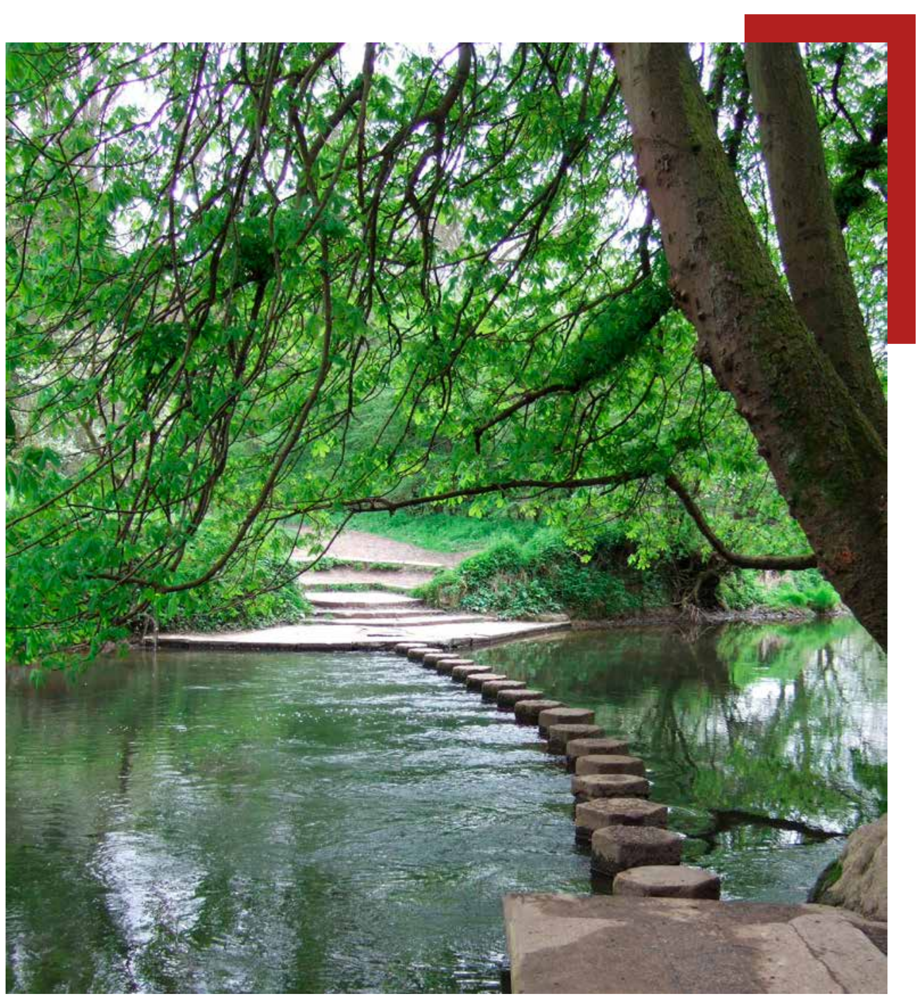
Machine Checked Proofs

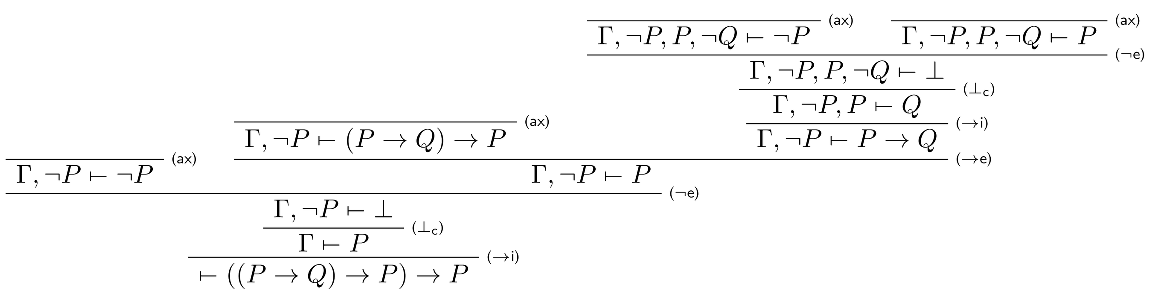
When computers improve mathematical rigour

Since the invention of the concept of proof in ancient Greece, mathematicians have always sought to write ever more rigourous proofs: identifying axioms precisely, defining every object used in the proof, avoiding the call to intuition, etc. Machine-checked proof is a new step in this never ending quest of rigour.
A machine-checked proof is written with such precision that a computer program can check its correctness.



Like the crossing of a river ford, a mathematical proof goes step by step

```
Goal ((P -> Q) -> P) -> P.
intro piqip.
assert (ponp: P \/ ~P).
exact (classic P).
destruct ponp as [p|np].
assumption.
apply piqip.
intro p.
destruct np.
assumption.
Qed.
```



Two proofs of Peirce's law, in COQ (above) and in the natural deduction calculus (below).

THE BEGINNING

The two first proof-checkers were Automath (de Bruijn, 1967), and then LCF (Milner, 1972). Their goals were different: Automath was designed to check general mathematical proofs, LCF, more specifically, proofs of properties of programs.

TODAY

The development of proof-checkers triggered the development of new theories, besides set theory, to express mathematics: each system innovates, introducing new features to express mathematical statements and proofs, just like each new programming language introduces new features to express programs.

Popular proof-checkers are ACL 2, Agda, Coq, HOL Light, HOL 4, Lean, Mizar, Nuprl, PVS, and many others. These proof-checkers are specific to one theory. Others, such as Beluga, Dedukti, Isabelle, Lambda-prolog, Twelf, and others are frameworks, where various theories can be defined.

They have in total more than 10,000 users.

RECENT PROOFS

2000 : four colour theorem (Gonthier et al.)
2008 : correctness of the C compiler CompCert (Leroy et al.)
2009 : correctness of the operating system seL4 (Klein et al.)
2012 : Feit-Thompson theorem (Gonthier et al.)
2014 : Kepler's conjecture (Hales et al.)
2014 : UniMath a body of mathematics using univalent foundations (Voevodsky et al.)

Several of these projects aim at gathering a substantial body of mathematics, like Euclid's *Elements* and Bourbaki's *Élements de mathématique* did.

*For long, mathematics was the only science not to use instruments.
The computer is becoming the telescope of mathematicians*