PROFESSOR: So, now we come to the place where arithmetic, modulo n or remainder arithmetic, starts to be a little bit different and that involves taking inverses and cancelling. Let's look at that. So first of all, we've already observed that we have these basic congruence rules that if a and b are congruent then c and d are congregant, then a plus c and b plus d are congruent, a times c and b times d are congruent. So, that's the sense in which arithmetic mod n is a lot like ordinary arithmetic.

But here's the main difference. Let's look at this one. 8 times 2 is 16, which means it's congruent to 6 mod 10, which is the same as 3 times 2. So, 8 times 2 is congruent to 3 times 2. And you'd be tempted, maybe, to cancel the twos. And what happens then, well then you could discover that you think that 8 is congruent to 3 mod 10, which it ain't. So in short, you can't cancel arbitrarily. You can't cancel two, in this case in particular.

So, that leads, naturally, to the question of when can you cancel a number? When can you cancel a number k when both sides of inequality are multiplied by k and I'd like to cancel k? And the answer is simple, when k has no common factors with a modulus n. So, the proof of that is based on the following idea. Let's say that a number k prime is an inverse of k mod n. If k prime times k is congruent to 1 mod n. So, k prime is like 1 over k with respect to mod n. But of course, 1 over k is going to be a fraction unless k is 1. And so, k prime is going to be an integer that simply acts like 1 over k.

So, how are we going to prove this? And it's going to turn out to be an easy consequence of the fact that the gcd is a linear combination. So, how am I going to prove-- find this k prime that's an inverse of k? Well remember, given the gcd of k and n is 1, I have a linear combination of k and n is 1. So, s times k plus t times n is 1. But if you stare at that for a moment, what that means is that k prime is simply the coefficient s of k.

So, all you have to do is apply the pulverizer to k and n to get the coefficient s of k in the linear combination of k and n is equal to 1. Let's look at that slightly more carefully and see what's going on. I have that sk plus tn is 1. So, that means in particular, since they're equal, they're certainly congruent to each other, modulo n. sk plus tn is congruent to 1 mod n. But, n is congruent to 0 mod n. So, this becomes t times 0, and we're left with sk congruent 1 mod n, which is exactly the definition of s being an inverse of k.

Now, I can also cancel k if it's relatively prime to n. And the reason is that if I have ak equivalent to bk mod n and the gcd of k and n is 1, then I have this k prime that's an inverse of k. So, I just multiply both sides by the inverse of k, namely k prime. And I get that the left hand side is a times k, k inverse. And the right hand side is b times k, k inverse. And of course, that's a times 1 is equivalent to b times 1. And so, a is congruent to b mod n. So I can cancel, in that case, trivially.

And in fact, you can work out the converse implications. The punch line of this-- well first of all, this is the cancellation rule. You can cancel providing that the gcd of k and n is 1 if k is relatively prime to n. So, this is the summary. [? k is ?] cancelable mod n if and only if k has an inverse mod n, if and only if the gcd of k and n is 1, which I can restate as k is relatively prime to n. And that's the story.