PROFESSOR: Another way to talk about congruence and remainder arithmetic is to work strictly with remainders, which makes things a little simpler because you don't have to worry about the fact that the product of two remainders may, for example, be too big to be a remainder. To knock it back in range, you have to take the remainder again. And that's what this abstract idea of the ring of integers modulo n, the ring Z sub n, captures in a quite elegant way. So it's going to allow us to talk strictly about equality instead of congruence.

And let's remind ourselves that the basic idea behind working with a remainder arithmetic was that every time we got a number that was too big to be a remainder, we just hit it with the remainder operation again to bring it back in range. And so the operations in Zn work exactly that way. The elements of Zn are the remainders. That is, the numbers from 0, including 0, up to n, but not including n. So there are n of them from 0, 1, up through n minus 1. And the definitions of the operations in Zn are given right here. Addition just means take this sum but then take the remainder immediately, just in case it's too big. And likewise, the product in Zn is simply multiply them and take the remainder. This isn't really a very dramatic idea, but it turns out to pay off in making some things just a little bit easier to say, because we're talking about equality instead of congruence.

So this package together, this mathematical structure consisting of the integers in this interval-- remember this notation, square bracket means inclusive and round parenthesis means exclusive. So this includes zero, it doesn't include n. The integers in that interval, under the operations of plus and times modulo Zn, as defined here, is called the ring of integers Zn. So it's got two operations and a bunch of things that are operated on.

Now I guess it's worth highlighting. That's what Zn is, the ring of integers. Mod n, or modulo n.

Now, arithmetic in Zn is really just arithmetic-- congruence arithmetic, except that it's equality now instead of congruence. So we can say, for example, in Z7 that 3 plus 6 is literally equal to 2 because, well, 3 plus 6 is 9, the remainder on division by 7 is 2, and we go directly to the two in Zn, suppressing the mention of taking remainders and not even really having to think about it, which is what's helpful about working with Zn. Likewise, 9 times 8 is literally equal to 6 in Z11.

So what's the connection between the set of all the integers and the integers mod n? And we

can state this abstractly in the following way. Let's just, for convenience, abbreviate the remainder of k on division by n as R of k. So n is fixed. And what's the connection between Z and Zn? Well, it's fairly simple. If you take the remainder of i plus j, that's literally equal to taking the sum of the remainders in Zn. Once you've taken the remainders, you're in the range of numbers that Zn works with. And this sum, then, keeps you in on the Zn side. Likewise, if you take the remainder of a product of real integers, that's literally equal to the product of the remainders in Zn. This operation, by the way, this connection between mathematical structures, the structure of the integers under plus and times and Zn under plus and times, is called a homomorphism. R, in this case, is defining a homomorphism from Z to Zn. That's a basic concept in algebra that you'll learn more about if you take some courses in algebra, but I'm just mentioning it for cultural reasons. We're not going to exploit it any further, or look further into this idea.

OK. What's the connection between equivalence mod n, or congruence mod n, and Zn? Well, it's fairly simple. In Zn, we convert congruences into equalities. So i is congruent to j mod n if and only if r of i is equal to r of j in Zn. And this is just a rephrasing of the fact that two numbers are congruent if and only if they have the same remainder.

Now once you've got this self-contained system Zn, you can start talking about algebraic rules that it satisfies. And now, they hold with equality and they're pretty familiar. So let's look at some of the rules for addition, for example, that hold true in Zn. First of all, addition is associative. i plus j plus k is i plus j plus k. We have an identity element, literally zero. Zero plus any i is i. We have a minus operation, an inverse operation, with respect to addition, which is that-- how do I get back some slides? Excuse me. OK, let's keep going.

I have an inverse operation, which is that for every i, there's an element called minus i. It's additive inverse such that if you add i and minus i, you get zero. And finally, commutativity, which is that i plus j is the same as j plus i. You don't really need to memorize these names, but you will probably hear them a lot in various other contexts, and especially in algebra courses, but even in terms of arithmetic. These are some of the basic rules that addition satisfies.

And in fact, multiplication satisfies pretty much the same rules. Multiplication is likewise associative. There's an identity for multiplication called 1. 1 times i is i. Multiplication is also commutative. The one obvious omission here is inverses. You can't count on there being inverses in Zn. And finally, there's an operation that connects addition and multiplication called

distributivity. Namely, i times j plus k is ij plus ik, as you well know from ordinary arithmetic. And this rule works fine for remainders and working in Zn.

As I said, the one thing we have to watch out for, it shouldn't be a surprise, is we know that you can't cancel with respect to congruence mod n. And that's reflected in the fact that you can't cancel in Zn. Namely, in Z12, for example, 3 times 2 is equal to 2 times 8. Again, 3 times 2 is 6, 2 times 8 is 16, you immediately take the remainder to get back to 6. In Z12, these two things are equal. But if you tried to cancel the 2, you'd conclude that 3 was 8, and neither 3-- 3 and 8 are different numbers in the range from 0 to 12, and they're different in Z12. So you can't cancel 2.

OK. Now the rules that we already figured out for when you can cancel in congruence translate directly over to when you can cancel in Zn. And now there's a standard abbreviation that's useful to use here. If I write Zn*, what I mean is the elements in Zn that are relatively prime to n. The elements whose GCD with n is 1.

So what we have is the following equivalent formulations of Zn*, which correspond to the facts we've already figured out about congruence. Namely, an integer i in the range from 0 to n is in Zn* if and only if the GCD of i and n is 1, or i is cancelable in Zn, or i has an inverse in Zn. All of these three things are equivalent. They give you the sense that Zn* is a kind of robust subset of Zn that you'd want to be thinking about. And in fact, it's very valuable to be paying attention to.

What else do we know about Zn*? Well, the definition of phi of n was the number of integers in the interval from 0 to n that are relatively prime to n. Of course, that's exactly the size of Zn*. So phi of n is simply the size of that collection of elements. Not surprising. They were defined that way.

So now I can restate Euler's Theorem in a slightly convenient way. Instead of mentioning congruence, we can just talk about equality. Euler's Theorem says that if you raise a number k to the power phi of n, it's literally equal to 1 in Zn, at least for those k's that are relatively prime to n. That is, those k's that are in Zn*. And it's going to turn out that the proof of Euler's Theorem is actually pretty easy. It just follows in a couple of steps from a couple of simple observations. So let's start on those.

So the first remark is that if I have any subset, S, of elements in Zn-- I don't care whether they are relatively prime to n or not-- if I multiply each of them by k, this notation for k times S

means that I'm taking the set of elements that are of the form k times an element of S over all the elements of S. So kS, which is this set of multiples of k-- multiples of elements of S by k, has exactly the same size as S.

Now, why is that? Well, this of course is only true for k that are cancelable. But the Lemma is, no matter what subset you take of Zn, if you multiplied every one of them by an element that's cancelable in Zn*, you get a set of the same size. And that's clear because how could ks1 and ks2 be equal? Well, only if s1 and s2 were equal. Or another way to say it is that if you had different elements in S, s1 not equal to s2, when you multiply them by k, you have to get different elements of ks, because k is cancelable.

OK. So that's an easy remark. Holds in general. Multiply any subset by a cancelable element, and you get a new set that's the same size. The second remark is that if you look at numbers i and j that are in the interval from 0 to n in Zn, then if you multiply the two of them, then you're going to get an element in Zn* if and only if the original two elements were in Zn*. Well, let's just look at it in the left to right direction, which is the only one we need.

If i and j are relatively prime to Zn*, then so is their product, because if neither i nor j has a prime factor in common with n, then their product obviously doesn't have a factor in common with n. And then when you take remainders, it's still going to be a number whose GCD is the same. And so we have this remark that if you multiply two cancelable elements, you get a cancelable element. If you multiply two elements relatively prime to Zn*, you get an element of Zn*. There's about-- every one of these formulations of Zn* in terms of GCDs are cancelable or inverse, and each of them gives a separate and straightforward proof of the fact that if i and j are in Zn*, then so is their product.

Now it's worth mentioning, by the way, that, in general, their sum is not. If you add two elements that are relatively prime to Zn*, even if their sum is non-zero, you will typically get an element that is no longer relatively prime to n. But for multiplication, it works great, and that's what matters to us.

OK. So as a corollary of this is that I can actually conclude that, if I choose an element that's cancelable, an element in Zn*, if I take the whole set Zn*, all those elements that are relatively prime to n, and I take multiples of k by each of them, then, in fact, I get the same set, Zn*. And the proof of that is really straightforward.

Let's think about it for a minute. Because what do I know is that these two sets are the same size. kZn* and Zn* are the same size. As long as k is cancelable, I don't even care that this was Zn*. On the other hand, if k is in Zn*, k times Zn* only gives you elements in Zn*. So kZn* is a subset of the left-hand side, and it's the same size by the Lemma that says that multiplying by k preserves sizes. So they have to be equal.

So basically what that means is that if you take all the elements in Z*, all the elements relatively prime to n, and you take another one of them, pick one out of that set, and multiply every element in the set by that element k, if you had them lined up in one order beforehand, when you multiplied by k you get exactly the same elements but just reordered. That is, multiplying by k has the effect of permuting the elements of Zn*.

Let's look at an example. So let's look at Z9. And we know that phi of 9, by the previous formula, is 3 squared minus 3, or 6. There are going to be 6 elements from 0 to n that are relatively prime to 9, and that comprise Zn*. So let's look at what they are. So you can do-- check the calculation. But Zn* is exactly the elements 1, 2, 4, 5, 7, 8. We know we got them all because there's only supposed to be six of them, and we can check that those are all relatively prime to 9. None of them has 3 as a divisor.

Now what happens, for example, if I multiply them all by 2? Two is another good number-- it's right here-- that's in Zn*. And multiplying them by 2, well, let's check. 2 times 1 is 2, 2 times 2 is 4, 2 times 4 is 8, 2 times 5 is 1-- because it's 10 with a remainder of 1-- 2 times 7 is 14-- translates into 5-- 2 times 8 is 16-- [INAUDIBLE] translates into 7. And, as claimed, look at this. Here's 2, 4, 8, 1, 5, 7. It's the same numbers as 1, 2, 4, 5, 7, 8, just in a different order.

Let's do one more example. Let's try multiplying by 7. That's another respectable element over here. 7 times 1 is 7, 7 times 2 is 14, which means it's 5 in Z9. 4 times 7 is 28. Well, 3 times 7 is 27, so that leaves a remainder of 1. And 4 times 7 is 1 in Z9. Likewise, 5 times 7 is 8, 7 times 7 is 4, and 7 times 8 is 56, which translates to 2. And sure enough, as claimed, I see the same numbers, 7, 5, 1, 8, 4, 2, just these numbers scrambled in order. They're permuted, which is the outcome of multiplying by 7.

OK. So let's go back. What we've just illustrated is this fact that we've already concluded that, if you take Zn* and you multiply it by an element k in Zn*, you get the same set in a different order. So Zn* is equal to k times Zn*. And now we're on the brink of proving Euler's Theorem. Because what I want to do is say, look, these two sets are the same. Let's multiply all the

elements on the left together, and multiply all the elements on the right together. Let's take the product of those elements. So let's take the product of Zn* and compare it to the product of kZn*. So big pi here is indicating the product of all of the elements in this set, the product of all of the elements in this set.

Well, let's look at the set on the right. This is the product of k times all the elements in Z*. Well how many elements are there? Phi of n elements in Z*, by definition. And let's factor out all the k's. So this expression here, the product of k times each element in Zn*, is the same as the product of the elements in Zn* times k to as many elements as there were, namely k to the phi of n. I'm just factoring k out of this product. And there's my k to the phi of n.

And now look what I got here. That's pi Zn*, and that's pi Zn*. What do I know about multiplying elements in Zn*? They're in Zn*. This product will be some other element is Zn*. So will this product. But what do I know about Zn*? They're cancelable. So just looking-- ignoring the middle term now, what I'm concluding is that the product of Zn* is k to the phi of n times the product of Zn*. Let's cancel those cancelable terms. And I'm done. I've just figured out that 1, which is the result of canceling the term on the left, is equal to k to the phi of n. And we have successfully proved Euler's Theorem, which is what we were aiming for in this segment.