NRICH

An Introduction to Proof by Contradiction

Age 14 to 18

Article by Katherine Körner and Vicky Neale

Published December 2005,February 2011.

Key to all mathematics is the notion of proof. We wish to be able to say with absolute certainty that a property holds for all numbers or all cases, not just those we've tried, and not just because it sounds convincing or would be quite nice if it were so. Certain types of proof come up again and again in all areas of mathematics, one of which is proof by contradiction.

To prove something by contradiction, we assume that what we want to prove is not true, and then show that the consequences of this are not possible. That is, the consequences contradict either what we have just assumed, or something we already know to be true (or, indeed, both) - we call this a contradiction.

A simple example of this principle can be seen by considering Sally and her parking ticket. We know that if Sally did not pay her parking ticket, she would have got a nasty letter from the council. We also know that she did not get any nasty letters. Either she paid her parking ticket or she didn't, and if she didn't then, from our original information, we know that she would have got a nasty letter. Since she didn't get a nasty letter, she must therefore have paid her ticket.

If we were formally proving by contradiction that Sally had paid her ticket, we would assume that she did not pay her ticket and deduce that therefore she should have got a nasty letter from the council. However, we know her post was particularly pleasant this week, and contained no nasty letters whatsoever. This is a contradiction, and therefore our assumption is wrong. In this example it all seems a bit long winded to prove something so obvious, but in more complicated examples it is useful to state exactly what we are assuming and where our contradiction is found.

One well-known use of this method is in the proof that $\sqrt{2}$ is irrational.

Rational numbers are those which can be written in fractions, that is as one integer divided by another ($1/2, 3/4, 4/2, 973/221, \ldots$). They can be put into what is called i*rreducible form* , which is where the numerator (top number) and denominator (bottom number) have no common factors other than 1, i.e. are coprime. Irrational numbers are those which cannot be put into such a form, such as π and - as we are about to see - $\sqrt{2}$.

Let us start by proving (by contradiction) that if p^2 is even then p is even, as this is a result we will wish to use in the main proof. We do this by considering a number p whose square, p^2, is even, and assuming that this p is not even. Then we try to arrive at a contradiction.

If p is not even, it is odd, and therefore of the form $2n + 1$, where n is a whole number. Then $p^2 = (2n + 1)^2 = 4n^2 + 4n + 1$. But $4n^2 + 4n$ is clearly even, so $4n^2 + 4n + 1$ is odd. This means p^2 is not even, so since we are only considering p *because* p^2 is even, we have a contradiction here. Therefore our assumption that p is not even must be wrong, i.e. p is even.

Now we are ready to start our proof that $\sqrt{2}$ is irrational, which of course we begin by assuming that it is not (i.e. that it is rational), and then trying to arrive at a contradiction.

Suppose $\sqrt{2}$ is rational. Then it can be written as p/q, where p and q are coprime integers.

Thus if $\sqrt{2} = p/q$ then squaring both sides gives $2 = p^2/q^2$.

Then $2q^2 = p^2$ and so p^2 is clearly even. If p^2 is even then we know from above that p must be even, and so can be written as $p = 2m$ where m is an integer. Thus $p^2 = 4m^2$ and so $2q^2 = 4m^2$.

Dividing $2q^2 = 4m^2$ through by 2 gives us that q^2 is also even, and so q must be even.

If p and q are both even then they have 2 as a common factor, which contradicts the assumption that they are coprime. Thus our assumption is incorrect, and $\sqrt{2}$ is not rational.
You may like to try this challenge http://nrich.maths.org/public/viewer.php?obj_id=1404&part=index which involves a slightly different proof by contradiction to prove the same result.
This alternative proof can be generalised to show that $\sqrt{n}$ is irrational when n is not a square number.

Proving something by contradiction can be a very nice method when it works, and there are many proofs in mathematics made easier or, indeed, possible by it. However, it is not always the best way of approaching a problem.

For instance, say for some reason we wish to prove that (positive) $\sqrt{4}$ is rational. Encouraged by our success with $\sqrt{2}$, we could suppose for a contradiction that $\sqrt{4}$ is not rational. Then it cannot be written as p/q where p and q are positive integers. However, if we let $p = 2$ and $q = 1$ then $(p/q)^2 = p^2/q^2 = 4/1 = 4$ Also, both 2 and 1 are positive, so $p/q = 2/1$ is positive. Thus $\sqrt{4} = 2/1$ so we have contradicted our assumption that $\sqrt{4}$ cannot be written as an integer divided by an integer. Therefore $\sqrt{4}$ is not irrational, i.e. it is rational.

All we really needed to do was point out that $\sqrt{4} = 2$, which is a perfectly good rational number in its own right. This would have been much quicker than going through the whole proof by contradiction. Even more importantly it was, in fact, a step in the above proof.

Having just warned you of the dangers of blindly trying to prove things by contradiction, we end with one of the nicest proofs - by contradiction or otherwise - I know. This is Euclid's proof that there are infinitely many prime numbers, and does indeed work by contradiction.

Before we begin this proof, we need to know that any natural number greater than 1 (so $2, 3, 4, \ldots$) has a prime factor.

We can prove this by, in fact, contradiction. Take the usual definition of a prime as a natural number greater than 1 divisible only by itself and 1. Suppose it is not the case that any natural number greater than 1 has a prime factor. Then there must be a least natural number greater than 1 which does not have a prime factor. Let us call this n. Then n is clearly not prime so it must have a factor m that is neither n nor 1. But m < n so m has a

prime factor p by assumption. Thus p is a factor of m, which is a factor of n, so p is a prime factor of n. Thus n has a prime factor, and this means it is not the case that there is a least natural number greater than 1 that does not have a prime factor. This therefore contradicts our assumption that not every natural number greater than 1 has a prime factor. So every natural number greater than 1 does have a prime factor.

Having proved this, we can now go on to our main proof.

We wish to prove there are infinitely many primes, so of course we suppose for contradiction that there are only finitely many, say n of them.

This means that we can list them: $\{p_1, p_2, p_3, \ldots, p_n\}$. Consider their product, $p_1 \times p_2 \times \cdots \times p_n = \prod_{i=1}^{n} p_i$. Now $\prod_{i=1}^{n} p_i + 1$ is a natural number (as it is the sum of two natural numbers) and it is clearly greater than 1. Thus as was noted earlier, it has a prime factor. Can you see where we need to go from here?

* * * * * * * * *

The answer is that $\prod_{i=1}^{n} p_i + 1$ has a prime factor, p. Since we are assuming that there are finitely many primes, p is one of $\{p_1, p_2, p_3, \ldots, p_n\}$. Thus p divides $\prod_{i=1}^{n} p_i$, too. Now, p cannot divide both $\prod_{i=1}^{n} p_i$ and $\prod_{i=1}^{n} p_i + 1$, or else it would divide their difference, 1.

Thus p is not in our complete list of primes, and so we have arrived at a contradiction. There are therefore infinitely many primes.

At the time of writing this article *Katherine was a third year undergraduate mathematician at Balliol College, Oxford.*
Vicky had just finished a degree in Maths at Cambridge and was doing a fourth year course studying Combinatorics, Number Theory and Algebra, still at Trinity College, Cambridge.