ClassRoom

HOW to PROVE it

SHAILESH SHIRALI

In this episode of "How To Prove It", we consider two similar sounding terms which have great significance in higher mathematics: contradiction and contrapositive. Both of them arise in connection with proofs. We give several examples of proofs of both these kinds.

A phrase used very often in higher mathematics is 'proof by contradiction.' A vast number of results are proved using this approach. Readers of *At Right Angles* would have seen this proof technique used numerous times.

A less familiar phrase is 'proof by the contrapositive.' But appearances are deceptive; though the phrase itself is not used so often, the approach is very widely used.

Both of these are examples of *indirect proof techniques*. In this edition of 'How to Prove It,' we dwell on proof by contradiction and proof by the contrapositive and explain what is 'indirect' about them.

Matters of notation

We shall use the following standard notation throughout this article.

- If integers a, b, c $(c \neq 0)$ are such that a and b leave the same remainder under division by c, then we write $a \equiv b \pmod{c}$. Otherwise put: $a \equiv b \pmod{c}$ means that $a - b$ is a multiple of c. Examples: $27 \equiv 7 \pmod{5}$; $53 \equiv 19 \pmod{17}$.
- If integers a, b $(a \neq 0)$ are such that a is a divisor of b, we write: $a \mid b$. Examples: $7 \mid 21$; $17 \mid 85$.
- Negation is indicated as follows: $13 \not\equiv 2 \pmod{5}$; $5 \nmid 12$; $2 \nmid 3$.

Keywords: Proof, direct proof, indirect proof, contradiction, contrapositive

Well-known facts from elementary number theory. We shall make repeated use of some well-known (and easily proved) results from elementary number theory, namely:

- If n is any integer, then $n^2 \equiv 0 \pmod 3$ or $n^2 \equiv 1 \pmod 3$.
- In particular, if n is not a multiple of 3, then $n^2 \equiv 1 \pmod 3$.
- If n is any integer, then $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.
- In particular, if n is odd, then $n^2 \equiv 1 \pmod 4$.
- There are no squares of the following forms: $2 \pmod 3$, $2 \pmod 4$, $3 \pmod 4$.

Direct proof and indirect proof

Direct proof. To start with, let us explain what is meant by 'direct proof.' Let us say that some statement or proposition q needs to be proved. The direct approach is to start with some statement p of an elementary and basic nature that is clearly true, and then go through a series of deductive steps which yield a sequence of statements, each of which is implied by the previous one, culminating in the statement q to be proved. That is, we start with some statement p whose truth is beyond dispute, then move through a sequence of statements $p_1, p_2, p_3, \ldots, p_n, q$ as follows:

$$p \implies p_1, \quad p_1 \implies p_2, \quad p_2 \implies p_3, \quad \ldots, \quad p_n \implies q.$$

At the end of this chain of reasoning, proposition q has been proved, as required.

Rather then a standalone proposition that needs to be proved, we may be faced with the task of proving an ***implication***, say $p \implies q$. That is, we need to show that ***if*** proposition p is true, ***then*** proposition q is true as well. Observe the 'if then' nature of what is to be proved.

In some cases, we may be able to show the desired implication in a single step. In case this proves difficult, we may opt to interpose a sequence of propositions $p_1, p_2, p_3, \ldots, p_n$ between p and q, and then establish the following implications:

$$p \implies p_1, \quad p_1 \implies p_2, \quad p_2 \implies p_3, \quad \ldots, \quad p_n \implies q.$$

The point of bringing in the additional propositions is that the in-between implications may be easier to establish. So, rather than take one large step, we take a number of relatively small steps, each of which is not too difficult in itself. At the end of this line of reasoning, the desired implication will have been proved. This too is a direct proof.

What is 'direct' about these approaches is that we have accomplished the desired task 'directly.' In the first situation, proposition q had to be proved; we have done so. In the second situation, the implication $p \implies q$ had to be proved; once again, we have done so.

Indirect proof. The path taken by an indirect proof is very different. It rests on the basic premise that *a proposition is either true or false*. This means that if a proposition is not true, it must be false; if it is not false, then it must be true.

This offers another way of proving a given proposition q to be true: show that it cannot be false! How do we do this? One way would be to assume q to be false, take *that* to be our starting point, and explore its consequences. If at some point we come across a consequence that we definitely *know* to be false, or a consequence that contradicts something we proved earlier, then we can conclude that the assumption made at the start (i.e., that q is false) is *itself* false. So q cannot be false and therefore it must be true!

Observe what has taken place here: the assumption that q is false has caused us to trip ourselves (to put it more colourfully, we have tripped on our own shoelaces), and therefore we are forced to conclude that there must be something wrong with this assumption. This manner of proceeding is known as *proof by contradiction*.

A similar line of reasoning can be used if we wish to show the truth of the implication $p \implies q$.

We assume that q is false and check whether we can show, in some way or the other, that p too is false. That is, the falsity of q leads to the falsity of p. But we have already been told that p is true; this is a given. From this, we conclude that q cannot be false; therefore, it must be true. This manner of proceeding is known as *proof by the contrapositive.*

It should be clear now why these two approaches are described as 'indirect.'

Examples of direct proof

(i) Prove that if m is an odd integer, then $m^2 \equiv 1 \pmod 8$.

Solution. An odd integer m can be written in the form $2n + 1$ where n is an integer. Squaring this expression, we get:

$$\begin{aligned} m^2 &= (2n+1)^2 \\ &= 4n^2 + 4n + 1 \\ &= 4n(n+1) + 1. \end{aligned}$$

In the last line, we focus our attention on the term $n(n + 1)$. Observe that it is a product of a pair of consecutive integers. One of these integers must be even, so their product is necessarily even. Hence $8 \mid 4n(n + 1)$. It follows that $m^2 \equiv 1 \pmod 8$. ■

(ii) *Prove the arithmetic mean-geometric mean (AM-GM) inequality: if a and b are any two positive real numbers, then $\frac{1}{2}(a+b) \geq \sqrt{ab}$.* (Here, $\frac{1}{2}(a+b)$ is the AM of a and b, while $\sqrt{ab}$ is the GM of a and b.)

Solution. We shall start with a statement that is clearly true: *the square of any real number is non-negative*. Applying this statement to the particular real number $\sqrt{a} - \sqrt{b}$, we deduce that

$$\left(\sqrt{a} - \sqrt{b}\right)^2 \geq 0.$$

Expanding the bracketed term and simplifying, we get:

$$\begin{aligned} a + b - 2\sqrt{ab} &\geq 0, \\ \therefore\ \frac{a+b}{2} &\geq \sqrt{ab}. \end{aligned}$$ ■

(iii) *Prove that the cube root of 3 exceeds the square root of 2.* (This is generally asked as a question: *Which is larger, $2^{1/2}$ or $3^{1/3}$?*)

Solution. We shall start with a statement that is clearly true: $9 > 8$. Taking the (real) sixth roots of both sides, we deduce that $9^{1/6} > 8^{1/6}$, hence

$$\begin{aligned} &\left(3^2\right)^{1/6} > \left(2^3\right)^{1/6}, \\ &\therefore\ 3^{1/3} > 2^{1/2}. \end{aligned}$$ ■

(iv) *In $\triangle ABC$, sides AB and AC have equal length. Prove that $\measuredangle ABC = \measuredangle ACB$.*

Solution. We give the original proof from Euclid's ***Elements*** (with the language modified slightly, so as to make it easier to understand).

It is very important to note the placement of this theorem in the original sequence of results proved by Euclid. *The only congruence theorem available to us is what we now call side-angle-side ('SAS') congruence.* In particular, the angle-side-angle ('ASA') and side-side-side ('SSS') congruence theorems are not available as they are themselves proved later on. The ingenuity of Euclid's proof is striking.

Let ABC be isosceles with $AB = AC$. Extend sides AB and AC to points D and E respectively such that $AD = AE$. (See Figure 1.)

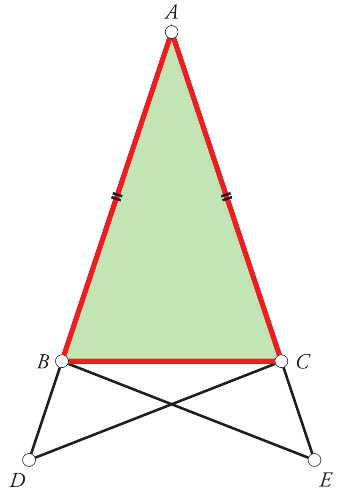

Figure 1.

By the SAS congruence theorem, $\triangle ABE$ is congruent to $\triangle ACD$; for: $AB = AC$, $AE = AD$, and the two triangles have a shared included angle, namely $\measuredangle A$. Therefore $BE = CD$ and $\measuredangle AEB = \measuredangle ADC$.

In the same way, we see that $\triangle BCD$ is congruent to $\triangle CBE$; for: $BD = CE$ (because $AD = AE$ and $AB = AC$), $CD = BE$ (just proved) and $\measuredangle BDC = \measuredangle CEB$ (just proved). Therefore $\measuredangle DBC = \measuredangle ECB$.

Since the straight angle at B equals the straight angle at C, it follows by subtraction that $\measuredangle ABC = \measuredangle ACB$. ■

Remark. There is another direct proof of this result which is not in Euclid's original text; it was found by Pappus a few centuries later; see [1]. It is a very ingenious proof but also counterintuitive. For example, it regards $\triangle ABC$ as a distinct object from $\triangle ACB$. For this reason, it has been described by some authors as "conceptually difficult."

Examples of indirect proof

(i) Prove that the integer 80000000000007 is not a perfect square.

Solution. A direct proof of this statement would involve computation of the square root of the given integer. The indirect proof is shorter; we make use of the first result proved in the previous section on direct proof: if m is an odd integer, then $m^2 \equiv 1 \pmod 8$. Note that this implies that any odd square is of the form $1 \pmod 8$.

Observe that the given integer is odd, and also observe that under division by 8, it leaves remainder 7. However, an odd square leaves remainder 1 under division by 8. It follows that 80000000000007 is not a perfect square. ■

(ii) *Prove that the square root of 2 is an irrational number.*

Solution. Just for fun, we give a proof that is slightly different from Euclid's original proof. (However, it is essentially modelled on that proof.)

Suppose that the square root of 2 is a rational number, say $\sqrt{2} = a/b$ where a and b are positive integers. Naturally, we may suppose that a and b share no common factors other than 1, i.e., a, b are coprime.

From the relation $\sqrt{2} = a/b$ we get, by squaring and simplifying, $a^2 = 2b^2$.

Now we ask: is either a or b divisible by 3? Suppose that $3 \mid a$. Then the relation $a^2 = 2b^2$ leads us to conclude that $3 \mid b$ as well. (Please fill in the details of the reasoning used to draw this conclusion.) But then $3 \mid a$ and $3 \mid b$, contrary to what we said above (that a and b are coprime). Hence a is not divisible by 3. If we suppose that $3 \mid b$, then by following the same reasoning, we are led to conclude that $3 \mid a$, and this again goes counter to what we said above; hence b is not divisible by 3. It follows that neither a nor b is divisible by 3.

The last statement implies that $a^2 \equiv 1 \pmod 3$ and $b^2 \equiv 1 \pmod 3$. From the second of these statements, we deduce that $2b^2 \equiv 2 \pmod 3$. But this contradicts the statement that $a^2 = 2b^2$, so we reach a contradictory state of affairs. It follows that the square root of 2 is not a rational number. ■

(iii) *Prove that if a, b, c are odd integers, then the equation $ax^2 + bx + c = 0$ has irrational roots.* Otherwise put: *if a, b, c are odd integers, then the expression $ax^2 + bx + c$ cannot be factorised over the rational numbers.*

Solution. The roots of the equation $ax^2 + bx + c = 0$ are the two quantities

$$\frac{-b \pm \sqrt{D}}{2a},$$

where $D = b^2 - 4ac$ is the discriminant. As a, b, c are integers, the roots are rational if and only if D is a perfect square. Expressed negatively, the roots are irrational if and only if D is *not* a perfect square.

So we need to establish that $b^2 - 4ac$ is not a perfect square. We need to do so under the hypothesis that a, b, c are all odd integers. Suppose this is not so; i.e., suppose that $b^2 - 4ac = d^2$, where d is an integer. Note that d^2 is odd, and therefore so is d. We now have:

$$b^2 - d^2 = 4ac.$$

We now use the following (proved above): *if m is an odd integer, then* $m^2 \equiv 1 \pmod 8$. This fact implies that $8 \mid b^2 - d^2$.

On the other hand, the quantity $4ac$ is of the form $4 \times$ an odd integer, which means that it cannot be a multiple of 8; indeed, we have $4ac \equiv 4 \pmod 8$.

This means that the equality $b^2 - d^2 = 4ac$ cannot hold. Hence the supposition that the discriminant $b^2 - 4ac$ is a perfect square cannot hold. It follows that the roots of the given equation are irrational. ■

(iv) Consider any three distinct perfect squares in arithmetic progression. Prove that the common difference of the AP is a multiple of 24.

Solution. Let the three squares be a^2, b^2 and c^2, where $a^2 < b^2 < c^2$. As they are in AP, we have $b^2 - a^2 = c^2 - b^2$, i.e., $2b^2 = a^2 + c^2$, which also implies that $c^2 = 2b^2 - a^2$. Let d be the common difference of the AP.

We may as well suppose that a, b, c are coprime. For, if they have divisors in common other than 1, we can divide all three of a, b, c by the common divisor and prove the proposition for the smaller squares. If proved, the proposition will then apply as well to the original squares.

We first focus attention on a. Suppose that a is even. If b too is even, then from the relation $c^2 = 2b^2 - a^2$, it follows that c too is even. However, we had already supposed that a, b, c are coprime, so the possibility of all three of a, b, c being even is not allowed. Next, suppose that b is odd. In that case we have $b^2 \equiv 1 \pmod 4$, which means that $d \equiv 1 \pmod 4$; but this leads to $c^2 \equiv 2 \pmod 4$. However, no square is of this form. As both the possibilities (b even, b odd) have led to contradictions, we are forced to conclude that a is not even; hence a is odd.

Now we focus attention on b. If b is even, then the relation $c^2 = 2b^2 - a^2$ implies that $c^2 \equiv -1 \pmod 4$; but this is not possible as no square is of this form. It follows that b cannot be even. Hence b is odd. This proves that c is odd as well (again using the relation $c^2 = 2b^2 - a^2$). That is, all three of a, b, c are odd. This implies that all three of a^2, b^2, c^2 are of the form $1 \pmod 8$, hence d is a multiple of 8.

We again focus attention on a. Suppose that $3 \mid a$. If $3 \mid b$ as well, then by virtue of the relation $c^2 = 2b^2 - a^2$, it follows that $3 \mid c$ too. However, we had already supposed that a, b, c are coprime, so this is disallowed. Hence b is not a multiple of 3. This leads to $b^2 \equiv 1 \pmod 3$, which means that $d \equiv 1 \pmod 3$. However, this in turn leads to $c^2 \equiv 2 \pmod 3$, which is not possible as no square is of the form $2 \pmod 3$. As both the possibilities have led to contradictions, we are forced to conclude that a is not a multiple of 3. Hence we have $a^2 \equiv 1 \pmod 3$.

Now we focus attention on b. If $3 \mid b$, then the relation $c^2 = 2b^2 - a^2$ would imply that $c^2 \equiv -1 \pmod 3$; but no square is of this form. It follows that b is not a multiple of 3. Hence we have $b^2 \equiv 1 \pmod 3$. From this it follows that d is a multiple of 3.

(From this, one may deduce that c too is not a multiple of 3; we again use the relation $c^2 = 2b^2 - a^2$. So all three of a, b, c are non-multiples of 3. However, we do not need to use this fact.)

Since $8 \mid d$ and $3 \mid d$, it follows that $24 \mid d$, as required. ■

Remark. Here are a few triples (a, b, c) of coprime positive integers for which a^2, b^2 and c^2 are in arithmetic progression (d is the common difference):

(a, b, c)	(a^2, b^2, c^2)	d
$(1, 5, 7)$	$(1, 25, 49)$	24
$(1, 29, 41)$	$(1, 841, 1681)$	840
$(7, 13, 17)$	$(49, 169, 289)$	120
$(7, 17, 23)$	$(49, 289, 529)$	240
$(17, 25, 31)$	$(289, 625, 961)$	336
$(23, 37, 47)$	$(529, 1369, 2209)$	840
$(31, 41, 49)$	$(961, 1681, 2401)$	720

(v) *In $\triangle ABC$, the angles opposite AB and AC have equal measure, i.e., $\measuredangle ABC = \measuredangle ACB$. Prove that sides AB and AC have equal length.*

Solution. In Euclid's text, this proposition comes immediately after the proposition that the base angles of an isosceles triangle are equal. So the only congruence result available to us is the SAS congruence theorem. The way Euclid handles this restriction is remarkable. It is a masterly demonstration of proof by contradiction. (As earlier, we have modified Euclid's original proof, to the extent of using words and sentences that would be more familiar to us in the current time.)

We are told that in $\triangle ABC$, $\measuredangle ABC = \measuredangle ACB$. We must prove that $AB = AC$. We shall suppose the contrary and show that this supposition leads to a contradiction.

Suppose that equality does not hold, i.e., $AB \neq AC$. Then one of them is greater than the other. Without loss of generality, we may suppose that $AB > AC$.

Locate point D on side AB such that $DB = AC$ (see Figure 2). This is possible as we have assumed that $AB > AC$.

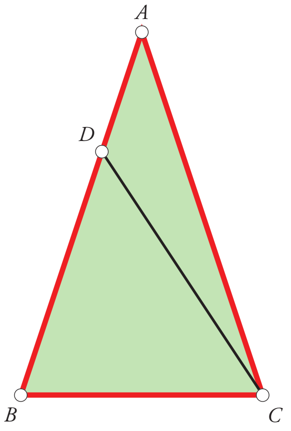

Figure 2.

Now consider the two triangles, $\triangle ACB$ and $\triangle DBC$. We have: $AC = DB$ (by construction); $CB = BC$ (this is a shared side); and $\measuredangle ACB = \measuredangle DBC$ (this is given; remember that $\measuredangle DBC$ is the same as $\measuredangle ABC$). It follows (SAS congruence) that $\triangle ACB$ is congruent to $\triangle DBC$.

But this is absurd, as $\triangle DBC$ is contained strictly within $\triangle ACB$. We have reached a self-contradiction.

The contradiction tells us that our initial supposition is itself incorrect; that is, the supposition that $AB \neq AC$ is false.

Hence $AB = AC$. ■

References

1. Proposition 5: Pappus's proof. https://mathcs.clarku.edu/ djoyce/java/elements/bookI/propI5.html
2. Proof by contradiction. https://en.wikipedia.org/wiki/Proof_by_contradiction
3. Contrapositive. https://en.wiktionary.org/wiki/contrapositive
4. Conditional Statement Forms. https://www.csm.ornl.gov/ sheldon/ds/sec1.2.html

SHAILESH SHIRALI is the Director of Sahyadri School (KFI), Pune, and heads the Community Mathematics Centre based in Rishi Valley School (AP) and Sahyadri School KFI. He has been closely involved with the Math Olympiad movement in India. He is the author of many mathematics books for high school students, and serves as Chief Editor for *At Right Angles*. He may be contacted at shailesh.shirali@gmail.com.

MAKING SENSE OF MATHEMATICS

A Visual Proof that $(a + b)^2 \neq a^2 + b^2$

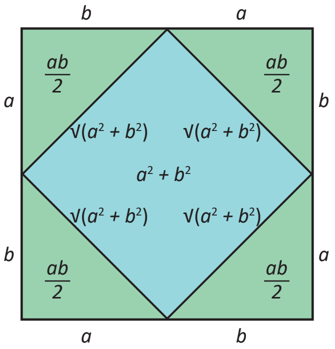

Figure 1: Seeing the difference

Many students have been drilled to remember that $(a + b)^2 \neq a^2 + b^2$. But a picture that makes sense can create a much more lasting impression and long term learning.

Figure 1 may persuade students that $(a + b)^2 \neq a^2 + b^2$.

The smaller inner square has sides of length $\sqrt{}(a^2 + b^2)$ since each side is the hypotenuse of a right triangle with legs a and b, so the area of the inner square is $[\sqrt{}(a^2 + b^2)]^2 = a^2 + b^2$.

The larger outer square has an area of $(a + b)^2$, so $(a + b)^2 \neq a^2 + b^2$.

Furthermore, the combined area of the four triangles is $2ab$, which is how much the area of the large square exceeds that of the smaller square.

That is, $(a + b)^2 = a^2 + b^2 + 4\,\frac{ab}{2} = a^2 + b^2 + 2ab$.