How To Prove It

This continues the 'Proof' column begun earlier. In this 'episode' we study some problems concerning the prime numbers, and a theorem from triangle geometry.

Shailesh Shirali

A property of prime numbers

The following is a striking property of the primes:

If p is a prime number exceeding 3, then p^2 -1 is a multiple of 24.

In general, statements about prime numbers are daunting to prove — in part because the primes are so highly irregular in their distribution. Indeed, we do not have any formula to generate the primes. So how might we go about proving the above statement?

Let's check it first. The primes exceeding 3 are: 5, 7, 11, 13, 17, 19, 23, ... Squaring them and subtracting 1, we get the numbers 24, 48, 120, 168, 288, 360, 528, ... It is easily checked that each of these numbers is a multiple of 24. Indeed, their greatest common factor or GCD is 24. (Another term for GCD is HCF: 'highest common factor'. But GCD is currently the accepted term in higher mathematics.)

A strategy for proving the result. Here is an approach to finding a proof: *Suppose that the claim is true. What does it lead to, what does it imply? By studying these implications, can we uncover a proof?* Let's do just this. An obvious implication of the given statement, which holds because 24 = 3 ×8, is the following: *If p is a prime number exceeding 3, then p^2 -1 is a multiple of both 3 and 8.*

Keywords: *Prime number, divisibility, least common multiple, direct proof, indirect proof, proof by contradiction, SAS congruence, Euclid*

Now an idea strikes us. If we show that a number K is a multiple of both 3 and 8, would it follow that K is a multiple of 24? Yes. The reason for this is seen by listing the multiples of 3 (namely: 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, …) and the multiples of 8 (namely: 8, 16, 24, 32, 40, …). On examining these lists we find that the numbers common to them are 24, 48, 72, …; they are all multiples of the least number in the list, which is 24 (that's precisely why 24 is called the 'least common multiple' or LCM of 3 and 8).

So we have found a strategy for solving the problem: *Prove that if* $p > 3$ *is prime, then* $p^2 - 1$ *is divisible by both* 3 *and by* 8.

But this is easy!

Divisibility by 8 Since p is a prime number exceeding 3, it is odd. But we know from what we proved in the an earlier (*How To Prove It*, November 2013) that if n is odd, then $n^2 - 1$ is a multiple of 8. Hence it must be true that if $p > 3$ is a prime number, $p^2 - 1$ is a multiple of 8.

(For those who missed that issue, here is a quick proof. Let n be odd. Then $n = 2k + 1$ for some integer k. This yields: $n^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k = 4k(k + 1)$. Since k and $k + 1$ are a pair of consecutive integers, one of them is even, hence $k(k + 1)$ is even; and this implies that $4k(k + 1)$ is a multiple of 8. Hence $n^2 - 1$ is a multiple of 8.)

Divisibility by 3 Since $p > 3$ is prime, on division by 3 it leaves a remainder of 1 or 2. So $p = 3k + 1$ or $3k + 2$ for some integer k. Now we need to check the divisibility of $p^2 - 1$ by 3 for these two forms.

- If $p = 3k + 1$, then $p^2 - 1 = (3k + 1)^2 - 1 = 9k^2 + 6k$, which is a multiple of 3.
- If $p = 3k + 2$, then $p^2 - 1 = (3k + 2)^2 - 1 = 9k^2 + 12k + 3$, which too is a multiple of 3.

Either way, $p^2 - 1$ is a multiple of 3.

Since $p^2 - 1$ is a multiple of both 3 and 8, it follows that $p^2 - 1$ is a multiple of 24.

Remark on the strategy followed You may wonder why we selected the numbers 3 and 8. Because $3 \times 8 = 24$? Not quite. Instead of 3 and 8, what if we select 4 and 6? It is easy to show that if $p > 3$ is prime, $p^2 - 1$ is a multiple of both 4 and 6. But since the LCM of 4 and 6 is 12, this would only prove that $p^2 - 1$ is a multiple of 12. It would *not* prove that $p^2 - 1$ is a multiple of 24.

Here are two more such results. In both we consider the effect of division by 120.

1. *If* p *is a prime number exceeding* 5, *the remainder when* p^2 *is divided by* 120 *is either* 1 *or* 49.
2. *If* p *is a prime number exceeding* 5, *then* $p^4 - 1$ *is a multiple of* 120.

For example, take the primes 17 and 19. We have:

$$17^2 = 289 = (120 \times 2) + 49,$$
$$19^2 = 361 = (120 \times 3) + 1,$$

and:

$$17^4 - 1 = 83520 = 120 \times 696,$$
$$19^4 - 1 = 130320 = 120 \times 1086.$$

We ask you to find the proofs of these statements. *Hint.* $120 = 3 \times 5 \times 8$. Hence you must consider the effect of dividing p^2 by 3, 5 and 8 respectively.

Direct and Indirect Proof

Proofs do not all follow the same approach; they come in different flavours and different colours. For example, proofs can be *direct* or *indirect*, and this is a crucial distinction. We now elaborate on this matter. Say we are given two 'propositions' or assertions, P and Q, and we are required to show: "If P is true, then Q is true" (more briefly: "If P, then Q", or "$P \implies Q$"). A "direct proof" is one where we start with P and travel 'directly' to Q, along a linear chain of deductions. In an 'indirect proof' the starting point may not be P. Instead we may ask: Could it be that Q is *not* true? What might be the consequences of assuming that Q is not true? What would it tell us about P? Thus we consider various alternatives to Q and then eliminate them, one by one, forcing us to 'accept' Q.

Direct proof We give two examples of direct proof. Note how they start with the given premise and proceed in a linear way to the desired conclusion.

Example 1. Prove: "For any integer n, the remainder in the division $n^2 \div 4$ is 0 or 1."

Proof: Suppose that n is even. Then $n = 2k$ where k is some integer. This implies that $n^2 = 4k^2$, so n^2 is a multiple of 4.

Next, suppose that n is odd. Then $n = 2k + 1$ where k is some integer. This implies that $n^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$, and we see that n^2 is 1 more than a multiple of 4 and hence leaves a remainder of 1 under division by 4.

Example 2. Prove: "If n is a positive integer such that the number $x := 2^n - 1$ is prime, then the number $\frac{1}{2}x(x + 1)$ is perfect." (A 'perfect number' is one for which the sum of the proper divisors equals the number itself. Example: 6 is perfect, since $1 + 2 + 3 = 6$. In the rule stated, if we take $n = 3$, we get $x = 7$, which is prime, and this gives us the perfect number $\frac{1}{2}(7 \times 8) = 28$. This general rule was first mentioned by Euclid in *The Elements*.)

Proof: We must show that $\frac{1}{2}x(x + 1) = 2^{n-1} \cdot x$ is perfect. The number has two distinct prime divisors (2 and x). This fact enables us to enumerate its full list of divisors:

$$\begin{cases} 1, & 2, & 2^2, & 2^3, & \dots, & 2^{n-1}, \\ x, & 2x, & 2^2 \cdot x, & 2^3 \cdot x, & \dots, & 2^{n-1} \cdot x. \end{cases}$$

Of these, all are proper factors except the very last one, $2^{n-1} \cdot x$, which is the number itself. We must now find the sum of all the proper factors. For this we use an often-used identity: *The sum of the first several powers of* 2*, starting with* 1*, is* 1 *less than the next higher power of* 2. Thus, $1 + 2 = 2^2 - 1$, $1 + 2 + 2^2 = 2^3 - 1$, $1 + 2 + 2^2 + 2^3 = 2^4 - 1$, and so on. Using the identity we find the sum of the proper factors of $2^{n-1} \cdot x$:

$$\begin{aligned} &(1 + 2 + 2^2 + \cdots + 2^{n-1}) + (1 + 2 + 2^2 + \cdots + 2^{n-2})\, x \\ &= (2^n - 1) + (2^{n-1} - 1)\, x \;=\; x + (2^{n-1} - 1)\, x \\ &= 2^{n-1} \cdot x. \end{aligned}$$

So the sum of the proper factors of $2^{n-1} \cdot x$ equals the original number, $2^{n-1} \cdot x$, just as we wished to prove.

Indirect proof Direct proof may seem the most natural kind of proof. But there are situations where a direct proof does not seem possible, or is too difficult. In such cases, it may be simpler to look for an indirect proof. Here, the significance of the word 'indirect' is that the proof proceeds by elimination of the alternatives other than the one we wish to prove. Occasionally we come across situations where the indirect route is more natural than the direct one; it may even be aesthetically more pleasing. A few examples will serve to illustrate these comments.

Example 3. Prove: "If $n > 1$ is an integer such that $2^n - 1$ is prime, then n is prime."

Proof: How do we show that a number (known to exceed 1) is prime? Here are two ways: either we show that it has no proper divisors; or we show that it cannot be composite. The latter is the indirect way, and it is what we adopt here.
We have been told that $2^n - 1$ is prime.
Since n is either prime or composite, there are two possible situations which can occur:

(A) $2^n - 1$ is prime and n is prime.

(B) $2^n - 1$ is prime and n is composite.

These two possibilities are contrary to each other (they cannot both occur). Also, there are no possibilities other than these. (So (A) and (B) form a mutually exclusive list.) We wish to show that it is (A) that occurs, and an obvious strategy for doing so is to show that (B) *cannot* occur. This is what we now do.

Suppose that $n > 1$ is composite; then $n = ab$ for some two integers $a > 1$ and $b > 1$, and $2^n - 1 = 2^{ab} - 1$. Let $k = 2^a$. Then:

$$2^n - 1 = (2^a)^b - 1 = k^b - 1. \qquad (1)$$

The number $k^b - 1$ has a factorization which is easy to anticipate:

$$k^b - 1 = (k-1)\left(k^{b-1} + k^{b-2} + k^{b-3} + \cdots + k + 1\right). \qquad (2)$$

(This comes from observing that
$k^2 - 1 = (k - 1)(k + 1)$,
$k^3 - 1 = (k - 1)\left(k^2 + k + 1\right)$, etc.)

Both factors in the factorization (2) exceed 1; for, the smaller of the two factors is $k - 1$, and $k - 1 = 2^a - 1$ which exceeds 1 since a exceeds 1. Hence $k^b - 1$ is not prime, i.e., $2^n - 1$ is not prime. Note what has happened: by supposing that n is composite, it has turned out that $2^n - 1$ is composite as well. But this means that possibility (B) has been falsified; it cannot occur. Hence it is possibility (A) which must occur. Therefore, if $2^n - 1$ is prime, it must be that n itself is prime.

Do you see why this proof is called 'indirect'?

Example 5. Prove: "If a triangle has two equal angles, then the sides opposite to the equal angles are equal." Stated otherwise: "In $\triangle ABC$, if $\angle B = \angle C$, then $AB = AC$."

Proof: First, some background. This problem is Theorem I.6 in *The Elements*; it comes just after I.5: "In an isosceles triangle, the angles opposite the equal sides are equal." (Or: "In $\triangle ABC$, if $AB = AC$, then $\angle B = \angle C$.") At this point in the text, the only congruence result available is "SAS congruence" (I.4): "If two sides of one triangle are equal, respectively, to two sides of another triangle, and the angles included by the two pairs of sides are equal, then the two triangles are congruent to each other." (The fact that the angle is 'included'between the two sides is crucial.) Euclid uses it to prove I.5 as shown in Figure 1.

If we attempt to prove Theorem I.6 the same way, we run into a difficulty. Try it out for yourself! You will find that no matter where we locate D on BC (possibilities: foot of internal bisector of angle BAC; midpoint of BC; foot of perpendicular from A to BC), we are unable, using SAS congruence, to show that $\triangle ABD \cong \triangle ACD$. In each case, we find that 'SAS' fails to apply; either the sides are wrong, or the angle itself is wrong.

Given: $AB = AC$. Draw AD to bisect $\angle BAC$. Now compare $\triangle ABD$ and $\triangle ACD$.

SAS congruence applies: $AB = AC$, AD is a shared side, and $\angle BAD = \angle CAD$. Hence $\triangle ABD \cong \triangle ACD$, and $\angle B = \angle C$.

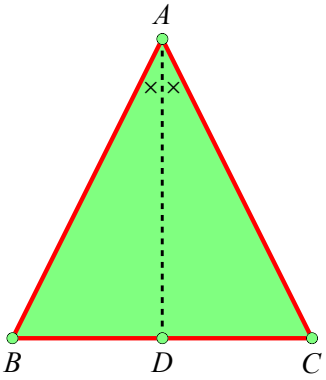

FIGURE 1. Theorem I.5: In Δ *ABC*, if *AB*= *AC*, then ∠B =∠C

Given: $\angle ABC = \angle ACB$. Suppose $AB > AC$. Locate D on AB such that $DB = AC$. Now compare $\triangle DBC$ and $\triangle ACB$.

SAS congruence applies: $DB = AC$, $BC = CB$, and $\angle DBC = \angle ACB$. Hence $\triangle DBC \cong \triangle ACB$. But this is absurd!

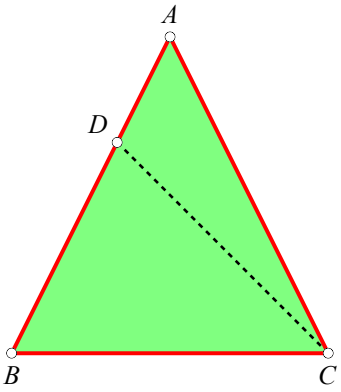

FIGURE 2. Theorem I.6: In Δ *ABC*, if ∠*B* = ∠*C*, then *AB* =∠*AC*

So Euclid uses a different strategy, and it is very ingenious. He asks, "Suppose that what is to be proved is *not* true (i.e., the sides are not equal). What happens then?" Now the possibility that $AB \neq AC$ can be subdivided into two possibilities: $AB > AC$, $AC > AB$. If we can show that both these are not possible (or "absurd" to use Euclid's words), then the desired conclusion would follow ($AB = AC$). To carry out this aim, Euclid assumes that $AB > AC$, argues as in Figure 2, and arrives at the conclusion that $\triangle DBC \cong \triangle ACB$. But this is absurd, since $\triangle DBC$ is contained within $\triangle ACB$, and the part cannot be equal to the whole. The absurd conclusion came about because of what we had assumed: $AB > AC$. If we had assumed instead that $AC > AB$, a similar absurdity would follow. So neither of these assumptions can be made. But then the only possibility left is $AB = AC$. And this is just what we wanted to show.

Note the indirectness of the strategy. The direct approach was found to be infeasible, so Euclid adopts the indirect route. His proof is an example of *proof by contradiction*.

Closing remark. When you see indirect proof for the first time in a mathematics class, you may get the impression that it is a form of reasoning peculiar to mathematics. But in fact we employ this kind of reasoning routinely in daily life, without realizing it. When you read a crime thriller and encounter the word 'alibi', you are dealing with just this form of reasoning! Here's how this happens. Say a crime has occurred in some house, and the police have pinpointed the time of the crime: it happened at 11 pm. The chief suspect for the crime is Mr. X. But the hopes of the police to lay the blame on Mr. X are dashed when

he produces an alibi: he can show that at 11 pm that night he was in some other city. The police case that X is the culprit now crumbles, as follows. *Claim.* X is not guilty. *Proof.* Suppose not; i.e., suppose that X committed the crime. But then he must have been at the scene of the crime at 11 pm. On the other hand, he was in some other city at exactly that time; that's what his alibi is all about! So we reach a contradictory state of affairs. (We assume that X does not belong to the league of 'X Men'and has not yet mastered the art of being in two places at the same time.) Consequently we must give up the assumption made at the beginning, about X being guilty. Hence, Mr. X is not guilty!

Note the laborious way in which we wrote out the argument. In actuality, such reasoning happens in a flash, and we are not even aware that we have thought it out in this way.

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 an editor for Resonance and At Right Angles. He may be contacted at shailesh.shirali@gmail.com.

A date-of-birth computation

Say you were born on day d of month m in year y. Here d is a number between 1 and 31, m is a number between 1 and 12, and y is a number between 0 and 99 (inclusive in each case).

For example, if the date of birth is 15 August 1947, then $d = 15$, $m = 8$, $y = 47$. We now do some arithmetical operations on d, m, y as described below.

1. **Write down d.**
2. **Multiply by 4. Add 13. Multiply by 25.**
3. **Subtract 200. Add m.**
4. **Multiply by 2. Subtract 40. Multiply by 50.**
5. **Add y.**
6. **Subtract 10,500.**

The result should be a number giving your birth day, month and last two digits of the year in which you were born.

Example

Suppose your birthdate happens to be 15 August 1947, or 15-08-47. Here is how the computations go, starting with $d = 15$:

- **15 → 15 x 4 = 60 → 60 + 13 = 73 → 73 x 25 = 1825**
- **1825 → 1825 – 200 = 1625 → 1625 + 08 = 1633**
- **1633 → 1633 x 2 = 3266 → 3266 – 40 = 3226 → 3226 x 50 = 161300**
- **161300 → 161300 + 47 = 161347 → 161347 – 10500 = 150847**

The number obtained at the end is 150847, or 15-08-47.

Why does this work? Find an explanation!