PROFESSOR: The elements that have inverses modulo and will be particularly important to us. And so the first question is how many of them are there, which is what Euler's function tells us.

So the definition of Euler's function, phi of n, is it's the number of integers in the remainder interval from 0 to n minus 1 such that k is relatively prime to n. So remember, there's the notation for the remainder interval that includes 0 and excludes n. And another way to say relatively prime to n is to say the gcd of k and n is 1.

So let's define that set of numbers that we're interested in-- gcd1 of n [? be ?] those numbers that have a gcd of 1 with n. That is, the numbers that have inverses and the numbers that are cancellable modulo n. So what it means is that phi of n is precisely equal to the size of gcd1 of n.

Now, some authors call gcd1 n star. I didn't find that a very informative notation and so I'm not using it. phi of n is also, for your information, called Euler's totient function, but we'll just stick to calling it phi or Euler's phi.

So let's look at an example-- gcd1 of 7. The numbers that are relatively prime to 7 are all the positive numbers less than 7 because 7 is prime. So it's the set 1, 2, 3, 4, 5, 6. gcd1 of 12 is the numbers that have no factor in common with 12. They are the numbers in green below. And the other red numbers do have a number in common with 12-- do have a prime in common with 12. The pattern here is not so apparent.

Anyway, phi of 7 is the size of gcd1 of 7-- namely the size of the set 1 through 6, which is 6. gcd 12 determines phi of 12. phi of 12 is the number of green elements, which is 4.

OK. A simple rule for calculating phi. When phi is prime we've already indicated, namely, everything-- every positive number less than p is relatively prime to p. And so phi of p is simply p minus 1.

Let's look at a more important example, or illustrative example-- namely, phi of 9. Well, OK. So there are the candidate numbers from 0 through 8, and which ones are relatively prime to 9?

Well, it's relatively prime to 9 if and only if it's relatively prime to 3. Now, which numbers in this interval are relatively prime to-- are relatively prime to 3, or, rather, are not relatively prime to 3? Well, it's every third number that's divisible by 3.

So, those are the bad ones. If we subtract the bad ones, we're left with the good ones-- the ones that are relatively prime.

So a phi of 9 is simply the set of all the numbers minus 1/3 of 9, which is the bad one-- bad one's namely 6. This generalizes to a power of a prime. If k is a positive integer then phi of p to the k-- the reasoning is that a number is relatively prime to the p to the k if and only if it's relatively prime to p.

p divides every pth number, so one pth of the numbers in the interval are bad, which means that phi of p is the good ones minus 1 pth of p to the k. Namely, phi of p to the k is p to the k minus p to the k over p, which can also be expressed in a more standard form-- p to the k minus p to the power k minus 1. And that knocks off the story of phi to the p for powers of primes.

Well, suppose you're dealing with a number that's not a power of a prime. And there's one very elegant little fact about phi that explains how to deal with non powers of primes. Namely, if a and b are relatively prime, then phi of a b is simply gotten by computing phi of a and multiplying it by phi of b.

This property of phi is called multiplicativity, by the way. It comes up a lot in number theory. A function is multiplicative when its value at a product of relatively prime numbers is the product of the values at those two relatively prime numbers. So phi is multiplicative.

Now, the proof of that-- one proof is on problem set 5, and there's another proof that we'll see in a couple of weeks when we get into counting the inclusion-exclusion principle. Let's just use this fact about phi-- the multiplicity of phi-- multiplicativity of phi to see how it lets us calculate phi of an arbitrary number.

So, in particular, phi of 12-- which looked complicated earlier-- well, 12 is 3 times 4. So that means that phi of 12 is phi of 3 times phi of 4. But now I'm in great shape because 3 is a power of a prime, namely 3 to the 1. And 4 is a power of a prime, namely 2 squared. So applying the power of prime formulas, I get that phi of 3 is 3 times 1 times 2 squared minus 2 to the 2 minus 1, which simplifies to 4, which is the answer that we saw before.

And the punchline for why we're examining phi is Euler's theorem, which tells us how powers of numbers in gcd1 of n behave. Namely, that if k is relatively prime to n, then if you raise k to

the power phi of n, it's congruent to 1 mod n.

And that will lead us. In the next section we will look at the proof of Euler's theorem.