How To Prove It

SHAILESH SHIRALI

In Part I of this article, we remarked that there are essentially three components of a proof by induction:

Step 0: Framing the hypothesis or conjecture.

Step 1: Anchoring the induction, i.e., verifying the initial step.

Step 2: The bridge step, i.e., establishing the link between successive propositions of the induction hypothesis.

We dwelt at length on Step 0 (framing the hypothesis or conjecture), remarking that this step is generally completely ignored in the teaching of mathematics, thereby giving the impression that the formula to be proved literally comes out of nowhere. To illustrate this, let me quote an actual experience that I have often had as a mathematics teacher at the class 11 level: I ask the class to prove, using the principle of induction, that the sum of the squares of the first n natural numbers is equal to $n(n+1)(2n+1)/6$. Most of them are able to do so successfully. And then, a student comes after the class and asks, "Excuse me, we have proved this formula using the principle of induction; but where did we get this formula in the first place?" This innocent question captures the precise point that we are trying to make.

Having dwelt on this point in detail earlier, we now dwell on the remaining two steps by focusing on a few case studies. We shall study some examples that may not be so familiar to readers.

Abstract structure of a proof by induction

To start with, we describe in abstract the essential features of Steps 1 and 2 of a proof by induction.

Our intention is to establish that a certain given proposition $P(n)$ is true for all positive integers n. Note that $P(n)$ is a *proposition* for each positive integer n; it is either true or false.

Keywords: Proof by induction, hypothesis, conjecture, anchor, bridge step

We start (Step 1) by showing that $P(1)$ is true. This typically simply consists of verifying a numerical equality.

Next (Step 2) we show that for an arbitrary positive integer k, the truth of $P(k)$ implies the truth of $P(k+1)$. Expressed compactly: we show that the implication

$$P(k) \implies P(k+1) \tag{1}$$

is true for any arbitrary positive integer k.

Here, the emphasis on the word 'arbitrary' needs to be noted. Precisely because k is arbitrary, what the above establishes is the following infinite chain of implications:

$$P(1) \implies P(2) \implies P(3) \implies P(4) \implies \cdots. \tag{2}$$

The conclusion is now: $P(1)$ is true, therefore $P(2)$ is true, therefore $P(3)$ is true, therefore $P(4)$ is true, and so on, indefinitely. In short, $P(n)$ is true for every positive integer n. So we have proved what we set out to prove. In practice, we do not bother to write this final sentence. We simply write: "As (1) and (2) have been proved, it follows that $P(n)$ is true for every positive integer n."

A few familiar examples

Example 1 (Sums of squares of the natural numbers)**.** The sum of the squares of the first n natural numbers is equal to $n(n+1)(2n+1)/6$.

This is the result about which the student had registered a protest! But we have already described in the first part of this article (the July 2020 issue of AtRiA) how it is possible to hit upon this formula by playing with the sequence.

Note carefully the sequence of steps set out below. Also note the notation that we use.

We start by defining $P(n)$ to be the proposition (or assertion),

$$\textit{The sum of the squares of the first n natural numbers is } \frac{n(n+1)(2n+1)}{6}. \tag{3}$$

Step 1 (anchor): We check that the conjectured relationship or proposition is true for some initial value of n, typically $n = 1$. In this instance, it amounts to checking that the first squared number (i.e., 1^2) is equal to

$$\frac{1 \times 2 \times 3}{6}.$$

This is clearly true (both sides are equal to 1). So $P(1)$ is true.

Step 2 (inductive step): We proceed to show that for any arbitrary positive integer k, the truth of $P(k)$ implies the truth of $P(k+1)$. So we must verify that

$$P(k) \implies P(k+1),$$

for an arbitrary positive integer k. Now, $P(k)$ is the assertion that

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6},$$

while $P(k+1)$ is the assertion that

$$1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}.$$

Therefore, proving that $P(k) \implies P(k+1)$ is the same thing as proving that

$$\frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}.$$

This in turn is equivalent to proving that

$$\frac{(k+1)(k+2)(2k+3)}{6} - \frac{k(k+1)(2k+1)}{6} = (k+1)^2,$$

$$\text{i.e.,} \quad (k+2)(2k+3) - k(2k+1) = 6(k+1).$$

The verification of the last line takes an instant. It follows that the stated formula giving the sum of the squares of the first n positive integers is true.

Example 2 (A divisibility problem)**.** The quantity $9^n - 2^n$ is a multiple of 7 for every positive integer n.

As earlier, we start by defining $P(n)$ to be the proposition,

$$\textit{The quantity } 9^n - 2^n \textit{ is a multiple of } 7. \qquad (4)$$

Step 1 (anchor): We check that the proposition is true for $n = 1$. In this instance, it amounts to checking that $9 - 2$ is a multiple of 7. This is true. So $P(1)$ is true.

Step 2 (inductive step): We must show that for any arbitrary positive integer k, the truth of $P(k)$ implies the truth of $P(k+1)$. Now, $P(k)$ is the assertion that

$$9^k - 2^k \textit{ is a multiple of } 7,$$

while $P(k+1)$ is the assertion that

$$9^{k+1} - 2^{k+1} \textit{ is a multiple of } 7.$$

This implication can be shown in several ways. Here is one such. Since $9^k - 2^k$ is a multiple of 7, we write

$$9^k - 2^k = 7m$$

for some integer m. We now have:

$$\begin{aligned} 9^{k+1} - 2^{k+1} &= 9 \cdot 9^k - 2 \cdot 2^k \\ &= 9 \cdot \left(2^k + 7m\right) - 2 \cdot 2^k \\ &= 7 \cdot 2^k + 63m = 7\left(2^k + 9m\right). \end{aligned}$$

The last line shows clearly that $9^{k+1} - 2^{k+1}$ is a multiple of 7. So we have shown that $P(k) \implies P(k+1)$. Since $P(1)$ is true, it follows that $9^n - 2^n$ is a multiple of 7 for all positive integers n.

A few not-so-familiar examples

Before continuing, we note that there are two obvious variations which may occur in the standard proof by induction.

- The conjecture may have to be proved not from $n = 1$ but from some subsequent point. For example, we may have a statement like this: "Such and such a statement is true for all integers $n \geq 3$." (Example: "For all integers $n \geq 3$, the sum of the angles of a n-sided convex polygon is equal to $(n-2)180°$.") In such cases, we must anchor the induction suitably, i.e., start by verifying the conjecture for the base value of the argument.

- The conjecture may have to be proved not for all positive integers n but for some suitable subset of the positive integers; for example, for all odd positive integers n; or for all positive integers n of the form 1 (mod 3); and so on. In such cases, the inductive step has to be modified suitably. The way this has to be done will depend on the specifics of the situation.

Some of the examples shown below exhibit these features.

Example 3 (Another divisibility problem)**.** The quantity $2^n + 3^n$ is a multiple of 5 for all odd positive integers n.

As earlier, we start by defining $P(n)$ to be the proposition,

$$\textit{The quantity } 2^n + 3^n \textit{ is a multiple of } 5. \tag{5}$$

So we have to prove that the propositions $P(1)$, $P(3)$, $P(5)$, $P(7)$, ... are all true.

Step 1 (anchor): We check that the proposition is true for $n = 1$. In this instance, it amounts to checking that $2 + 3$ is a multiple of 5. This is true. So $P(1)$ is true.

Step 2 (inductive step): We are required to prove the proposition for the *odd* integers. To move from each odd integer to the next one requires an addition of 2. So our task is the following. We must show that for any arbitrary positive integer k, the truth of $P(k)$ implies the truth of $P(k+2)$. Now, $P(k)$ is the assertion that

$$2^k + 3^k \textit{ is a multiple of } 5,$$

while $P(k+2)$ is the assertion that

$$2^{k+2} + 3^{k+2} \textit{ is a multiple of } 5.$$

This implication can be shown in several ways. Here is one such. Since $2^k + 3^k$ is a multiple of 5, we write

$$2^k + 3^k = 5m$$

for some integer m. We now have:

$$\begin{aligned} 2^{k+2} + 3^{k+2} &= 4 \cdot 2^k + 9 \cdot 3^k \\ &= 4 \cdot 2^k + 9 \cdot \left(5m - 2^k\right) \\ &= 45m - 5 \cdot 2^k = 5\left(9m - 2^k\right). \end{aligned} \tag{6}$$

The last line shows clearly that $2^{k+2} + 3^{k+2}$ is a multiple of 5. So we have shown that $P(k) \implies P(k+2)$. Since $P(1)$ is true, it follows that $2^n + 3^n$ is a multiple of 5 for all odd positive integers n.

Comment. A little tweak to the above analysis shows that we can get more from this line of thinking than had been asked for at the start. From the relation (6) obtained above, we see that:

$$2^{k+2} + 3^{k+2} = 9 \cdot \left(2^k + 3^k\right) - 5 \cdot 2^k. \tag{7}$$

Since $5 \cdot 2^k$ is a multiple of 5, and 9 is coprime to 5, relation (7) implies the following:

$$2^{k+2} + 3^{k+2} \text{ is a multiple of } 5 \iff 2^k + 3^k \text{ is a multiple of } 5. \tag{8}$$

Since $2^2 + 3^2 = 13$ is not a multiple of 5, the above relation (8) shows that the quantities

$$2^4 + 3^4, \quad 2^6 + 3^6, \quad 2^8 + 3^8, \quad 2^{10} + 3^{10}, \quad \ldots$$

are all non-multiples of 5.

Example 4 (Yet another divisibility problem)**.** The quantity $1^n + 2^n + 3^n + 4^n$ is a multiple of 5 for all positive integers n except the multiples of 4.

We start by defining $P(n)$ to be the proposition,

$$\textit{The quantity } 1^n + 2^n + 3^n + 4^n \textit{ is a multiple of } 5. \tag{9}$$

So we must prove that the propositions $P(1)$, $P(2)$, $P(3)$, $P(5)$, $P(6)$, ... are all true.

As the proposition to be proved is of a more complex nature, we can expect to have to apply the inductive approach in a more flexible manner.

Step 1 (anchor): In general, this step consists of a single verification. However, the situation is of an unusual nature here. So we shall examine whether the propositions $P(1)$, $P(2)$, $P(3)$, $P(4)$ are true. Here are the results:

n	$1^n + 2^n + 3^n + 4^n$	Divisible by 5?	Conclusion
1	10	Yes	$P(1)$ is true
2	30	Yes	$P(2)$ is true
3	100	Yes	$P(3)$ is true
4	354	No	$P(4)$ is **not** true

Step 2 (inductive step): We have just seen that $P(n)$ is true for $n = 1, 2, 3$, and false for $n = 4$. The wording of the proposition suggests that this pattern will repeat: $P(n)$ will be found to be true for $n = 5, 6, 7$, and false for $n = 8$. Observe that the numbers in the second group are 4 more than the numbers in the first group. This suggests the strategy we need to use. Instead of advancing from n to $n + 1$ (as we generally do), or from n to $n + 2$ (as we did in the previous example), why don't we advance from n to $n + 4$? That is, why don't we try to prove the following? —

$$P(n) \implies P(n+4). \tag{10}$$

This is just the task that we now take up. We have:

$$\begin{aligned} &\left(1^{n+4} + 2^{n+4} + 3^{n+4} + 4^{n+4}\right) - \left(1^n + 2^n + 3^n + 4^n\right) \\ &= \left(1 + 16 \cdot 2^n + 81 \cdot 3^n + 256 \cdot 4^n\right) - \left(1^n + 2^n + 3^n + 4^n\right) \\ &= 15 \cdot 2^n + 80 \cdot 3^n + 255 \cdot 4^n. \end{aligned}$$

The above result shows that

$$\left(1^{n+4} + 2^{n+4} + 3^{n+4} + 4^{n+4}\right) - \left(1^n + 2^n + 3^n + 4^n\right) \tag{11}$$

is a multiple of 5. Hence:

$$1^{n+4} + 2^{n+4} + 3^{n+4} + 4^{n+4} \text{ is a multiple of } 5 \tag{12}$$

$$\iff 1^n + 2^n + 3^n + 4^n \text{ is a multiple of } 5. \tag{13}$$

The above relation shows that we have proved more than what was required! We had set out to prove that $P(n) \implies P(n + 4)$; instead we have proved:

$$P(n) \iff P(n+4). \tag{14}$$

We already know that $P(1)$ is true. From the above relation, we deduce that all of the following are true as well:

$$P(5), \quad P(9), \quad P(13), \quad P(17), \quad P(21), \quad \ldots.$$

Similarly, as we already know that $P(2)$ and $P(3)$ are true, we deduce that all of the following are true as well:

$$P(6),\quad P(10),\quad P(14),\quad P(18),\quad P(22),\quad \dots,$$
$$P(7),\quad P(11),\quad P(15),\quad P(19),\quad P(23),\quad \dots.$$

And finally (and most importantly), as we already know that $P(4)$ is not true, we deduce that all of the following are not true as well:

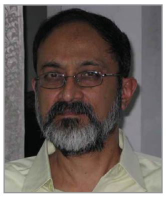
$$P(8),\quad P(12),\quad P(16),\quad P(20),\quad P(24),\quad \dots.$$

We have now proved proposition (9) in full.

In Part III of this article, we shall consider a few more non-standard examples.

References

1. Wikipedia, "Mathematical induction" from https://en.wikipedia.org/wiki/Mathematical_induction



SHAILESH SHIRALI is Director of Sahyadri School (KFI), Pune, and Head of the Community Mathematics Centre in Rishi Valley School (AP). 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.