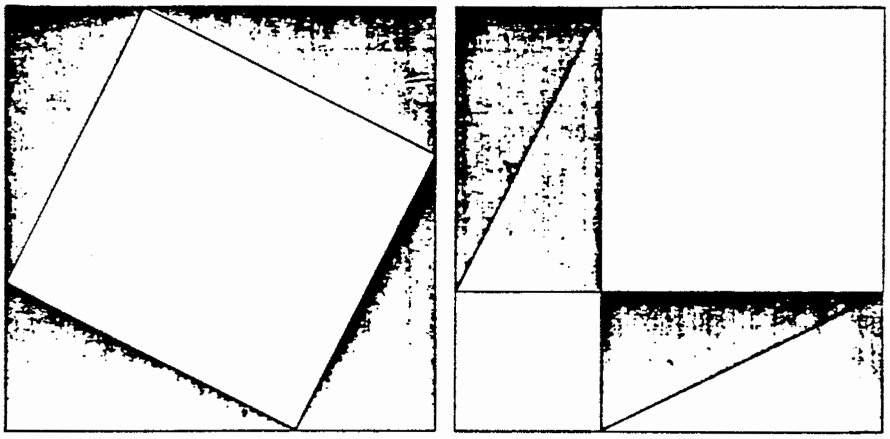
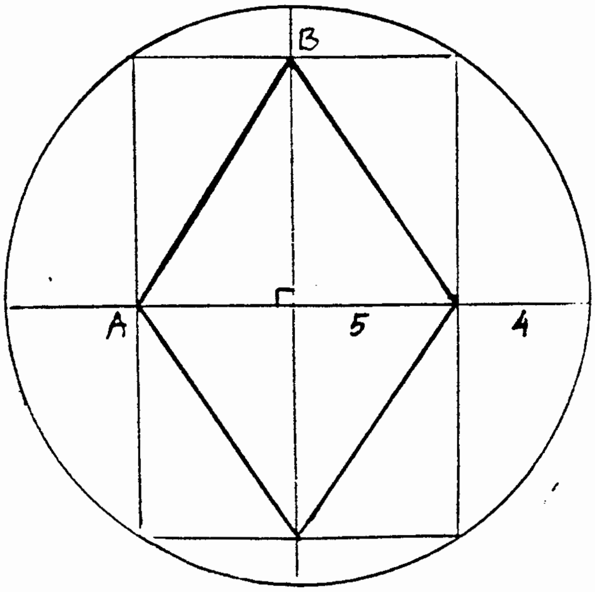
A famous proof: The Pythagorean theorem.

A "look-see" proof of the theorem for any type of right triangle



When do we accept that a mathematical theorem has been proven?
Where does our certainty come from?
Plato's dialogue "Meno" has a lot to do with these questions! So does this neat problem:

How long is the side AB?



Euclid's proof
– that there is no greatest prime number

From: Nagel & Newman "Gödel's Proof". N.Y. Uni. Press 1974.

Ordinarily, even when mathematical proofs conform to accepted standards of professional rigor, they suffer from an important omission. They embody principles (or rules) of inference not explicitly formulated, of which mathematicians are frequently unaware.

Take Euclid's proof that there is no greatest prime number (a number is prime if it is divisible without remainder by no number other than 1 and the number itself). The argument, cast in the form of a *reductio ad absurdum*, runs as follows:

Suppose, in contradiction to what the proof seeks to establish, that there is a greatest prime number. We designate it by 'x'. Then:

1. x is the greatest prime
2. Form the product of all primes less than or equal to x, and add 1 to the product. This yields a new number y, where $y =$

$$(2 \times 3 \times 5 \times 7 \times \ldots \times x) + 1$$

3. If y is itself a prime, then x is not the greatest prime, for y is obviously greater than x
4. If y is composite (i.e., not a prime), then again x is not the greatest prime. For if y is composite, it must have a prime divisor z; and z must be different from each of the prime numbers 2, 3, 5, 7, . . . , x, smaller than or equal to x; hence z must be a prime greater than x
5. But y is either prime or composite
6. Hence x is not the greatest prime
7. There is no greatest prime

Proofs 3

We have stated only the main links of the proof. It can be shown, however, that in forging the complete chain a fairly large number of tacitly accepted rules of inference, as well as theorems of logic, are essential. Some of these belong to the most elementary part of formal logic, others to more advanced branches; for example, rules and theorems are incorporated that belong to the "theory of quantification." This deals with relations between statements containing such "quantifying" particles as 'all', 'some', and their synonyms. We shall exhibit one elementary theorem of logic and one rule of inference, each of which is a necessary but silent partner in the demonstration.

Look at line 5 of the proof. Where does it come from? The answer is, from the logical theorem (or necessary truth): 'Either *p* or non-*p*', where '*p*' is called a sentential variable. But how do we get line 5 from this theorem? The answer is, by using the rule of inference known as the "Rule of Substitution for Sentential Variables," according to which a statement can be derived from another containing such variables by substituting any statement (in this case, '*y* is prime') for each occurrence of a distinct variable (in this case, the variable '*p*'). The use of these rules and logical theorems is, as we have said, frequently an all but unconscious action. And the analysis that exposes them, even in such relatively simple proofs as Euclid's, depends upon advances in logical theory made only within the past one hundred years.[5] Like Molière's M. Jourdain, who spoke prose all his life without knowing it, mathematicians have been reasoning for at least two millennia without being aware of all the principles underlying what they were doing. The real nature of the tools of their craft has become evident only within recent times.

Fermat's "Last Theorem" (Pierre de Fermat 1601–1665)

If n integer > 2 and x, y, z integers > 0 then:

the equation $x^n + y^n = z^n$ cannot be solved.

Proved June 1993.

Fermat's hypothesis of primes

$$2^{(2^n)} + 1, \; n \in N, \text{ is a prime}$$

Disproved by Euler (1707–83).

$n = 1$:	$2^{(2^1)} + 1$	$= 5$	prime
$n = 2$:	$2^{(2^2)} + 1$	$= 17$	prime
$n = 3$:	$2^{(2^3)} + 1$	$= 257$	prime
$n = 4$:	$2^{(2^4)} + 1$	$= 65{,}537$	prime
$n = 5$:	$2^{(2^5)} + 1$	$= 4{,}294{,}967{,}297 = 641 \times 6.700.417$	

The Goldbach conjecture (1690–1764)

Every even number is the sum of two prime numbers.

Yet neither proved nor disproved.

$\sqrt{2}$ is irrational

Proof: If $\sqrt{2}$ were rational, then it can be expressed as a fraction in its lowest terms: $\sqrt{2} = p/q$, where p and q are integers with no common factor greater than 1. Then:

$$\sqrt{2} = \frac{p}{q} \Rightarrow 2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2 \Rightarrow p^2 \text{ even} \Rightarrow p \text{ even.}$$

$$\Rightarrow \tfrac{1}{2}p \text{ is integer} \Rightarrow \tfrac{1}{4}p^2 = \tfrac{2}{4}q^2 \text{ integer} \Rightarrow \tfrac{1}{2}q^2 \text{ integer} \Rightarrow q^2 \text{ even}$$

$\Rightarrow q$ even. Then p and q has 2 as common factor, wich contradicts the assumption in the start.

Proof 5

<u>There exists</u> x and y, both irrational, and z, rational, such that $x^y = z$.

Proof: Look at the number $\sqrt{2}^{\sqrt{2}}$. It is either rational or irrational.

If $\sqrt{2}^{\sqrt{2}}$ is rational, then put $x = \sqrt{2}$, $y = \sqrt{2}$, $z = \sqrt{2}^{\sqrt{2}}$. q.e.d.

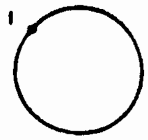
If $\sqrt{2}^{\sqrt{2}}$ is irrational, then put $x = \sqrt{2}^{\sqrt{2}}$, $y = \sqrt{2}$, $z = 2$. q.e.d.

$\left(\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2 \right).$

This proof shows, that a solution must exist, but it does not give us any solution to the problem.

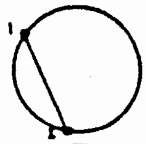
Consider the maximum number of regions R formed when n points on a circle are joined to each other by straight lines. Proceed as follows:

n = 1



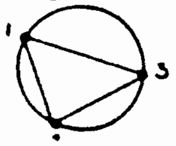
R = 1

n = 2



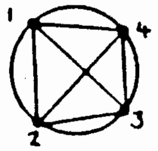
R = 2

n = 3



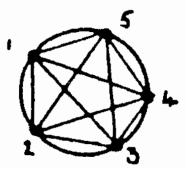
R = 4

n = 4



R = ?

n = 5



R = ?

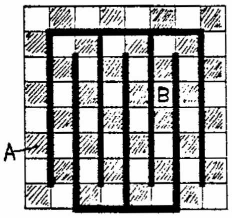
n = 6

R = ?

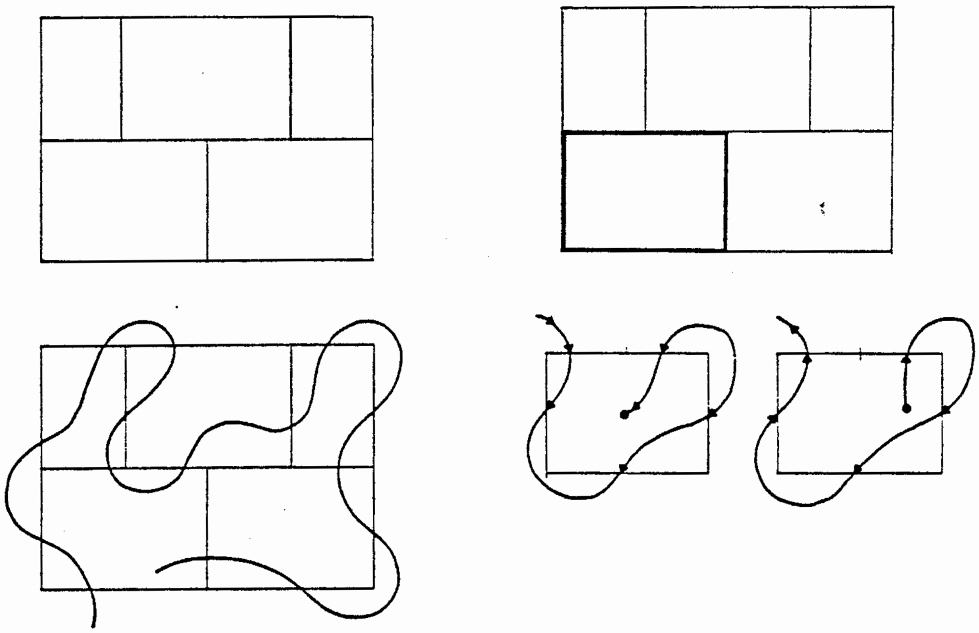
Proof 6

Gomory's Theorem. Remove one white and one black square from an ordinary checkerboard. The reduced board can always be covered with 31 dominos of size 2 × 1.

Analog Proof. Convert the checkerboard into a labyrinth as in the accompanying figure. No matter which black square "A" and which white square "B" are deleted, the board can be covered by threading through the labyrinth with a caterpillar tractor chain of dominos which break off at "A" and "B."



From: Davis & Hersh, "The Mathematical Experience", Penguin Books



Why is it not possible to draw a line that intersects all the line sections in the figure once and only once?
Well, look, for instance, at the lower left rectangle. Any line either starts inside that rectangle, or outside it. And since any line that solves the problem will have to intersect each of the five "sides" of this rectangle, a line starting outside must end inside, and a line starting inside must end outside. This follows from the fact that five is an odd number. So, in either case it has one end inside the rectangle. The line will, of course, also have to intersect all other sectins in the large figure, but no matter how this is accomplished, it must necessarily have one end inside the lower left rectangle.
Now, precisely the same could be said about the lower right rectangle: It has five "sides", that all have to be intersected, so a line that solves the problem must necessarily have one end inside it.
And finally: By the same token the line must have one end inside the central rectangle just above the two just mentioned, since this too has five "sides".
But no line can have three ends, so there can be no line that solves the problem!

Did you understand this proof? What does understanding really mean? Well, are you willing to bet (almost) anything that no one will ever come along and solve the problem after all? If not, it might well be argued that you didn't <u>really</u> understand the proof!