PROFESSOR: Now we come to a more serious application of the fact that the GCD is a linear combination. We're going to use it to prove the prime factorization theorem-- which we've talked about earlier. This is the unique prime factorization theorem.

So let's begin by looking at a technical property of primes, which is familiar, but we're going to need to prove it. If you believe in prime factorization, then this Lemma-- which says that if p divides a product, it divides one or the other of the components of the product-- that's an immediate consequence of the prime factorization theorem. But we mustn't prove it that way, because we're trying to use this to prove prime factorization.

So how can I prove, based on the facts of what we know about GCDs, without appealing to prime factorization that if p is a prime, and p divides a product, then it divides one of the components of the product, either the multiplier or the [? multiplicand? ?] OK, well here's how to prove that.

Suppose that p divides ab, but it doesn't divide a. Of course it does divide a, I'm done. So we may as well assume that it doesn't divide a. Now that means that since the only divisors p are p and 1-- the only positive divisors of p are p and 1-- that if p doesn't divide a, the GCD of a and p is 1.

All right, now comes the linear combination trick. Given that the GCD of p and a is 1, that means that I have a linear combination of a and p that's equal to 1-- sa plus tp is equal to 1, for some coefficients, s and t. Cool-- multiply everything by b on the right. So that means that sab plus tpb is equal to 1 times b.

But look at what we have now. The first term on the left is something times ab, and p divides ab, so that first term is divisible by p. The second term explicitly has a p in it, so it's certainly divisible by p.

So the left hand side is a linear combination of multiples of p, and therefore, itself is a multiple of p-- which means the right hand side is a multiple of p, and the right hand side is b. So sure enough, p divides b. We're done-- a very elegant little proof that follows immediately from the fact that you can express the GCD of two numbers as a linear combination of those numbers.

Now this is the key technical Lemma that we need to prove unique factorization. A corollary of this that I'm actually going to need is that if p divides a product of more than two things-- if p divides a product of a lot of things-- it has to divide at least one of them. And this you could prove by induction, with the base case being that it works for m equals 2. But it's not very interesting, and we're going to take that for granted. If p divides a product of any size, it divides one of the components of the product.

All right, now we're ready to prove what's called the fundamental theorem of arithmetic, which says that every integer greater than one factors uniquely into a weakly decreasing sequence of primes. Now the statement of weakly decreasing is a little bit technical and unexpected. What we want to say is that a number factors into the same set of primes. Well that's not quite right, because the set of primes doesn't take into account how many times each prime occurs.

You could try to make a statement about every number uniquely is a multiple of a certain number of each kind of prime. But a slick way to do that is simply to say, take all the prime factors, including multiple occurrences of a prime, and line them up in weakly decreasing order. And when you do that, that sequence is unique.

This fundamental theorem of arithmetic is also called the prime factorization theorem. And here's what it says when we spell it out-- without using the words weakly decreasing. It says that every integer, n, greater than 1 has a unique factorization into primes-- mainly it can be expressed as a product of p 1 through p k is equal to n. With p 1 greater than or equal to p 2, greater than or equal to each successive prime in the sequence, with the smallest one last.

Let's do an example. So there's a number that was not chosen by accident, because I worked out what the factorization was. And it factors into the following weakly decreasing sequence. You start with the prime 53, you followed by three occurrences of 37, two 11s, a 7 and three 3s. And the point is that if you try to express this ugly number as a weakly decreasing sequence of primes, you're always going to get exactly this sequence-- it's the only way to do it.

All right, how are we going to prove that? Well, let's suppose that it wasn't true. Suppose that there was some number that could be factored in two different ways. Well, by the well-ordering principle, there's at least one. So we're talking about numbers that are greater than 1, so there's a least number greater than 1 that can be factored in two different ways. Supposed that it's n.

So what I have is that n is a product p 1 through p k. And it's equal to another product, q 1 through q m, where the p's and the q's are all prime. And these two weakly decreasing sequences are not the same. They differ somehow.

So we can assume that the p's are listed in a weakly decreasing order, and the q's are likewise listed in weakly decreasing order. Now the first observation-- suppose that q 1 is equal to p 1. Well that's not really possible, because if q 1 is equal to p 1, then I could cancel the p 1 from both sides, and I would get the p 2 through p k is equal to q 2 through q m, and these would still be different. Since they were different, and I took the same thing from their beginning, I'm left with a smaller number that does not have unique factorization, contradicting the minimality of n.

So in short, it's not possible for q 1 to equal p 1. So one of them has to be greater. We may as well assume that q 1 is bigger than p 1. So q 1 is bigger than p 1, and p 1 is greater than or equal to all the other p's, so in fact, q 1 is bigger than every one of the p's. Well that's going reach a contradiction because of the corollary.

What I know is that q 1 divides n, and n is a product of the p's. And since q divides the product of the p's, by the corollary, it's got to divide one of them-- q 1 must divide p i for some i, but that contradicts the fact that q 1 is bigger than p i. That's not possible for the larger number to divide the smaller number.

And we're done. And we have proved the unique factorization theorem.