



© 1997–2009, Millennium Mathematics Project, University of Cambridge.

Permission is granted to print and copy this page on paper for non-commercial use. For other uses, including electronic redistribution, please contact us.

September 1999

Features



## The origins of proof III: Proof and puzzles through the ages



In the Millennia since Euclid, people's conceptions of mathematical proof have been revolutionised. From the discovery of Calculus and the rise of abstract mathematics, to Gödel's amazing discovery. There have been many changes and a few surprises along the way.

### Proof In Ancient Times (*It's all Greek To Me*)

Earlier in this series we looked at the axioms and deductive reasoning of the ancient Greeks, especially Euclid. For them, a statement could be considered proved if it had been derived using deductive reasoning from a given set of basic axioms. This method is one of the most important contributions of the ancient Greek scholars to present day mathematics. However, it was not always this way. During the time of the school of Pythagoras it was common to simply check that a result was true in some special cases. It is possible that the famous Pythagorean Theorem was not actually *proved* by Pythagoras.

What *was* proved during this time was that the square root of two is irrational. A rational number is one which can be written in the form  $p/q$  where  $p$  and  $q$  are whole numbers (and  $q$  is non-zero). Irrational numbers cannot. This apparently brought the life of Hippiasus of Metapontum to a watery end, thrown overboard by irate Pythagoreans! They believed that the entire universe could be reduced to whole numbers and their ratios.

Hippiasus's result is an example of proof by contradiction. This is not quite what he wrote but the idea is the same.

Suppose that  $\sqrt{2}$  is rational. Then we can find whole numbers  $A$  and  $B$  such that

$$\sqrt{2} = \frac{A}{B},$$

and  $A$  and  $B$  have no common factors. From this it follows that

$$A^2 = 2B^2.$$

Thus  $A^2$  is even, and since the squares of odd numbers are always odd we can deduce that  $A$  is also even. So,  $A = 2a$  where  $a$  is also a whole number, and re-writing the above line gives

$$2a^2 = B^2.$$

We now know that  $B$  is also even and thus  $B = 2b$ . This means that 2 divides both  $A$  and  $B$  and as such is a common factor. This contradicts our hypothesis, which then cannot be true. From this it follows that  $\sqrt{2}$  is irrational.

**Can you use the same method to prove that  $\sqrt{3}$  and  $\sqrt{5}$  are irrational? Why doesn't it work for  $\sqrt{4}$ ? How about  $\sqrt{p}$  where  $p$  is a prime number?**

This revelation, and the need for a sure way of dealing with such unexpected quantities, could only have added to the importance placed on the deductive system.

After the Greeks there was little development in the theory of proof. Arithmetic and Algebra flourished among Hindu and Arab mathematicians. However, many of their advances were not accompanied by watertight proof. This lack of awareness or concern about the need for logical foundations in algebra continued for centuries.

## Until 1800: Calculus, Newton & Leibniz

Until the 18th century, mathematicians continued to further the study of algebra. New rules and operations were added and many of their proofs relied on the "evident" properties of integers and geometry. Kepler, in the 16th and 17th centuries, justified his results on the basis of physical observations, as explained in our previous article about his work. Often results were asserted true simply by the method of induction.

In this sense, induction means that if a statement is true in enough specific cases then one could reason that it is true in all. *This is not correct!* Below are a couple of tricks to illustrate this.

Q1. First of all, can you suggest the statement of a theorem about positive integers that holds for the first 1,000,000 cases but then breaks down?

Q2. Here is an interesting "formula for primes".

$$P_n = n^2 + n + 41 \text{ where } n \text{ is a whole number.}$$

$P_0 = 41, P_1 = 43, P_2 = 47$  all of which are prime. For what value of  $n$  does this first generate a composite number?

## The origins of proof III: Proof and puzzles through the ages

So, mathematicians of the time went on to use irrational and complex numbers as well as the concept of continuity without really having a solid basis for their work.

One of the great revolutions in mathematics was the development of Calculus by the German mathematician Leibniz and, independently, Isaac Newton. Newton was almost certainly first with the concept of Calculus (although this was hotly disputed), but Leibniz carried the ideas further. The seeds of Calculus were sown by the earlier works of Fermat, Pascal and Barrow. Pascal asserted that his rules for infinitesimal geometry were equivalent to those used by the ancient Greeks. "What is demonstrated by the true rules of indivisibles could be demonstrated also with the rigour and the manner of the ancients." As regards differentiation, early work done by such people as Fermat was justified on the basis that gradients had a clear geometric interpretation and thus the theory could be put on a rigorous footing.

Newton also thought that the methods he used to obtain his results were an extension of pure geometry. In preparing his most famous work, the *Principia Mathematica*, published in 1686, it is certain that Newton used his new mathematics of Fluxions (which would later become known as Calculus) to obtain many of the results. However, the work was published using geometric proofs. This was probably done so it could be understood more readily. Equally, many people simply did not believe in the new maths of Fluxions!

Leibniz, however, saw the power of Calculus and was eager to declare the dawn of a new science. He was not too concerned about the lack of rigour in his methods. In the same spirit, Johann Bernoulli, who wrote a text devoted to Calculus in 1696, explained his method with analogies! "Infinitely large quantities are like astronomical distances and the infinitely small are like animalcules revealed by the microscope."

Much confusion centred around the use of infinitesimal quantities such as  $dx$  and  $dy$  in the expression  $dy/dx$ . If these quantities were zero then what did  $dy/dx$  mean? If not then how could Calculus work? For example let  $y = x^2$ ;

$$\text{then } \frac{dy}{dx} = \frac{(x + dx)^2 - x^2}{dx} = 2x + dx.$$

Mathematicians had to justify why the  $dx$  could be dropped to give the derivative that we all expect. What was lacking was an established idea of a limit. Using limits we now think of  $dy/dx$  as follows.

$$\frac{dy}{dx} = \lim_{\Delta x \rightarrow 0} \frac{\Delta y}{\Delta x}$$

where  $|\Delta x| > 0$ . Our example then becomes

$$\frac{dy}{dx} = \lim_{\Delta x \rightarrow 0} \frac{(x + \Delta x)^2 - x^2}{\Delta x} = \lim_{\Delta x \rightarrow 0} 2x + \Delta x = 2x.$$

The trend continued with claims that Calculus could be rigorised by the methods of the ancient Greeks. The reality was that the work of Newton and Leibniz was a radical departure from existing maths and would need its own foundations.

Calculus was also attacked in the 18th century. Bishop Berkeley published the work *The Analyst, Or a discourse addressed to an infidel mathematician*. This century also saw numerous attempts to put Calculus on a more solid footing, notably by Maclaurin, Lagrange and d'Alembert. Their goal, though, was not to be achieved until the 19th century.

## The origins of proof III: Proof and puzzles through the ages

The atmosphere of this period is captured beautifully in a quotation from d'Alembert. "Up to the present... more concern has been given to enlarging the building than to illuminating the entrance, to raising it higher than to giving it proper foundations." Many great discoveries and inventions had been made but the next challenge would be to build the foundations.

## The 19th Century, Back To Basics

The 19th century also saw great leaps forward in the development of subject matter. However, one of the most important trends was the return of rigorous proof. The striking developments of Quaternions (numbers that did not obey the normal laws of arithmetic) and non-Euclidean Geometry (as explained in [The Origins of Proof, Part I in Issue 7](#)) highlighted how complacent people had been. These discoveries forced mathematicians to question whether their rules of arithmetic and geometry were so dependable after all. It became clear that many proofs previously thought to be rigorous were instead based purely on intuition.

Quaternions do not "commute" under multiplication, in other words  $a \times b \neq b \times a$ . The Quaternion numbers denoted by  $j$  and  $k$  obey  $jk = -kj$ . Real numbers and complex numbers both commute under multiplication.

Accordingly, mathematicians developed precise formulations for irrational numbers, continuity, integrals and derivatives. Among other things, this led to the precedence of algebra over geometry. Numbers and geometry had been *axiomatised* and mathematicians no longer needed to resort to intuition to substantiate their ideas.

With the axiomatisation of maths came logical foundations for both old and new subjects. This helped to clarify exactly what assumptions underlay each area. It was also now easier to find connections between different branches of maths. Mathematics, again, became about the study of consequences of axioms: it was now abstract, and not purely about physical phenomena. The famous Cambridge mathematician [G.H. Hardy](#) wrote, "I believe that mathematical reality lies outside us, that our function is to discover or observe it and the theorems we describe grandiloquently as our creations are simply the notes of our observations."

Before, when all maths was seen as intimately linked to nature, it would have seemed impossible for contradictions to occur. However, with the new discoveries and new view of maths, this question gained importance. People began to wonder whether maths was consistent after all.

Answering this question became more urgent with the discovery of "paradoxes", especially in set theory. A famous example is the Russell paradox. Here is an illustration of the problem. A barber lived in a village and one day advertised that he shaves all the people in the village who do *not* shave themselves. Of course, he says, I don't shave those people who *do* shave themselves. The next morning the barber was wondering whether or not he should shave himself...

The paradox in its original set theoretic form reads:

Let  $X$  be the set of all sets which do not contain themselves, that is

$$X = \{A : A \text{ is a set and } A \notin A\}$$

Is  $X \in X$ ? In other words, is  $X$  contained in itself?

If  $X \notin X$  then  $X$  is not a set which does not contain itself, so it does contain itself and thus  $X \in X$ . Contradiction.

On the other hand, if  $X \in X$  then  $X$  is a set which doesn't contain itself and so  $X \notin X$ . Contradiction.

The first attempts to resolve these paradoxes involved the axiomatisation of set theory. The existing grounding, which had been given by Cantor, was in some respects inadequate. Zermelo, Fraenkel, von Neumann and others developed a formal set theory that now seems adequate for nearly all of classical analysis. As yet nobody has found a paradox!

Around the turn of the century, one of the great challenges was to show that mathematics itself was consistent. David Hilbert attempted to use a technique known as Metamathematics. Metamathematics excluded the use of proof by contradiction and used only very concrete reasoning. The consistency of a large portion of maths can be reduced to the consistency of the arithmetic of natural numbers (known as number theory). Hence attention focused on this area. Hilbert and his team had received some success and thought they were on the verge of a breakthrough. However, they were about to receive a serious blow.

## Gödel And Incompleteness

Kurt Gödel showed that the consistency of number theory could not be proved using the narrow logic of metamathematics. This was a consequence of his best known result, Gödel's Incompleteness Theorem.

Gödel's theorem states that any consistent axiomatic system that embraces arithmetic is incomplete. To be incomplete means that within the system are statements (known as undecidable) that can neither be proved nor disproved using the axioms!

Gödel went on to show that this implies that the consistency of a deductive system cannot be established using the system itself. Hilbert's goal of showing the consistency of maths was ultimately unattainable.

It was not just Hilbert who suffered as a result of this incredible theorem. Russell and Whitehead had developed their own formal system of reasoning. This had been laid out in their text, also titled *Principia Mathematica*. With the advent of the incompleteness theorem, it became clear that all hope of proving the consistency of the Russell–Whitehead system had faded.

However, Gödel's theorem did have some positive results as it contributed to the development of the theory of computability. Computability is the study of whether within a deductive system, there is an algorithm that will decide whether a given statement is logically true. Also, whether an algorithm exists that will determine whether a given statement is decidable.

The proof of Gödel's theorem uses self reference of the same type as in some well known brain teasers. For example, "this sentence is false". Or, doubly confusing, imagine a card on one side of which is printed

**"The statement on the other side of this card is true."**

and on the other

**"The statement on the other side of this card is false."**

Is this possible or is there a paradox? Gödel's theorem is wonderfully illustrated in a book called *What is the name of this book?* by Raymond Smullyan. He uses logic puzzles which are like some found in Lewis

## The origins of proof III: Proof and puzzles through the ages

Carroll's *Alice in Wonderland*.



Knights or Knaves?

Imagine there are two types of people, Knights (who always tell the truth) and Knaves (who always lie). There are three such people sitting under a tree, A, B and C.

A says, "All of us are Knaves."

B says, "Exactly one of us is a Knight."

**What are A, B and C? It is possible to tell!**

Smullyan constructs an island inhabited by such people. However, there exist both Knights and Knaves whose true nature is impossible to prove. These characters correspond to the undecidable statements in Gödel's theorem.

So mathematicians, having slowly accepted the Greek notion of axioms and deductive logic, even now have to face the new problem that this approach still might not be enough!

### Answers to Problems

A1. Let  $N$  be a positive integer; then  $N \leq 1,000,000$ .

A2. The first few are all prime and it soon becomes difficult to check. However, it certainly doesn't generate a prime for  $n = 40$ .

Oh, and the identities of our three friends are: A, Knave, B, Knight, C, Knave.

## Bibliography/Further Reading

- *What Is The Name Of This Book?* by Raymond Smullyan, Penguin Books, 1990.
  - *Gödel, Escher, Bach: An Eternal Golden Braid* by Douglas R. Hofstadter, Random House USA / Penguin Books. This book has lots of examples of puzzles and paradoxes through the centuries, and explains some of the ideas behind Gödel's theorems.
- 

## About the author



Jon Walthoe is presently a graduate student at the University of Sussex. As well as his graduate research, he is involved in the EPSRC–funded Pupil Researcher Initiative.

After finishing his first degree at the University of Exeter, he opted out of Maths for a while. This involved working in local government among other things, and travelling in Latin America. When not doing his research, his favourite escape is sailing on the local waters in Brighton.

---



*Plus* is part of the family of activities in the Millennium Mathematics Project, which also includes the NRICH and MOTIVATE sites.