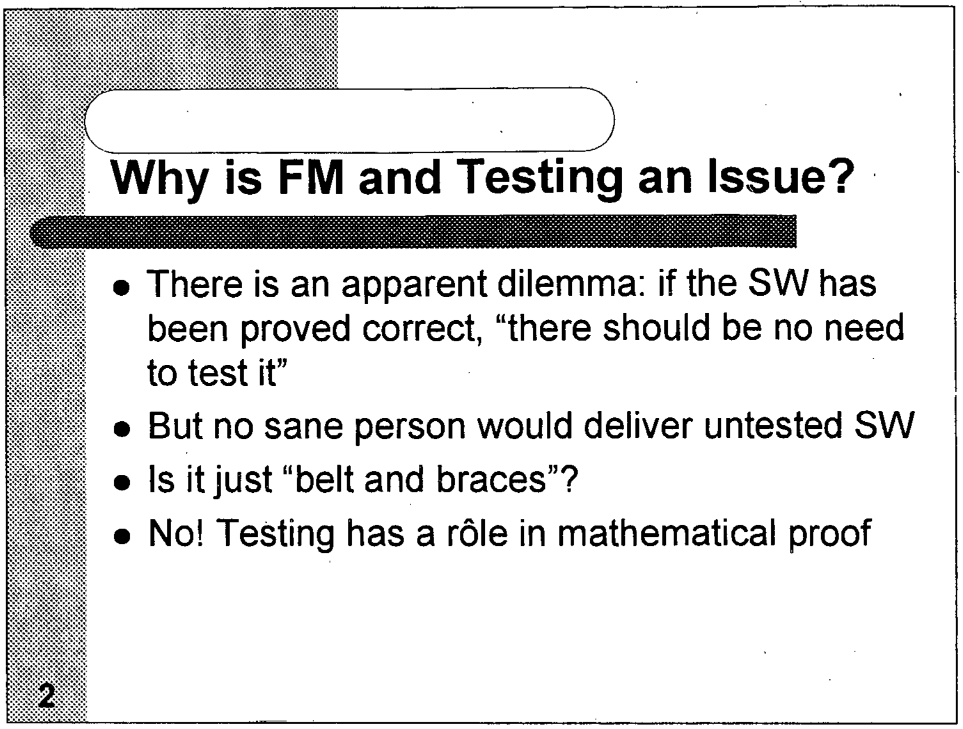


Why is FM and Testing an Issue?

- There is an apparent dilemma: if the SW has been proved correct, “there should be no need to test it”
- But no sane person would deliver untested SW
- Is it just “belt and braces”?
- No! Testing has a rôle in mathematical proof

2

One can imagine a dialogue between a customer and a supplier.

Customer: “What are you doing?”

Supplier: “Testing the software we are about to deliver to you”

Customer: “But I thought you’ve proved it correct?”

Supplier: “Oh yes, we have!”

Customer: “Why then do you need to waste time and money testing it? If you have proved it correct there is no need to, surely?”

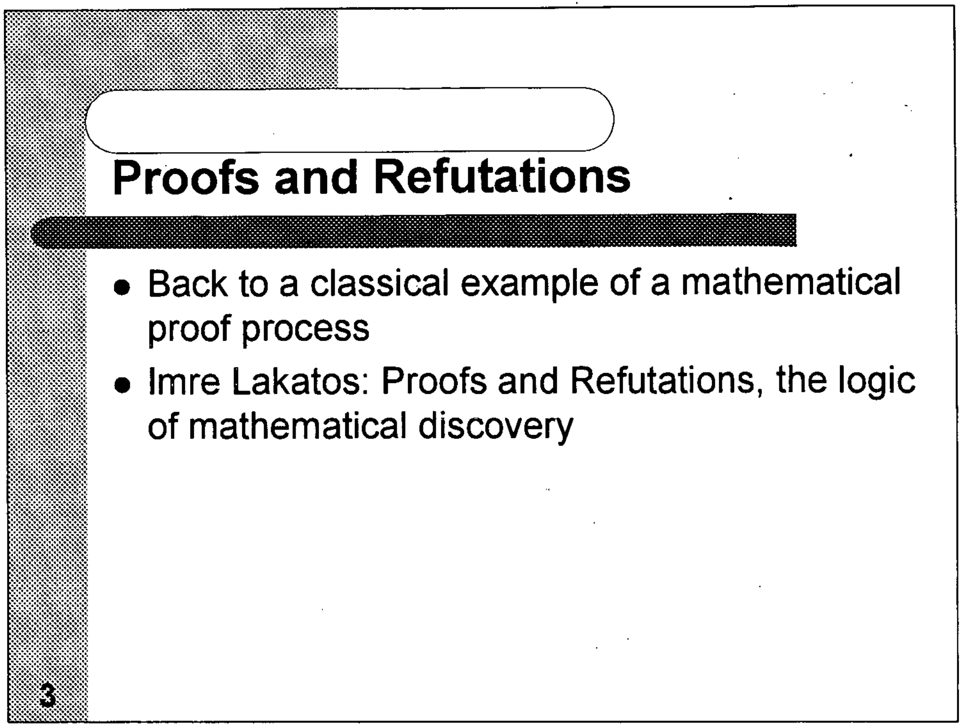
Supplier: “Er, well we just wanted to make sure.”

Consultant in charge of supplier: “Just in case there is a fault in the proof!”

Customer: “Well, that doesn’t sound too good. I thought if the software was proved correct, it was certain to be correct!”

But I felt that there was more to testing in a formal development than just a kind of belt and braces approach, a making sure that there was no fault in the proof. I felt in my bones that testing has a proper, mathematically respectable role in a formal development process.

Peter Amey touched on this when he said something along the lines of "testing is not properly for bug hunting but to check dynamic properties" - and by extension non-fn requirements more generally

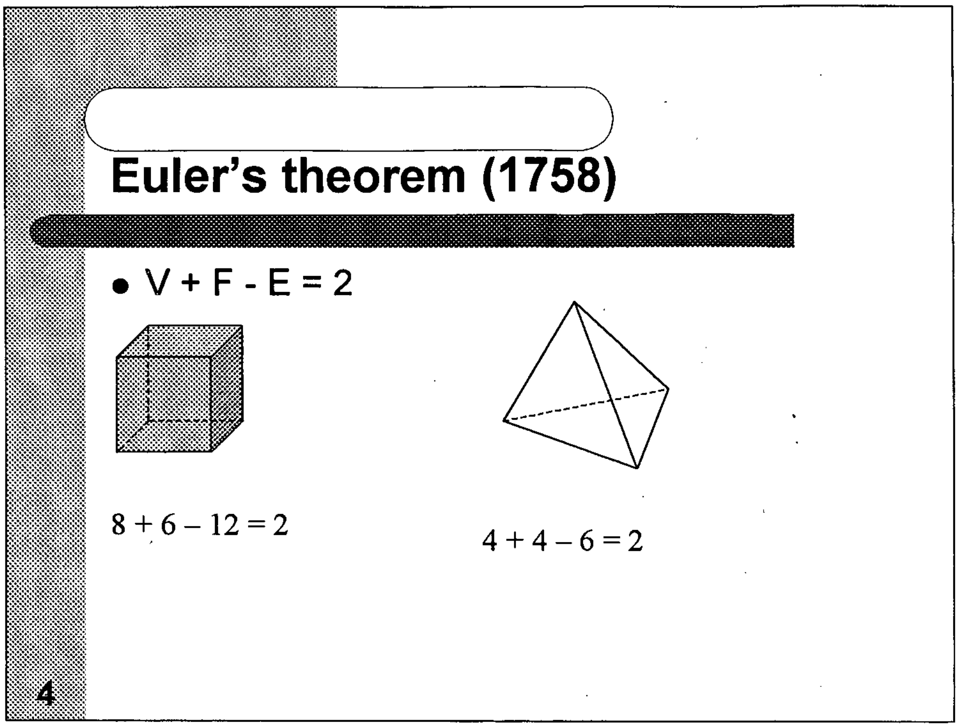


Proofs and Refutations

- Back to a classical example of a mathematical proof process
- Imre Lakatos: Proofs and Refutations, the logic of mathematical discovery

3

I was reminded of Imre Lakatos's famous thesis "Proofs and Refutations". In it he takes several classical mathematical problems.



Euler's theorem (1758)

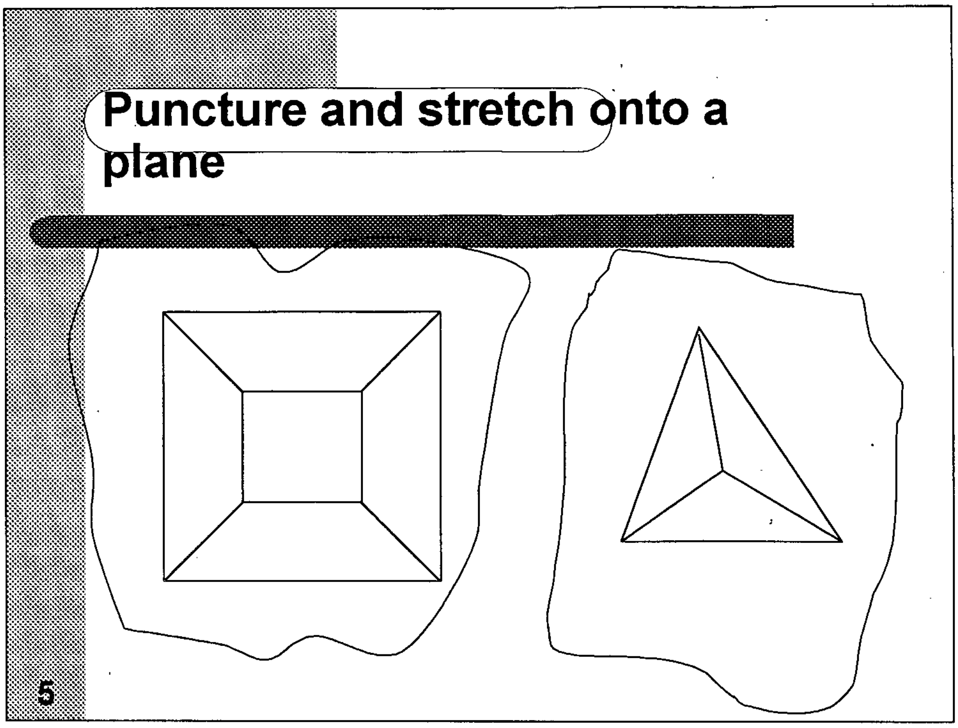
- V + F - E = 2

8 + 6 – 12 = 2

4 + 4 – 6 = 2

4

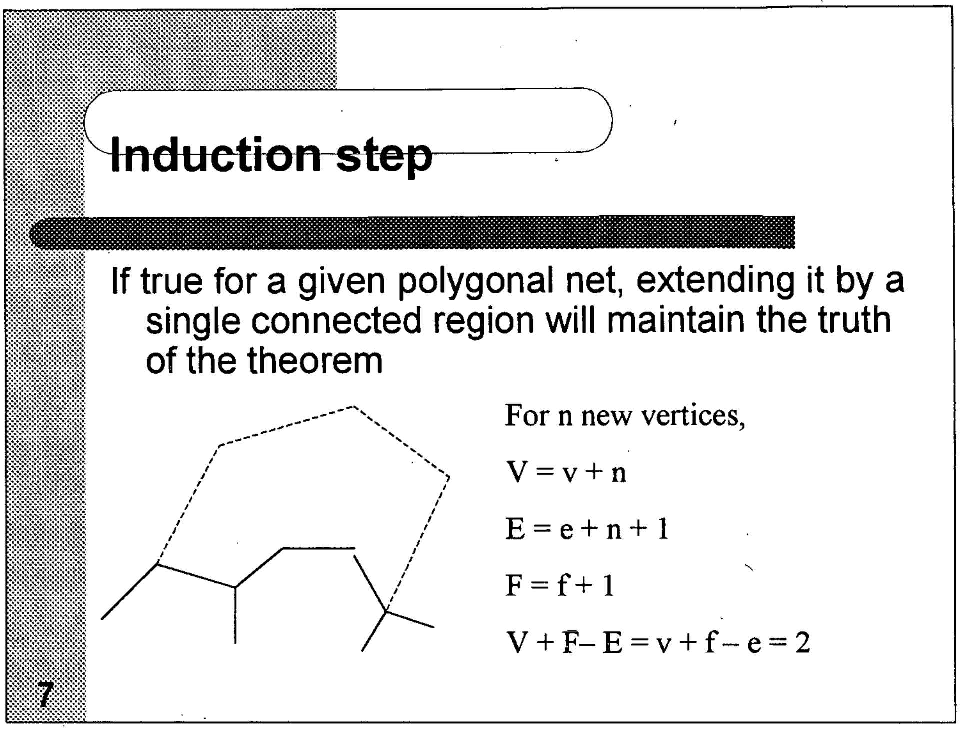
One of them is Euler's theorem V+F-E=2 for the vertices, faces and edges of a solid figure bounded by polygons. Each refutation consists of a "test" in which the calculation of V+F-E for a slightly unusual polygonal solid figure is carried out, to give a result other than 2.



Puncture and stretch onto a plane

5

The original proof runs as follows. Your are probably all remembering this from long ago now. First you take one of the faces and puncture a hole in it. Then you stretch the solid figure into a planar one. Now the problem resolves to showing that V + F – E = 2 for a connected polygonal net.



Induction step

If true for a given polygonal net, extending it by a single connected region will maintain the truth of the theorem

For n new vertices,

$V = v + n$

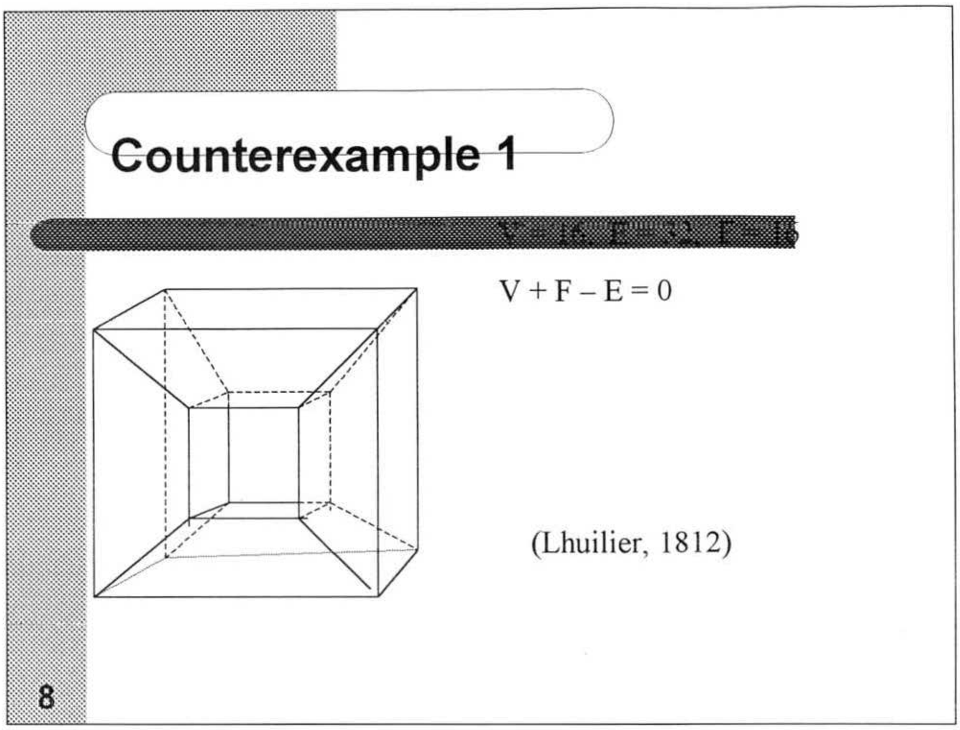
$E = e + n + 1$

$F = f + 1$

$V + F - E = v + f - e = 2$

7

And any finite connected polygonal network can be built from a single polygon by finite piecewise extensions.



Counterexample 1

V = 16, E = 32, F = 16

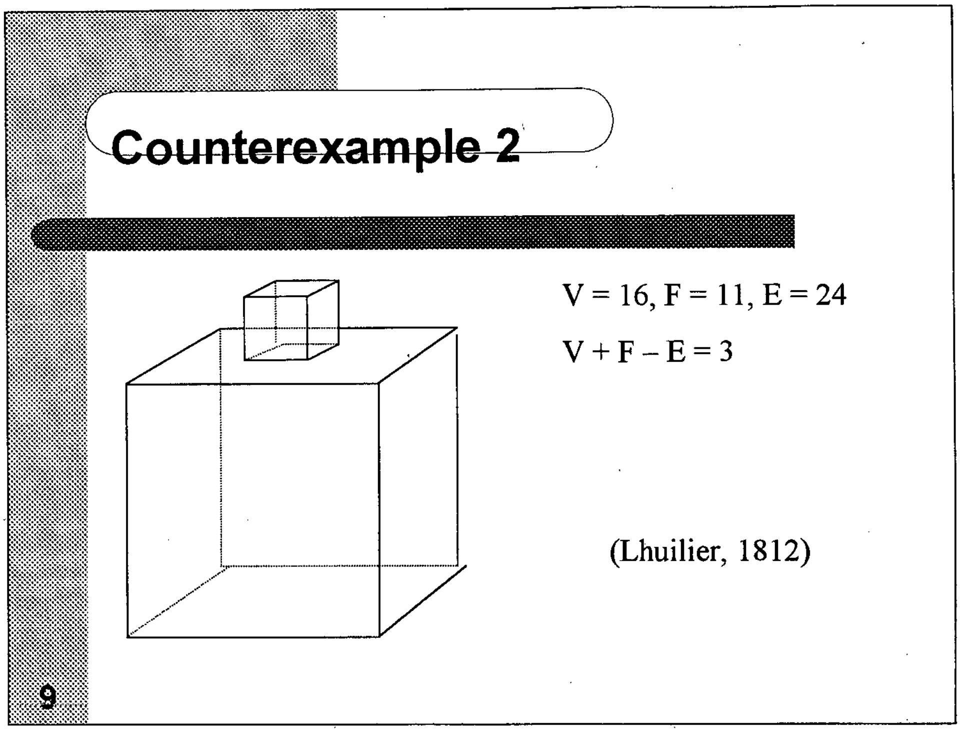
$V + F - E = 0$

(Lhuilier, 1812)

8

This theorem fascinated mathematicians for at least 150 years, some well known, others lesser known: Cauchy, de Jonquière, Lhuuilier, Hessel, Kepler, Meister, Möbius, Poinsot.

This counterexample invalidates the proof because you can't puncture the solid figure and spread it on to a plane.



Counterexample 2

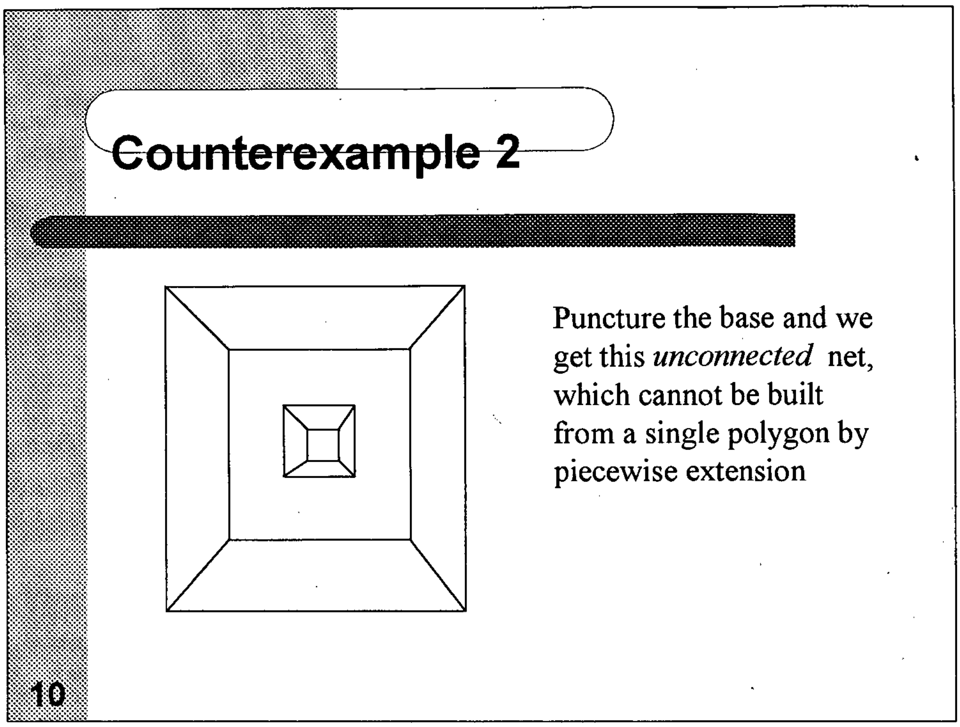
$V = 16, F = 11, E = 24$

$V + F - E = 3$

(Lhuilier, 1812)

9

This solid *can* be punctured and stretched onto a plane.



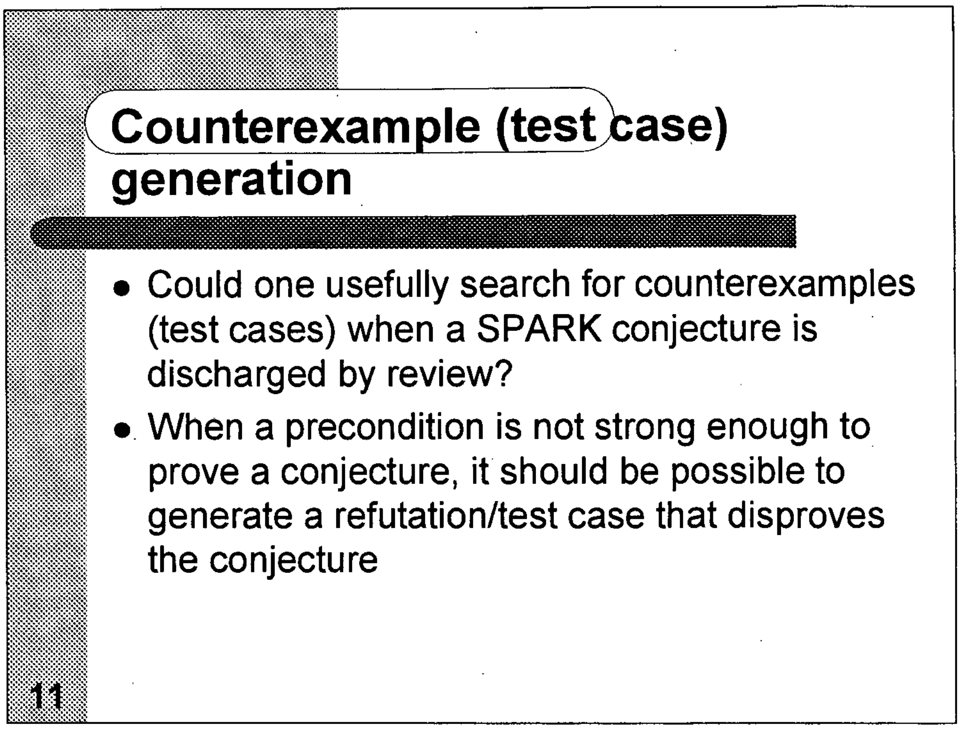
Counterexample 2

Puncture the base and we get this *unconnected* net, which cannot be built from a single polygon by piecewise extension

10

So the two counterexamples are tests of the theorem, which focus on the assumptions made in the proof, the "obvious" lemmas if you will.

and I was gratified to hear Daniel Jackson identify Testing with its search for Counterexamples.



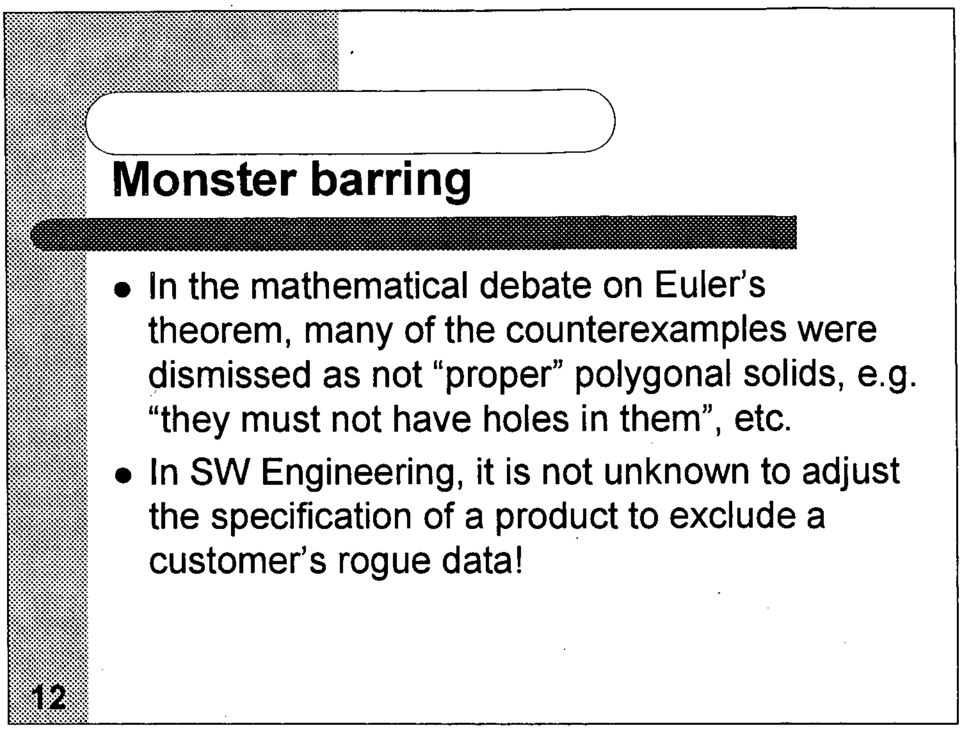
Counterexample (test case) generation

- Could one usefully search for counterexamples (test cases) when a SPARK conjecture is discharged by review?
- When a precondition is not strong enough to prove a conjecture, it should be possible to generate a refutation/test case that disproves the conjecture

11

I am reminded of the talk on Proof Plans that Andrew Ireland gave at the meeting in York. Test plans and test formulation could be directed by examining proof strategies and identifying "gaps"

And again today, if a goal cannot be proved, can part of the Test Plan process be inverted so to speak and generate possible data values or test cases which may be counterexamples/refutations of the goal? – perhaps you could answer that at the end of my talk



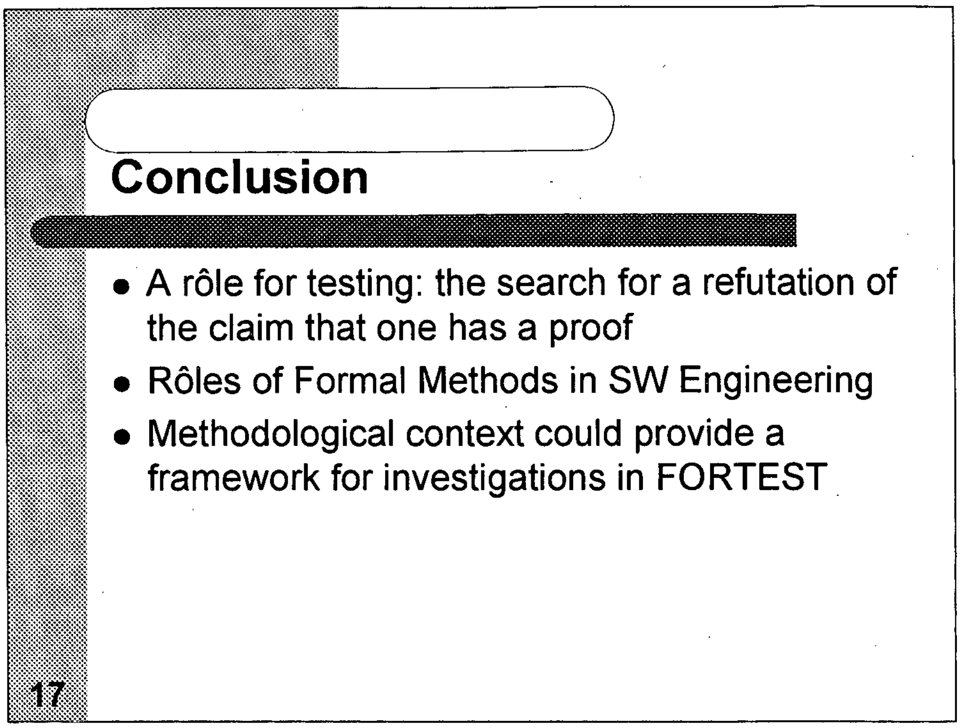
Monster barring

- In the mathematical debate on Euler's theorem, many of the counterexamples were dismissed as not "proper" polygonal solids, e.g. "they must not have holes in them", etc.
- In SW Engineering, it is not unknown to adjust the specification of a product to exclude a customer's rogue data!

12

This came close to redefining a polyhedron as one which fulfilled Euler's theorem.

Of course Praxis never do anything like that, but when I was working somewhere else, before I worked at Praxis…



Conclusion

- A rôle for testing: the search for a refutation of the claim that one has a proof
- Rôles of Formal Methods in SW Engineering
- Methodological context could provide a framework for investigations in FORTEST

17

Bullet 3 – and help to provide focus and structure.