PROFESSOR: The idea of congruence was introduced to the world by Gauss in the early 18th century. You've heard of him before, I think. He's responsible for some work on magnetism also. And it turns out that this idea, after several centuries, remains an active field of application and research.

And in particular, in computer science it's used significantly in crypto, which is what we're going to be leading up to now in this unit. It's plays a role in hashing, which is a key method for managing data in memory. But we are not going to go into that application.

Anyway, the definition of congruence is real simple. Congruence is a relation between two numbers, a and b. It's determined by another parameter n, where n is considered to be greater than one. All of these, as usual, are integers.

And the definition is simply that a is congruent to b mod n if n divides a minus b or a minus b is a multiple of n. So that's a key definition to remember. There's other ways to define it. We'll see very shortly an equivalent formulation that could equally well have been used as a definition. But this is a standard one.

A is equivalent to b means that a minus b is a multiple of n. Well let's just practice. 30 is equivalent to 12 mod 9 because 30 minus 12 is 18, and 9 divides 18.

OK. An immediate application is that does this number with a lot of 6's is ending in a 3 is equivalent to 788253 modulo 10. Now why is that? Well, there's a very simple reason.

If you think about subtracting the 6 number ending in 3 from the 7 number ending in 3, what you can immediately see without doing much of any of the subtraction-- just do the low order digits-- when you subtract these, you're going to get a number that ends in 0.

Which means that it's divisible by 10. And therefore those two numbers are congruent. It's very easy to tell when two numbers are congruent mod 10 because they just have the same lower digit.

OK. Another way to understand congruency and what it's really all about is the so-called remainder lemma, which sets that a is congruent to b mod n, if and only if a and b have the same remainder on division by n.

So let's work with that definition. We can conclude using this formulation, equivalent formulation, that 30 is equivalent to 12 mod 9 because the remainder of 30 divided by 9, well it's 3 times 9 is 27, remainder 3. And the remainder of 12 by 9 is 3. So they do indeed have the same remainder 3. And they're congruent.

By the way, this equivalent sign with the three horizontal bars is read as both equivalent and congruent. And I will be bouncing back between the two pronunciations indiscriminately. They are synonyms.

OK, let's think about proving this remainder lemma just for practice. And in order to fit on the slide, I'm going to have to abbreviate this idea of the remainder of b divided by n with a shorter notation r sub b n. Just to fit.

OK. So the if direction of proving the remainder limit that they're congruent if and only if they have the same remainder. The if direction here in an if and only if is from right to left. I've got to prove that if they have the same remainder, then they're congruent.

So there are the two numbers, a and b. By the division theorem, or division algorithm, they can each be expressed as a quotient of a divided by n times the quotient sub a plus the remainder of a divided by n. And likewise, b can be expressed in terms of quotient and remainder.

And what we're given here is that the remainders are equal. But if the remainders are equal, then clearly when I subtract a minus b, I get qa minus qb times n. Sure enough, a minus b is a multiple of n. And that takes care of that one.

The only if direction now goes from left to right. So in the converse, I'm going to assume that n divides a minus b, where a and b are expressed in this form by the division algorithm or division theorem.

So if n divides a minus b, looking at a minus b in that form what we're seeing is that n divides this qa minus qb times n, plus the difference of the remainders. That's what I get just by subtracting a and b.

But if you look at this n divides that term, the quotient times n. And it therefore has to divide the other term as well. Because the only way that n can divide a sum, when it divides one of the sum ands, is if it divides the other sum and. So n divides ra minus the remainder of 8 divided by n from b divided by n.

But remember, these are remainders. So that means that they're both in the interval from 0 to n minus 1 inclusive. And the distance between them has got to be less than 1. So if n divides a number that's between 0 and n minus 1, that number has to be 0. Because it's the only number that n divides in there.

So in fact, the difference of the remainders is 0. And therefore, the remainders are equal. And we've knocked that one off. So there it is restated. The remainder lemma says that they're congruent if and only if they have the same remainders.

And that's worth putting a box around to highlight this crucial fact, which could equally well have used as the definition of congruence. And then you'd prove the division definition that we began with.

Now some immediate consequences of this remainder lemma are that a congruence inherits a lot of properties of equality. Because it means nothing more than that the remainders are equal. So for example, we can say the congruence is symmetric, meaning that if a is congruent to b, then b is congruent to a.

And that's obvious cause a congruent to b means that a and b have the same remainder. So b and a have the same remainder. One that would actually take a little bit of work to prove from the division definition-- not a lot, but a little bit-- would be that if a is congruent to b, and b is congruent to c, then a is congruent to c.

But we can read it is saying the first says that a and b have the same remainder. The second says that b and c have the same remainder. So obviously a and c have the same remainder. And we've prove this property that's known as transitivity of congruence.

Another simple consequence of the remainder theorem is a little technical result that's enormously useful called remainder lemma, which says simply that a number is congruent to its own remainder, modulo n.

The proof is easy. Let's prove it by showing that a and the remainder of a have the same remainder. Well, what if I take remainders of both sides, the left hand side becomes the remainder of a divided by n. The right hand side is the remainder of the remainder.

But the point is that the remainder is in the interval from 0 to n. And that means when you take its remainder mod and its itself. And therefore the left hand side is the remainder of a divided by n, and the right hand side is also the remainder of the a divided by n. And we have proved

this corollary that's the basis of remainder arithmetic.

Which will basically allow us whenever we feel like it to replace numbers by their remainders, and that way keep the numbers small. And that also merits a highlight.

OK. Now, in addition to these properties like equality that congruence has, it also interacts very well the operations. Which is why it's called a congruence. A congruence is an equality-like relation that respects the operations that are relevant to the discussion. In this case, we're going to be talking about plus and times. And the first fact about congruent says that if a and b are congruent, then a plus c and b plus c are congruent.

The proof of that follows trivially from the definition. Because the a congruent to b mod, n says that n divides a minus b. And if n divides a minus b, obviously n divides a plus c minus b plus c. Because a plus c minus b plus c is equal to a minus b. That one is deceptively trivial.

It's also the case that if a is congruent to b, then a times c is congruent to b times c. This one takes a one line proof. We're given that n divides a minus b. That certainly implies that n divides any multiple of a minus b. So multiply it by c and then apply distributivity, and you discover that n divides ac minus bc, which means ac is congruent to bc modulo n.

It's a small step that I'm going to omit to go from adding the same constant to both sides to adding any two congruent numbers to the same sides. So if a is congruent to b and c is congruent to d, then in fact, a plus c is congruent to b plus d.

So again, congruence is acting a lot like ordinary equality. If you add equals to equals, you get equals. And of course the same fact applies to multiplication. If you multiply equals by equals, you get equals.

A corollary of this is that if I have two numbers that are congruent modulo n, then if I have any kind of arithmetic formula involving plus and times and minus-- and what I want to know is what it's equivalent to modulo n-- I can figure that out freely substituting a by a prime or a prime by a. I can replace any number by a number that it's congruent to, and the final congruence result of the formula is going to remain unchanged.

So overall what this shows is that arithmetic modulo n is a lot like ordinary arithmetic. And the other crucial point thought that follows from this fact about remainders is that because a is congruent to the remainder of a divided by n, then when I'm doing arithmetic on congruences,

I can always keep the numbers involved in the remainder interval. That is, in the remainder range from 0 to n minus 1.

And we use this standard closed open interval notation to mean the interval from 0 to n. So it's sometimes used in analysis to mean the real interval of reals. But we're always talking about integers. So this means-- the integers that square bracket means 0 is included. And a round parenthesis means that n is excluded.

So that's exactly a description of the integers that are greater and equal to 0 and less than n. Let's do an application of this remainder arithmetic idea. Suppose I want to figure out what's 287 to the ninth power modulo 4?

Well, for a start but if I take the remainder of 287 divided by 4, it's not very hard to check that that's 3. And that means that 287 to the ninth is congruent mod 4 to 3 to the ninth. So already I got rid of the three digit number, the base of the exponent, and replaced it just by a one digit number, 3. That's progress.

Well, we can make more progress because 3 to the ninth can be expressed as 3 squared, squared, squared times 3, right? Because when you iterate taking powers, it means that the exponents multiply. So this is 3 to the 2 times 2 times 2, or 8, times 3-- which adds 1 to the exponent-- or 9. So that's simple exponent arithmetic.

But notice that 3 squared is 9. And 9 is congruent to 1 mod 4. So that means I can replace 3 squared by 1, and the outer 2 squared stays. It becomes 1 squared squared, but that's 1 times 3.

And the punchline is that 287 to the ninth is congruent to 3 mod 4 by a really easy calculation that did not involve taking anything to the ninth power.