PROFESSOR: It's doubtful if you really understand something if you can explain why it's true. That's what proofs are about in mathematics and in computer science. So we're going to be talking about proofs of lots of things that we're trying to understand.

And in particular, we're going to look at a proof technique now called proof by contradiction, which is probably so familiar that you never noticed you were using it. And now we're going to call explicit attention to it, and think about it. So let's do an example first to see what's going on.

Suppose that I wanted to prove that the cube root of 1,332 was less than or equal to 11. Or more precisely, suppose I didn't know and I'm asking this question, is the cube root of 1,332 less than or equal to 11? Well, one way to do it would be to simply compute the cube root of 1,332, which is a small bother, but manageable.

But there's a simpler way than figuring out how to compute a cube root of a four-digit number. Let's just suppose that this inequality was true-- that is, that the cube root of 1,332 was less than or equal to 11. Well, if that was true, then what I could do is cube both sides.

And I'll conclude that 1,332 is less than or equal to 11 cubed. Now, 11 cubed is a lot easier to compute than the cube root of 1,332. As a matter of fact, 11 cubed is 1,331.

Wait a minute, I've just concluded that 1,332 is less than 1,331. That's obviously not true, which means that my assumption that this inequality held doesn't make sense. It leads to this immediate contradiction, which means that in fact, the inequality doesn't hold.

And I have now precisely and unambiguously-- I hope clearly-- proved that the cube root of 1,332 is greater than 11, even though we never actually computed the cube root of 1,332. This is kind of a [? toy ?] and simple-minded example to illustrate proof by contradiction. So let's step back and explain, and say what it is in general.

If an assertion implies something false, then the assertion itself must be false. That's what's going on here. If you're reasoning step by step, and at every step your reasoning is good-- which means that if you had something true and then you reached a conclusion from it in one step, the conclusion that you reached was also true-- then if you start off with some assumption, you keep proving things step by step in a way that preserves truth, and you arrive

at something false, it's inevitable that what you started with must have been false. Or else the thing you finished with would have been true.

OK, let's look at a real example of this-- an amazing fact that was known thousands of years ago to the ancient Greeks, which is that the square root of 2 is irrational. Now, let's remember that a rational number is a fraction. A rational number is a quotient of integers.

And the way we're going to prove that the square root of 2 is not a quotient of integers is by assuming that it was. So let's assume that the square root of 2 was a rational number, which means that we've got integers n and d without common prime factors, such that the square root of 2 is equal to n over d.

What I'm doing here is I'm saying squared of 2 as a fraction, n over d. And we know that you can always reduce a fraction to lowest terms, which means there are no common prime factors. So let's get that done.

We have the square root of 2 is equal to n over d, with no prime that divides both n and d. From this assumption, I'm going to prove to you that both n and d are even. And that, of course, is an immediate contradiction, because then both n and d have the common factor 2.

So all I've got to do in order to conclude that the square root of 2 is an irrational number-- it's not a fraction-- is prove to you that n and d are both even if the square root of 2 is equal to n over d. Let's do that.

We'll start off with what I'm assuming-- square root of 2 is n over d. And let's get rid of the denominator. So let's multiply through both sides by d, and get that the square root of 2 times d is equal to n.

Let's get rid of the square root of 2 now by squaring both sides. And I get 2d squared is n squared. Well, that's great, because look-- the left-hand side is divisible by 2. There it is.

Which means that n squared is divisible by 2. The right-hand side is even. But if n squared is even, then n is even, and I'm halfway there. I've shown that the numerator is even.

OK, let's keep going. Now, since n is even, it's equal to twice something. So n is 2k for some number k. I don't care what k is.

Let's square both sides of that, and conclude that n squared is equal to 4k squared. Why did I

square it? So that I could connect up here with the other question that I had about it n squared-- that n squared it was 2d squared. So combining these two, what I get is that 2d squared is equal to 4k squared.

And of course, I can cancel 2, and get that d squared is equal to 2k squared. And again, I've got the right-hand side divisible by 2. So the left-hand side is divisible by 2.

d squared is even, and therefore, d is even. And we've completed the proof as claimed. n and d both have 2 as a common factor, contradicting the fact that their in lowest terms. Now, I did assume something that is kind of obvious-- namely, that if n squared is even, then n is even.

Why is this true? Well, you might think about it for a moment. There's a simple way to see it, and it's a proof by contradiction.

We're going to use the fact that you can verify easily enough by doing a little arithmetic-- namely, the product of two odd numbers is odd. Let's assume that. So if the product of two numbers is odd, if I tell you that n squared is even, and suppose that n was not even, well, that means it's odd.

But that would mean that n squared was odd, contradicting the fact that n is even. Therefore, it's a contradiction to assume that n is odd. It must be even

That's an ad hoc proof that has to do with evenness and oddness. There's a more general way to understand this that actually will come in handy-- namely, that what I know is that numbers factor into primes in a unique way. So if I tell you that n squared is even, what I know about n squared is that all the primes that divide n squared come from n.

So if there's a 2 among the primes that divide n squared, it has to be a 2 that is one of the prime divisors of n. And that would work even if I told you that n squared was divisible by 3. It would follow by that reasoning that n is divisible by 3.

Now, that's a powerful fact. I'm assuming the prime factorization of integers. And it's not obvious at all that that's true, although it's very familiar. It's OK to assume.

In a few weeks we'll actually look back at how to carefully prove that. But for now, it's OK to assume. And we also have the simple argument that worked based on properties of even and odd-- that if n squared is even, then n is even. That's the last gap in the proof, and so we're done.