How To Prove It

Starting with this issue we will run a regular column on the art and science of proof, and in honour of George Pólya's book, 'How To Solve It', we have named it "How To Prove It." There is of course no single way to prove things in mathematics. But there are many general ideas and strategies that do help, and that's what this column is about.

Shailesh A Shirali

Formal proof is one of the striking features of mathematics. You do not find this feature in any of the sciences. What you do meet in the sciences would be more accurately described as 'verification'. You may for example perform an experiment in the laboratory to verify the formula $t = 2\pi\sqrt{l/g}$ for the time period of oscillation of a pendulum. What do you do? You set up the apparatus and take a lot of readings, then draw a graph or two and check how close are your results to the prediction. At the end you say, 'The formula has been verified to be true within experimental error' or something like that. This is done routinely in the sciences. It is important to see that *this is not the same as proof in mathematics.*

In a proof what you are attempting to do is to build a logical bridge from one set of statements (or suppositions) to another statement, using intermediate steps that are small and of a kind which no one would dispute. The jump from the initial statement to the final one may seem large, but when broken down to a sequence of small steps it does not appear so. The logic used in mathematics is

Keywords: *Polya, formal proof, number patterns, algebra, pattern, sequence*

actually no different from that used in ordinary life (though it may seem different, especially when expressed using symbols and formal mathematical language); indeed, daily life is the source of all logical methods. You could say, in fact, that much of mathematical logic is plain and simple 'kitchen logic'!

It is believed by many that at the school level proof is encountered mainly in the realm of geometry; and that geometry is the only platform available for teaching proof. Both these statements are false. *Proof lies at the heart of mathematics, in every single branch*. At the school level, one resource that is heavily underutilized with regard to the teaching of proof is *Number Patterns and Algebra*. In this column we shall demonstrate many principles of proof using themes from number theory (which at this level is mainly applied algebra). Of course, we shall consider themes from geometry too.

It is equally a fallacy to imagine that proof can be introduced only when students are in their upper primary classes or in high school. Formal written proof, yes; symbolic proof, yes; but informal and clearly articulated, verbalized reasoning can and should be introduced much earlier — indeed, in the lower primary years. We shall elaborate on this theme in subsequent columns.

An example from algebra

In the first 'episode' of this serial we study an example from number theory:

Show that the square of any odd number leaves remainder 1 when divided by 8.

We experiment with some numbers to get a sense of the task: $1^2 = 0 \times 8 + 1$, $3^2 = 9 = 1 \times 8 + 1$, $5^2 = 25 = 3 \times 8 + 1$, $7^2 = 49 = 6 \times 8 + 1$, $9^2 = 81 = 10 \times 8 + 1$, $11^2 = 121 = 15 \times 8 + 1$, $13^2 = 169 = 21 \times 8 + 1$, ... We see that the claim has worked for the odd squares from 1^2 till 13^2. Is this enough evidence to conclude that the pattern will always be true?

Not quite! As we said earlier, empirical evidence is suggestive of the truth of a proposition — but that's all. In number theory there are numerous instances of statements which fail despite the evidence in their favour being very strong. A well known example of this is Euler's prime-generating function $n^2 + n + 41$, which yields prime values for 40 consecutive values of n (namely, $n = 0, 1, 2, 3, \ldots, 39$; we get the primes 41, 43, 47, . . . , 1447, 1523, 1601), and just as we are beginning to be certain that the expression will always yield a prime, the formula disappoints us: the pattern breaks, with $n = 40$ yielding a composite number. (It is easy to check that $n = 40$ does yield a composite number, for $40^2 + 40 + 41$ is clearly a multiple of 41. Indeed, it equals 41^2.)

So if we want actual proof then we have to produce something that will stand up in the 'mathematical court' before the toughest lawyer, who will be looking for ways to dash your arguments to bits. Here are some approaches which should satisfy such a lawyer.

First proof. What is an odd number? Clearly, one that leaves remainder 1 when it is divided by 2. This means that an odd number A is of the form 2 × an integer + 1, i.e., $A = 2n + 1$ where n is a positive integer. Let us see what happens when we square this expression:

$$A^2 = (2n + 1)^2 = 4n^2 + 4n + 1.$$

We see readily that A^2 is of the form 4 × (some integer)+1. That is, A^2 leaves remainder 1 when divided by 4. While this comes close, it is not good enough: we need division by 8, not by 4. What do we do now?

Let's look more closely. We see that $A^2 = 4n\,(n + 1) + 1$. If only we can show that $n\,(n + 1)$ is an even number, then our task will be done, for the number $4n\,(n + 1)$ will then be twice a multiple of 4, and therefore a multiple of 8.

But $n\,(n + 1)$ is even; for, it is the product of two consecutive numbers, of which one clearly must be even. So our job is done!

Second proof. This approach may appear a bit strange at first but is perfectly valid. The idea comes from the fact that the problem has to do with division by 8, so it seems natural to check if there is some underlying pattern which repeats each time n increases by 8. So we consider the expression: $(n + 8)^2 - n^2$. We have:

$(n + 8)^2 - n^2 = (n^2 + 16n + 64) - n^2 = 16n + 64 = 8(2n + 8)$.

We see clearly that the last quantity is a multiple of 8. *So when n increases by* 8, *the remainder in the division* $n^2 \div 8$ *stays unchanged.*

It follows that if the given statement is true for the odd squares 1^2, 3^2, 5^2 and 7^2, then it will necessarily be true for 9^2, 11^2, 13^2 and 15^2; and therefore it will necessarily be true for 17^2, 19^2, 21^2 and 23^2; and so on, indefinitely. But the statement is indeed true for 1^2, 3^2, 5^2 and 7^2, as is easily checked. Therefore it is true for the square of every odd number!

Remark. This proof can be hugely improved once we notice that we do not need to consider integers separated by a gap of 8. In fact, since we are studying the squares only of odd numbers, a gap of 2 is good enough! For, if we consider any two consecutive odd numbers, say 2n − 1 and 2n + 1, the difference between their squares is

$(2n + 1)^2 - (2n - 1)^2 = (2n - 1 + 2n + 1) \times 2 = 4n \times 2 = 8n$,

which is a multiple of 8. So if the hypothesis is true for the first odd square (namely: 1^2), which it clearly is, then it will be true for every subsequent odd square. Hence proved!

Third proof. Just for variety we give a third proof. It is based on the fact that the sum of the first n odd numbers is n^2. For example, $1 + 3 = 4 = 2^2$ and $1 + 3 + 5 = 9 = 3^2$. So to show that $(2n - 1)^2$ is 1 more than a multiple of 8, we must show that the sum of the first $2n - 1$ odd numbers is 1 more than a multiple of 8.

Now we observe the following simple pattern in the sequence of odd numbers: the sums 3 + 5, 7 + 9, 11 + 13, 15 + 17, . . . are all *multiples of* 8. It is easy to see why this must be so; for, 3 + 5 = 8, and in advancing from 3 + 5 to 7 + 9 we increase the sum by 4 + 4 = 8. Likewise, in advancing from 7 + 9 to 11 + 13 we increase the sum by 4 + 4 = 8. As the sums increase by 8 each time, and we start off at a multiple of 8, the sum will always be a multiple of 8.

The statement now proves itself; for, in the sum of the first $2n - 1$ odd numbers, we can pair the last two odd numbers, then the two odd numbers just before that pair, and so on, down to {3, 5}. The sum of each pair is a multiple of 8, and the remaining number, 1, ensures that the sum is 1 more than amultiple of 8. The following depicts a typical situation:

$9^2 = 1 + \underbrace{3 + 5} + \underbrace{7 + 9} + \underbrace{11 + 13} + \underbrace{15 + 17}$.

Closing remarks. We quote Professor Gila Hanna, from [1]:

The recognition that proofs can convey new mathematical techniques effectively, and thus should be treated as important bearers of mathematical knowledge, is a fertile point of view that mathematics educators seem to have overlooked to a large extent. Adopting this approach to proof in the classroom does not challenge in any way the accepted "Euclidean" definition of a mathematical proof (as a finite sequence of formulae in a given system, where each formula of the sequence is either an axiom of the system or is derived from preceding formulae by rules of inference of the system), nor does it challenge the teaching of proof as a Euclidean derivation. It is rather an acknowledgement that the teaching of proof has the potential to further students' mathematical knowledge in other ways. It offers an opportunity to make new connections between the process of proving and mathematical techniques, and also gives us an additional reason for keeping proof in the mathematics curriculum.

References

[1] Gila Hanna, *Proof can teach you new methods*, http://www.unige.ch/math/EnsMath/ Rome2008/WG1/Papers/ HANNA.pdf

[2] David Reid, *Understanding proof and transforming teaching*, http://www.pmena.org/2011/ presentations/ PMENA_2011_Reid.pdf

SHAILESH SHIRALI is Head of the Community Mathematics Centre in Rishi Valley School (AP) and Director of Sahyadri School (KFI), Pune. He has been involved in math education and math olympiads since the 1980s. He is the author of many math books addressed to high school students, and serves as an editor for the science magazine Resonance and for the magazine At Right Angles. He is engaged in many outreach projects in teacher education through the Community Mathematics Centre. He may be contacted on shailesh.shirali@gmail.com.

A poem on the prime number theorem

The prime numbers are mysterious because they have the two `opposing' properties: there are arbitrarily large gaps in between them and they satisfy no simple formula, while simultaneously their distribution is regular in the sense of the famous prime number theorem. This theorem can be informally stated as saying that the probability of a number n being prime is 1/log(n). This can be poetically worded as:

Numbers in their prime --
for no reason or rhyme,
show up at a rhythm
with probability 1/logarithm.
If this is a law they knew,
they also break quite a few
but then, that is not a crime!

-- B Sury