Proof by Contradiction

Constructive proof

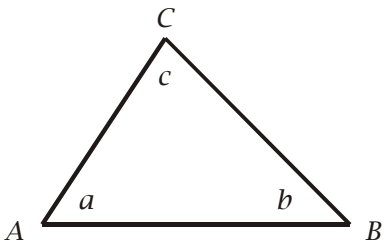
Mathematicians make use of results and theorems. These are statements of general truth that capture some part of our mathematical knowledge. For example, *the square root of a prime number is not a fraction, you cannot divide by zero,* and *there is an infinite number of prime numbers*, are examples of mathematical statements.

But how do we establish the truth of these statements? Broadly speaking, these truths are established in mathematics by one of three methods: (1) constructive proof, (2) mathematical induction and (3) proof by contradiction.

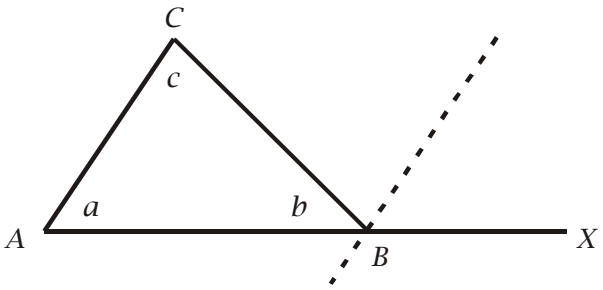
A constructive proof is as it sounds. It is a construction of the result from other well-known facts. Ultimately, there must be some primitive facts from which to construct a proof. These "facts" are called axioms. In his famous book, *The Elements*, the Greek mathematician Euclid claimed that there were just five axioms from which all the theorems of geometry could be derived. We think that he left some of the axioms out, and we have expanded the list to fourteen or so. Proofs in geometry are very often *constructive* proofs.

Example (1)
The proof that the angle sum of a triangle is 180° is an example of a constructive proof.

Proof
Let ABC be any triangle, with angles a, b and c respectively.



Extend the line AB to the point X as shown in the following diagram and construct a line, BY, parallel to AC passing through B.



Then the angle $C\hat{B}Y$ is equal to the angle *c* since they are alternating angles; and the angle $Y\hat{B}X$ is equal to the angle *a* since they are corresponding angles. However

$b + C\hat{B}Y + Y\hat{B}X = 180°$

since these angles add up to the angle subtended by a straight line, which by definition is 180°. Hence $b + c + a = 180°$ and the angle sum of any triangle is 180°.

This simple proof illustrates the general principles of a constructive proof. Firstly, the constructive proof builds on definitions and axioms.

Definitions

The angle subtended by a straight-line is 180°.

A triangle is a plane, closed figure of three straight lines.

Axioms

Alternating angles are equal

Corresponding angles are equal

Secondly, the constructive proof begins with the statement, "Let…". This introduces an arbitrary object (or figure). The only property assumed of this figure is that it is a triangle, so whatever is true of it is true of *all* triangles. The constructive proof rests on the idea of taking an argument true of *any* object to be also true of *all* objects of that kind. This is how the generality is created.

Example (2)

(*a*) Prove that for an arithmetic progression with first term *a* and common difference *d*, the sum to *n* terms is given by $S_n = \frac{n}{2}\left(2a + (n-1)d\right)$.

(*b*) Identify the definitions and axioms employed in this proof.

(*c*) Explain why the sum of an arithmetic progression is an example of a "short cut" theorem.

Solution

(*a*) **Proof**

The sum to n terms of the arithmetic progression with first term a and common difference d is

$S_n = u_1 + u_2 + u_3 + ... + u_{n-1} + u_n$

That is

$S_n = a + (a + d) + (a + 2d) + ... + (a + (n-1)d)$ (1)

Reversing the order of the terms in this then the sum is also given by

$S_n = u_n + u_{n-1} + u_{n-2} + ... + u_2 + u_1$

That is

$S_n = (a + (n-1)d) + (a + (n-2)d) + \ldots + (a + d) + a$ (2)

Adding the two equations, (1) and (2), together on a term by term basis we get

$2S_n = (2a + (n-1)d) + (2a + (n-1)d) + \ldots + (2a + (n-1)d)$

Thus, when we add up all the terms on a term-by-term basis we obtain $2a + (n-1)d$

added to itself n times. Hence

$2S_n = n(2a + (n-1)d)$

$\therefore S_n = \frac{n}{2}(2a + (n-1)d)$

(*b*) **Definitions**

1. Definition of a sequence as an ordered collection of numbers

   $u_1,\ u_2, u_3,\ \ldots, u_{n-1}, u_n, \ldots$

2. Definition of an arithmetic progression as a sequence with general term

   $u_n = (a + (n-1)d)$

3. Definition of the sum of an arithmetic progression to n terms

   $S_n = a + (a + d) + (a + 2d) + ... + (a + (n-1)d)$

Axioms

1. The axioms of algebra – a large topic in its own right that we will reserve full discussion to a further chapter. However, note that at the line after (1) above we wrote, "Reversing the order of the terms in this then the sum is also given by $S_n = u_n + u_{n-1} + u_{n-2} + ... + u_2 + u_1$". In this we were employing an axiom of algebra that says that when two numbers a and b are added are added the sum is the same regardless of the order in which they are added, $a + b = b + c$. Addition is said to be *commutative*. This is an example of an axiom of algebra.

2. The axioms of set theory. A sequence is a set of numbers. In fact, it is an *ordered* set of numbers. The rules for employing collections of numbers are called *axiomatic set theory*. The precise rules for axiomatic set theory is a matter of debate and it is possible to construct all the axioms of algebra from set theory.

(*c*) The theorem is a short cut from the sequence

$$S_n = a + (a + d) + (a + 2d) + ... + (a + (n-1)d)$$

to its sum $S_n = \frac{n}{2}(2a + (n-1)d)$ without having to go through the long-winded process of actually adding up all the terms. However, if we did not have the short cut we could always just add up all the terms. In a sense short cut theorems (constructive proofs generally) tell you nothing you did not know already.

Mathematical miscellany – an amusing story

Arguably the most famous mathematician of all time was Carl Friedrich Gauss (1777 – 1855). When he was seven years old his tutor set him the problem of adding up all the integers from 1 to 100. Guass did this almost immediately by identifying that the sum comprised 50 pairs of numbers each adding to 101. He had discovered the short cut theorem that we know as the sum of an arithmetic progression. That was bad news for his teachers! Among Guass's contributions to mathematics and science are (1) statistics – method of least squares, normal distribution. (2) physics and astronomy – developed of theory of potentials and established the existence of two magnetic poles for the Earth, identifying the location of the South Pole; accurately predicted the orbit of the asteroid *Ceres*. (3) Geometry – (Guassian) curvature of space, study of geodesics, anticipated the discovery of non-Euclidean geometry. (4) Land survey – invented the heliotrope. (5) Electricity – established Kirchhoff's circuit laws and collaborated with Weber to build the electromagnetic telegraph. (6) Contributions to number theory. (7) Finance – made a fortune by the analytical study of bonds.

Example (3)

Go through your entire maths course and list all the examples of constructive proofs you have met to date.

Solution

Here are some examples of constructive proofs you have met.

1. All the rules of indices.
2. The quadratic formula.
3. The remainder and factor theorems.
4. The sine and cosine rules.
5. The sum of a geometric progression.

6. The Cartesian equation of the circle.
7. The rules for logarithms.
8. All the trigonometric identities.
9. The rules for the differentiation of products, quotients and chains.

The limitations of constructive proof

One aspect of constructive proofs is that they are all really just short cuts. The result, *the angle sum of a triangle is 180° is* a short cut for the proof. So it would always be possible to reconstruct any proof that used this result by going back to the original definitions and axioms. Short cuts are very useful, but there is a sense in which the short cut provides you with nothing new. If there are two points in a town, *A* and *B*, you can still walk from *A* to *B* even if you do not know the short-cut between them!

Proof by contradiction

The idea behind a proof by contradiction is as follows. Suppose you assume that a result is true. You then proceed by techniques of constructive proof to *construct* a contradiction. This is a statement like "black is white" or "zero is one" or $\sqrt{2} \neq \sqrt{2}$. Such statements cannot be true. Therefore, you conclude that the original assumption must have been false. We will illustrate this with three well-known proofs by contradiction: *the square root of a prime number is not a fraction, you cannot divide by zero,* and *there is an infinite number of prime numbers.* Note, when a contradiction has been established, we often meet the phrase *reductio ad absurdam.* This is Latin for "reduced to absurdity" – in other words, by this phrase you indicate that the original assumption has lead to a contradiction, so the original assumption must be false. The use of this phrase will be illustrated in the proof that follows.

The irrationality of $\sqrt{2}$

To say that a number is "rational" is to say that it cannot be written as a fraction. A number is irrational if it is not rational – that means, if you cannot write it as a fraction. It is usual to be taught, without proof, at quite an early stage that the square root of any prime number is irrational, and that the number π is also irrational. The proof of the irrationality of π is beyond the scope of this introduction to proof by contradiction. However, the proof of the irrationality of

prime numbers is attributed to Pythagoras, who lived during the C6th BC, and we should be able to follow it. It begins by assuming the thing that we expect to be false, and then derives a contradiction from that assumption.

Proof of the irrationality of $\sqrt{2}$

Suppose $\sqrt{2}$ is rational. Then $\sqrt{2}$ can be written as a fraction, so it can be expressed as a ratio $\sqrt{2} = \frac{p}{q}$ where p and q are integers. We may also assume that p and q do not have any common factors, because if they did these common factors could be cancelled out. Taking the equation $\sqrt{2} = \frac{p}{q}$ and squaring both sides, we obtain $2 = \frac{p^2}{q^2}$. Hence

$$2q^2 = p^2 \qquad (1)$$

This means that p is an even number, since 2 is a factor of p. Hence

$$p = 2r$$

where r is a whole number. On substituting for p in equation (1) we obtain

$$2q^2 = (2r)^2$$

$$2q^2 = 4r^2$$

$$q^2 = 2r^2$$

This means that q is even. So both p and q are even. This contradicts our assumption that p and q had no common factors. Hence, by reductio ad absurdam, $\sqrt{2}$ is irrational.

You cannot divide by zero

Great care must be taken when manipulating algebraic expressions.

Example (4)

What is the error in the following argument?

$$0 = 0$$

$$1 \times 0 = 0 \times 0$$

$$\left(\tfrac{1}{2} + \tfrac{1}{2}\right)\left(\tfrac{1}{2} - \tfrac{1}{2}\right) = \left(\tfrac{1}{2} - \tfrac{1}{2}\right)\left(\tfrac{1}{2} - \tfrac{1}{2}\right)$$

$$\left(\tfrac{1}{2} + \tfrac{1}{2}\right) = \left(\tfrac{1}{2} - \tfrac{1}{2}\right)$$

$$1 = 0$$

Solution

This appears to be a paradox. Let us annotate the argument to see why.

$0 = 0$	[A true statement]
$1 \times 0 = 0 \times 0$	[Multiplying both sides by zero]
$\left(\frac{1}{2}+\frac{1}{2}\right)\left(\frac{1}{2}-\frac{1}{2}\right)=\left(\frac{1}{2}-\frac{1}{2}\right)\left(\frac{1}{2}-\frac{1}{2}\right)$	[$1=\frac{1}{2}+\frac{1}{2}$, and $0=\frac{1}{2}-\frac{1}{2}$]
$\left(\frac{1}{2}+\frac{1}{2}\right)=\left(\frac{1}{2}-\frac{1}{2}\right)$	[Cancelling both sides by $\left(\frac{1}{2}-\frac{1}{2}\right)$]
$1 = 0$	[This is a manifest absurdity]

Something must have gone wrong. The error was in line (4) where we divided both sides by $\left(\frac{1}{2}-\frac{1}{2}\right)$. This is equal to zero, so in effect we have divided both sides by zero. Since all the other steps must be valid, and since this action has led to an absurdity, we conclude by *reductio ad absurdam*, that you cannot divide both sides of an equation by zero.

Proof that there are an infinite number of prime numbers

The following proof was presented by Euclid in his work *The Elements* (c. 300 BC), though it is likely that it was already well known by the time he wrote his book.

Proof that there an infinite number of primes

Suppose there are only a finite number of prime numbers.

Let p_n be the last prime number, and let the prime numbers be listed in order thus

$p_1,\ p_2,\ p_3,\ .....,\ p_{n-1},\ p_n$

(Recall that $p_1 = 2,\ p_2 = 3,\ p_3 = 5,$ and so on)

Construct the following number

$M = (p_1 \times p_2 \times\ p_3 \times\ .....\times\ p_{n-1} \times p_n) + 1$

That is, *M* is the number that is formed by multiplying all the prime numbers together and then adding 1. This number is larger than p_n so it must be a composite number, meaning that it is not prime and has prime factors. Suppose p_k is a prime number that divides into *M*. Then p_k must be one of the prime numbers on the list $p_1,\ p_2,\ p_3,\ .....,\ p_{n-1},\ p_n$. So

$M = (p_1 \times p_2 \times\ p_3 \times\quad \times p_k \times\ .....\times\ p_{n-1} \times p_n) + 1$

Hence, since p_k divides into M then p_k divides into 1 since it divides into

$p_1 \times p_2 \times p_3 \times \quad \times p_k \times \ldots\ldots \times p_{n-1} \times p_n$

But no prime number divides into 1 (1 is not a prime number by definition).

Hence, by reductio ad absurdam M must be prime.

Since M is larger than p_n then p_n cannot be the largest prime number.

So there must be an infinite number of prime numbers.