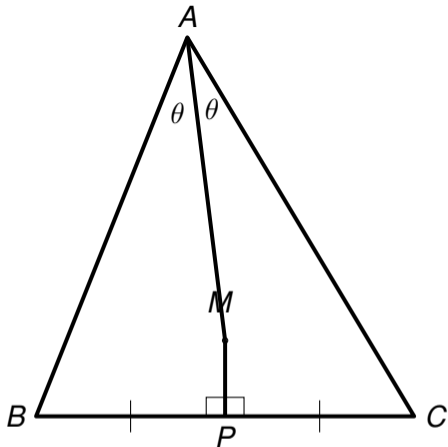
I'm a professor in the maths department at Imperial College London, and I have taught our "Introduction to proof" course around ten times.

The students are fresh from high school, so the only proofs which you can guarantee that they've seen are triangle and circle theorems.

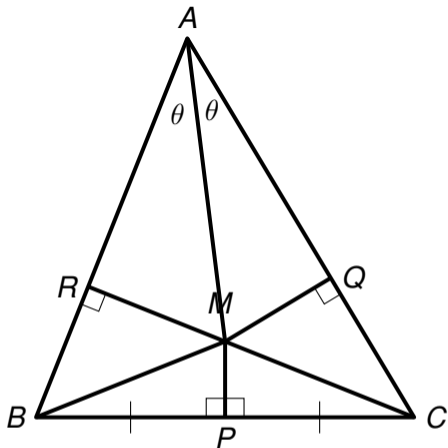
Here's the first proof that I show to these students.



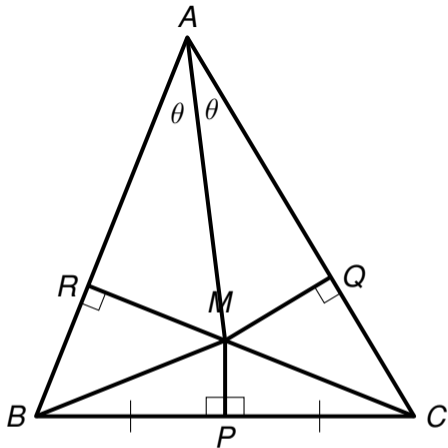
Let  $ABC$  be any triangle.



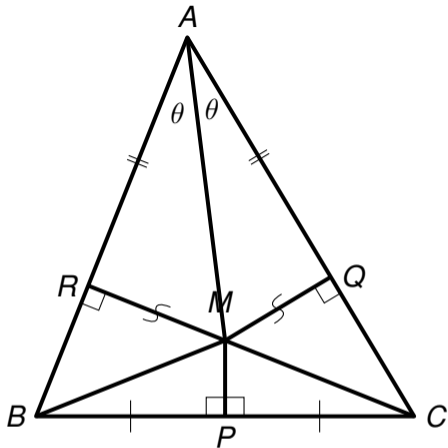
Let  $M$  be the point where the angle bisector of  $A$  meets the perpendicular bisector of  $BC$ .



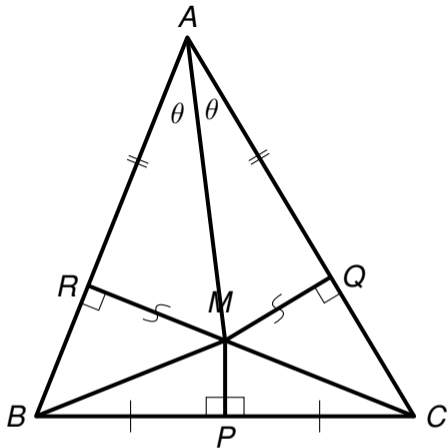
Draw  $MB$  and  $MC$ , and drop perpendiculars from  $M$  to  $AB$  and  $AC$ .



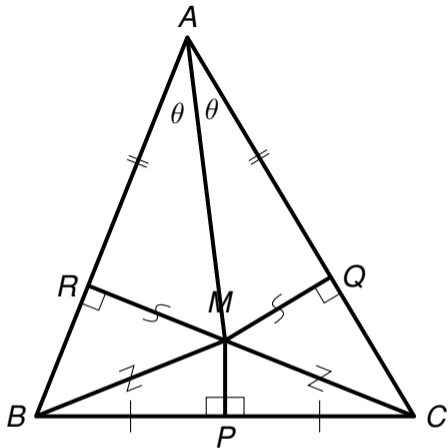
The triangles  $ARM$  and  $AQM$  are congruent, because all their angles are equal, and they share the side  $AM$ .



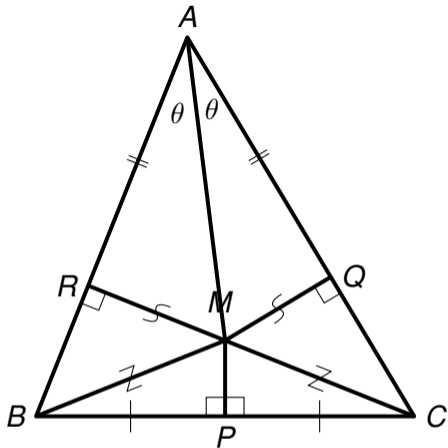
The triangles  $ARM$  and  $AQM$  are congruent, because all their angles are equal, and they share the side  $AM$ . Hence  $AR = AQ$  and  $RM = QM$ .



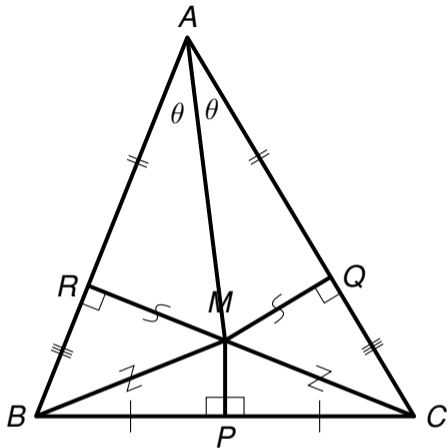
The triangles  $BPM$  and  $CPM$  are congruent, by two sides and included angle.



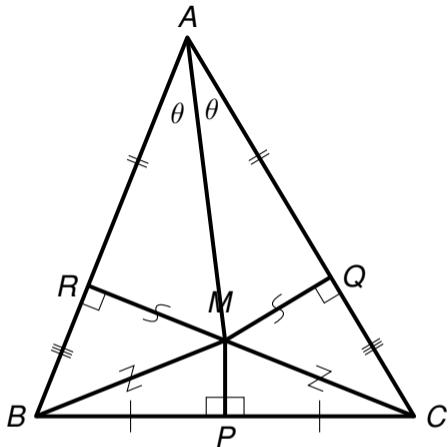
The triangles  $BPM$  and  $CPM$  are congruent, by two sides and included angle.  
Hence  $BM = CM$ .



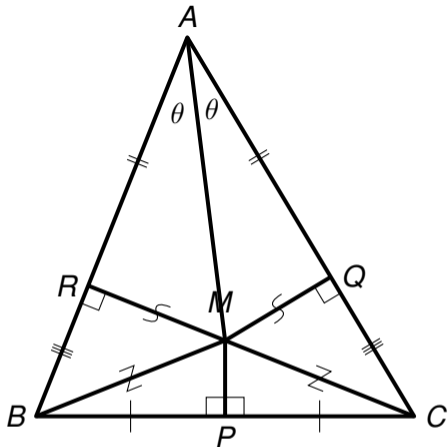
Finally, the triangles  $BRM$  and  $CQM$  are congruent, by “right angle, hypotenuse, and one other side”.



Finally, the triangles  $BRM$  and  $CQM$  are congruent, by “right angle, hypotenuse, and one other side”. Hence  $BR = CQ$ .



This means that  $AB = AR + RB$  and  $AC = AQ + QC$  are equal. Hence  $ABC$  is isosceles. But  $ABC$  was an arbitrary triangle. Hence all triangles are isosceles.



Now applying the same trick to the angle bisector of angle  $B$ , we deduce that all triangles are equilateral.

## Problematic proofs

In the course I try and persuade first year undergraduates that a proof of a mathematical statement is a finite sequence of logical claims, each of which follows from the previous claims, the hypotheses of the statement, and the axioms of mathematics, using only the rules of logic.

But if you open any research-level paper and read a proof, you will not see this *at all*.

In reality, a human-written proof is like a *story*.

## A proof is a story

A proof in a textbook or a research paper is a story.

The story attempts to persuade you that the ideas in it can *in theory* be turned into a finite sequence of logical claims etc etc etc.

In the old days, the stories were quite short.

By 1900 one of the stories was the proof of global class field theory, which is a long, technical and challenging proof (and remains long, technical and challenging in 2025).

By 2000 one of the stories was the proof of the classification of finite simple groups, which was an epic, running to many thousands of pages.

## A proof is a story

In 2025, “normal” proofs in my area (Langlands) can run to hundreds of pages.

I know from first hand experience that these things are not being reviewed carefully.

And who but a fool would review them carefully anyway? We're not being paid for this.

## The problems with human proofs

I want to highlight two problems with human-written proofs.

- They are sometimes incorrect;
- They are sometimes incomplete.

I have now seen two proofs by induction written by Fields Medallists which, when formalised, turned out to have an error in the base case.

I also just “proved” that all triangles were isosceles.

I conclude: humans are not as smart as we think we are (we are not *perfect*).

Furthermore, I say: this situation is a disgrace, it is 2025, and we can do better.

If there are bugs in software on your phone, then software updates make these bugs go away.

The “erratum” system in mathematics is far weaker (and, I would argue, doesn’t actually work).

## Formal proofs

Let me now refer to human proofs as “informal proofs”.

A *formal proof* is one which has been checked by an interactive theorem prover (Lean, Rocq, Isabelle etc etc etc).

I have *never* seen an example of an incorrect formal proof which a theorem prover’s typechecker claims is correct.

Formalisation was not always available to humanity, but it is here now, it is the gold standard, and in my mind it should be the only acceptable standard.

Example: Fermat’s Last Theorem was one of the highlights of 20th century mathematics and I am involved in a project whose ultimate aim is to formalise it in Lean.

One reason for this: A bunch of Langlandsy stuff is used in the proof, and I don’t quite trust some of the Langlands experts.

## Are we ready for formal proofs?

Example : Ben Green, Tim Gowers, Freddie Manners and Terry Tao proved the polynomial Freiman–Ruzsa conjecture in 2023.

Four days later, Tao announced a project to formalise the entire proof.

Three weeks after that, it was done.

During the process, there was an informal announcement that a 12 in the headline result could be changed to an 11, making the statement stronger.

Instead of having to re-read the entire 38 page paper, we could just change the 12 to an 11 in the theorem, recompile, see what broke, and fix it.

If only I had had a formal proof when I was generalising Ribet's level-lowering paper to  $p = 2$  in the 1990s.

## The problem with formal proofs

Here's the problem with formal proofs.

I go to the London Number Theory Seminar and every week ask myself “can we *state* the main theorems of this seminar in Lean?”

More often than not, the answer is “no, we are missing key definitions.”

## Theorems at the boundary

Another one of my projects: I am about to start supervising 4 post-docs who are translating *statements* of recent Annals papers into Lean.

As a consequence, we shall be seeing more important modern mathematical definitions appearing in Lean's mathematics library `mathlib`.

This will hopefully help to resolve the issue of missing definitions.

But what about being able to *prove* recent Annals theorems formally?

Maybe machines can do that bit.

## Morph Labs/math.inc

Last week, the tech company `math.inc` announced a computer-assisted Lean formalisation of the prime number theorem.

The way it worked: humans broke the proof up into small pieces, which they typed up in a LaTeX “blueprint”, and then a machine wrote the Lean code.

If the machine got stuck, then humans wrote more details.

# Example of LaTeX blueprint

**Lemma 246. (Identity theorem R)✓**

*Let  $0 < R < 1$  and  $f : \overline{\mathbb{D}}_1 \rightarrow \mathbb{C}$  be analytic. Suppose there exists  $\rho_0 \in \overline{\mathbb{D}}_R$  an accumulation point of  $\{\rho \in \mathbb{D}_1 : f(\rho) = 0\}$ . Then  $f(z) = 0$  for all  $z \in \mathbb{D}_1$ .*

**Proof ▼**

Apply Lemmas [245](#) and [239](#).

**Lemma 247. (Identity on K)✓**

*Let  $0 < R < 1$  and  $f : \overline{\mathbb{D}}_1 \rightarrow \mathbb{C}$  be analytic. Suppose there exists  $\rho_0 \in \overline{\mathbb{D}}_R$  an accumulation point of  $\mathcal{K}_f(R)$ . Then  $f(z) = 0$  for all  $z \in \mathbb{D}_1$ .*

**Proof ▼**

Apply Lemmas [246](#) and [242](#).

**Lemma 248. (Infinite zeros imply)✓**

*Let  $0 < R < 1$  and  $f : \overline{\mathbb{D}}_1 \rightarrow \mathbb{C}$  be analytic. If  $\mathcal{K}_f(R)$  is infinite, then  $f(z) = 0$  for all  $z \in \mathbb{D}_1$ .*

**Proof ▼**

Apply Lemmas [247](#) and [244](#).

## The future?

Some people dream of a future where machines are proving the Riemann Hypothesis all by themselves.

In fact journal editors tell me that this future is already here and it is very dystopian.

Language models are creating plausible-looking incorrect proofs of all sorts of things, and journals are being spammed with them.

So let's roll back a bit.

## The future?

I dream of a future where we have formally verified what we already *think that we know*.

I genuinely wonder how much we will discover that we didn't know after all.

If we have tools which can verify our literature, we have tools that can check our future work and referee our papers.

And hopefully, our beliefs about what we already know will not be damaged too much.

Once we have all that, I will perhaps regain an interest in curiosity-driven research.

Until the machines start doing that too. Thanks for listening!