EXAMPLES OF PROOFS

Geometry

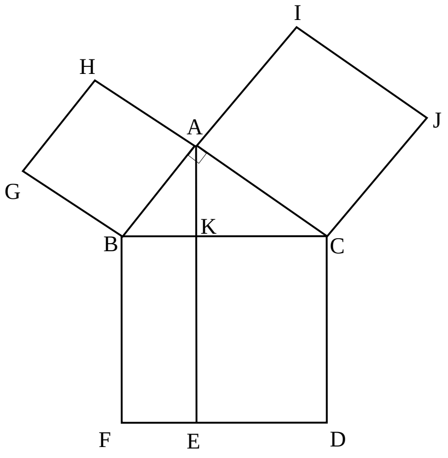
The *Pythagorean Theorem* is Proposition 47 of Book I of Euclid's *Elements*.

Theorem. In a right-angled triangle, the square of the length of the hypotenuse is equal to the square of the lengths of the other two sides.

The proof requires two previously established facts:

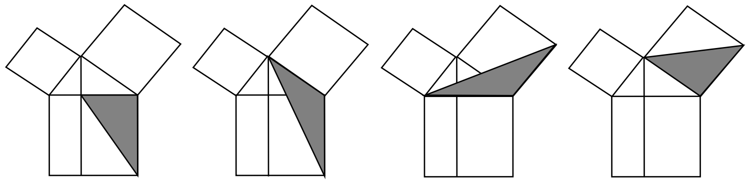
1. If a pair of triangles have the same base and the same height, they have the same area.
2. If, in a pair of triangles, two sides and an included angle are congruent, the triangles are congruent.

Given triangle ABC, construct the diagram below.



We need to show that the area of square $BCDF$ is equal to the area of square $ABGH$ plus the area of square $ACJI$. The strategy is to show that the area of rectangle $BKEF$ is the same as the area of square $ABGH$, and that the area of rectangle $CDEK$ is the same as the area of square $ACJI$.

Let us focus on $CDEK$ and $ACJI$ (the other part of similar). The trick is to divide both these figures in half, to obtain triangles; and show that the resulting triangles have the same area. More explicitly, the proof shows that the four triangles indicated below have the same area. For the first and last pairs, one uses fact 1 above; for the middle pair, one uses fact 2.



Here is the explicit proof.

1. The area of triangle ACD is the same as the area of triangle CKD by Fact 1, because they have the same base (CD) and the same height.
2. Angle ACD is congruent to angle ACJ, because they are both equal to a right angle plus angle ACB.
3. Side AC is congruent to CJ, because $ACJI$ is a square.
4. Side BC is congruent to CD, because $BCDF$ is a square.
5. Triangle BCJ is congruent to ACD, by 2, 3, 4, and Fact 2. So these two triangles have the same area.
6. The area of triangle BCJ is the same as the area of triangle ACJ by Fact 1, because they have the same base (CJ) and height.
7. Triangles CKD and ACJ have the same area, by 1, 5, and 6.
8. The area of rectangle $CDEK$ is twice the area of triangle CKD.
9. The area of square $ACJI$ is twice the area of triangle ACJ.
10. Square $ACJI$ and rectangle $CDEK$ have the same area, by 7, 8, and 9.
11. By a similar argument, square $ABGH$ and rectangle $BFEK$ have the same area.
12. The area of square $BCDF$ is equal to the area of rectangle $BFEK$ plus the area of rectangle $CDEK$.
13. So the area of square $BCDF$ is equal to the area of sequare $ACJI$ plus the area of square $ABGH$, by 10, 11, and 12.
14. The area of triangle CKD, and so the area of ACD, is half the area of rectangle $CDEK$. QED.

There are many other proofs of the Pythagorean theorem.

The following story about the philosopher Thomas Hobbes is taken from John Aubrey's biographical work, *Brief Lives*, and is also excerpted in Davis and Hersh, *The Mathematical Experience.*

> He was 40 yeares old before he looked on Geometry; which happened accidentally. Being in a Gentleman's Library, Euclid's Elements lay open, and 'twas the 47 *El. libri* I. He read the Proposition. By G— sayd he (he would now and then sweare and emphaticall Oath by way of emphasis) *this is impossible!* So he reads the Demonstration of it, which referred him back to such a Proposition; which proposition he read. That refereed him back to another, which he also read. *Et sic deincips* [and so on] that at last he was demonstratively convinced of that trueth. This made him in love with Geometry.

Number Theory

Let us start with a fact that was known to the Pythagoreans:

Theorem. $\sqrt{2}$ is irrational.

Proof. Suppose $\sqrt{2}$ were rational. Then we could write it as a fraction, $\sqrt{2} = a/b$, in lowest terms. In particular, saying that a/b is in lowest terms means that a and b are not both even.

Multiplying both sides of the equation by b yields

$$\sqrt{2}b = a.$$

Squaring both sides yields

$$2b^2 = a^2.$$

Since squaring an odd number yields an odd number, a has to be even, which means that it is twice some other number. In other words, for some number c, we have $a = 2c$. Then we have

$$\begin{aligned} 2b^2 &= (2c)^2 \\ &= 4c^2. \end{aligned}$$

Dividing both sides by 2 yields

$$b^2 = 2c^2.$$

But this means that b is also even, contradicting the fact that a/b is a fraction in lowest terms. $\square$

For another example, let us consider Euclid's proof that there are infinitely many prime numbers.

Definition. The set of *natural numbers*, denoted $\mathbb{N}$, is the set $\{0, 1, 2, 3, \ldots\}$. A number larger than 1 is *composite* if it is the product of two smaller numbers, and *prime* otherwise.

For example, 6 and 15 are composite, 7 and 11 are prime. Note that we are calling 0 and 1 neither prime nor composite.

Proposition. Every natural number other than 0 and 1 can be factored into primes. In other words, every natural number n other than 0 and 1 can be written in the form

$$n = p_1 \times p_2 \times p_3 \times \ldots \times p_k$$

where each p_i is prime.

Proof. Suppose n is a number other than 0 or 1. If n is prime, we are done. Otherwise, n can is composite, and so can be written as a product of smaller numbers, $n = k \times l$. If k and l are not both prime, repeat the process. Since the factors get smaller each time, the procedure has to end. $\square$

More precisely, one uses the principle of induction (or, equivalently, the least element principle) to justify the claim that the procedure described above has to stop. The "fundemantal theorem of arithmetic" makes the stronger statement that every natural number can be factored into primes in a *unique* way, up to the order of $p_1, \ldots, p_k$. This is somewhat harder to prove.

Theorem. There are infinitely many primes.

Another way of saying this is given any prime number, you can find a bigger one. The following proof can also be found in Euclid's *Elements.*

Proof. Suppose we are given a number, p. I will show you how to find a bigger one. Let

$$N = p \times (p - 1) \times \ldots \times 2 \times 1 + 1.$$

Notice that N is bigger than p. Furthermore, N has no factors less than or equal to p, because dividing N by any number between 2 and p leaves a remainder of 1.

Now, either N is prime or composite. If N is prime, we are done. Otherwise, factor N into primes. Then any of these factors is bigger than p, and we are done. $\square$

The Existence of God

The ontological argument (Anselm, Descartes):

1. We can conceive of a perfect being.
2. Anything that is conceived of exists in the mind of the conceiver.
3. It is more perfect to exist in actuality, than not to exist.
4. From 1 and 2, a perfect being exists in our minds.
5. From 4 and 3, this perfect being exists in actuality.

The cosmological argument (Aristotle, Aquinas):

1. Every event is caused by another event.
2. An infinite regress of causes is not possible.
3. From 1 and 2, there is a first cause.

God is, by definition, the first cause.

The argument from design (Aquinas, Descartes, Leibniz, Berkeley):

1. Things in the world show evidence of design.
2. There is no design without a designer.

God is, by definition, this designer.

Set theory, and the infinite

Definition. A function f from a set A to a set B is called a *bijection*, or a *one to one correspondence*, if for every element y of B there is exactly one element x of A such that $f(x) = y$. Two sets A and B are said to *have the same cardinality* if there is a bijection between them.

This definition provides a natural way of extending the notion of "has the same size" to infinite sets.

For example, let A be the set $\{1, 2, 3, 4\}$ and let B be the Beatles, i.e. the set $\{John, Paul, George, Ringo\}$. Let f be the function defined by $f(1) =$ John, $f(2) =$ Paul, $f(3) =$ George, $f(4) =$ Ringo. Then f is a bijection from

A to B, and so A and B have the same cardinality. This is a mathematical analysis of the assertion "There are four Beatles."

For another example, due to Galileo, let A be the set of natural numbers, and let B be the set of perfect squares,

$$B = \{0, 1, 4, 9, 16, \ldots\}.$$

Then A and B have the same cardinality, because $f(x) = x^2$ is a bijection between them.

The following is one version of Cantor's theorem.

Theorem. The set of natural numbers, $\mathbb{N}$, and the set of real numbers, $\mathbb{R}$, do *not* have the same cardinality.

Proof. Suppose we are given a function f from $\mathbb{N}$ to $\mathbb{R}$. Think of f as giving us an infinite list of real numbers,

$$f(0), f(1), f(2), \ldots$$

To show that f is not a bijection, it suffices to show that there is at least one number that is not on the list.

The proof uses the fact that every real number has an infinite decimal expansion

$$n.n_0 n_1 n_2 \ldots$$

where n is an integer, and each of $n_0, n_1, \ldots$ is a digit between 0 and 9.

Write each of $f(0), f(1), f(2), \ldots$ as an infinite decimal. Construct a sequence of digits $a_0, a_1, a_2, \ldots$ as follows: for each i, define a_i to be 3 if the ith digit of $f(i)$ after the decimal place is 7, and 7 otherwise. Now consider the number

$$0.a_0 a_1 a_2 a_3 \ldots$$

differs from $f(0)$ in the first digit, differs from $f(1)$ in the second digits, and so on. So this a real number is different from each one on the list. $\square$

The diagram below (with particular digits chosen as an example) shows why this argument is often called *Cantor's diagonal argument*: we have constructed a new number by changing each digit on the diagonal.