[SQUEAKING]

[RUSTLING]

[CLICKING]

BRYNMOR CHAPMAN: Can people hear me in the back? We good? OK. Nice. Let's get started. So last week, last week? Yes, last week, we started talking about our number theory unit and in particular, divisibility. And we saw a very exciting application of divisibility, saving New York City.

Today we're going to look at an even more exciting example, modular arithmetic. So recall, so we saw Bézout's identity and the pulverizer. So I'll just write that up here. So for all integers a and b, there exists s and t such that-- that's a little bit confusing, sorry-- gcd of a, comma b equals as plus bt. And moreover, we can compute these efficiently, using the pulverizer, the extended Euclidean algorithm.

Then the other useful fact that we're going to make use of today, every number can be written as an ILC of a and b if and only if it is divisible by their gcd. So we are going to make use of these two facts. So do not forget. Let's see. Oh, sorry about that.

So let's start talking about modular arithmetic then. I expect that at least in some form, it is something that's fairly familiar to all of you. So presumably you learned back in grade school, what is the sum of an even integer and an odd integer? What do you know about it? Did people not learn this? Yeah?

AUDIENCE: It's odd.

BRYNMOR CHAPMAN: Yeah, it's odd. So, first example, even plus odd is odd. Even plus odd is odd. What is the last digit of, say, 357 by 994? Yeah?

AUDIENCE: 8.

BRYNMOR CHAPMAN: 8, yeah, so ends in 8. Why is that?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah, you can basically ignore everything except the last two digits. You multiply those together. You get 28. That ends in an 8. So this is also going to end in an 8.

It's currently 2:39 PM. What time will it be in 49 hours?

AUDIENCE: 3:30.

BRYNMOR CHAPMAN: 3:30 yeah, about, 3:39 and 49 hours. And why is that? Yeah, someone else say? How are we getting to that? Yeah?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah. So 49 hours is one hour more than two full days. We can forget about those two days and just add an hour onto the current time. What day of the week will it be 100 days from now?

AUDIENCE: Thursday.

BRYNMOR CHAPMAN: Thursday, yeah. 100 days is two days more than 14 weeks. So we can forget about those 14 weeks. Add those two days, and we get Thursday. So these are all fairly familiar examples to most of you, hopefully, of modular arithmetic.

And the theme is that when you're working modulo n, you're just ignoring all multiples of n and only focusing on remainders. So even and odd, this is the remainder when dividing by 2. Days of the week, we divide by 7. Look at the remainder, last digit. This is remainder when we divide by 10; hour remainder when we divide by 12 or 24, depending on whether you care about AM or PM.

And so we often call modular arithmetic clock arithmetic for this reason. Because it's something that people are familiar with in that context. So let's define what we mean. Actually, why don't we use a new board for this.

So we're going to say that a is congruent. We want n to b. So this will usually be pronounced a is congruent to b modulo n if and only if n divides a minus b. So you might also see this written as a congruent to b mod n. Who has seen this notation before? Many. Who has seen this notation? A couple, not quite as many.

So for the purposes of this class, we're going to generally be using this notation. We're going to try not to use the right one. Yes, right. And I will explain why in a few minutes. The right one, Even. For people who think they're familiar, it often leads to some confusion. So let's try and stick with this one until you really know what you're doing. But for future reference, if you see the right one, it means the same thing.

So basically, we would like to consider a and b to be the same. You can think of this, roughly speaking, as equals if n divides their difference. So for example, if we're working modulo 5, there are only five different distinct values.

So we're going to notate them like this. So this is the congruence class of 0 modulo 5, so everything that's congruent to 0. So this is going to be 0 plus or minus 5 plus or minus 10, et cetera. So that's one set of values that are the same.

Got a second one, represented by 1. And this is going to be 1, 6, 11, minus 4, minus 9, so everything that's equivalent to 1 modulo 5. And then we've got three more defined analogously.

And so for a general k, which of these five groups is it going to belong to? How would we figure it out? Yeah?

AUDIENCE: Divided by [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah, so the answer was we're going to divide it by the modulus 5 and look at the remainder. So a general k is going to be an element of the remainder when we divide k by 5. Does that make sense to everybody?

So in particular, if we write k equals 5q plus r, where r is between 0 and 5, then k is going to be an element of this set. Does that makes sense to everybody? Reasonably happy with this? OK.

So more generally, recall the division theorem. So the division theorem says, for all pairs n, d with d greater than 0, there exists a unique pair of integers q and r with 0 less than or equal to r less than d such that n equals qd plus r. And we say that q here is the quotient.

And we sometimes denote this as div n, d. Or sometimes, we might write this in infix notation, n div d. And r is the remainder. So this is going to be rem n, d. Or sometimes, we also write this as n rem d. Yeah?

AUDIENCE: [INAUDIBLE]?

BRYNMOR CHAPMAN: Sorry?

AUDIENCE: The exclamation after [INAUDIBLE].

BRYNMOR CHAPMAN: Oh, the exclamation after the exists. This means there exists a unique pair. So not only does there exists some pair, but there's only one of them.

So when working modulo n, a number is always going to be equivalent to its remainder. Sometimes we'll also call this its residue. And just as we saw up here, these residue classes form a partition of all of the integers. Oh, sorry. So the number is 0 up through n minus 1. These represent all of the possible groupings modulo n. Does that make sense to everybody?

So the following theorem is quite useful. So a and b are congruent modulo n if and only if the remainder of a, n is equal to the remainder when you divide b by n. So how might we prove this rigorously? Any ideas? Somebody? Volunteers? Yeah?

AUDIENCE: [INAUDIBLE] a is q bar. And do the same for each. You can have q [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah. So we're going to use the division theorem. If we apply the division theorem to both a and b, we're going to get the same r. I'm going to back up a step first.

At a very high level, what do we need to do in order to prove a statement like this? We're trying to prove an if and only if. We have to prove implications in both directions. So first direction, if rem a, n equals rem b, n, then a is congruent mod n to b.

So we're going to assume that these are equal. So then the r that we get from the division theorem is the same in both cases. So a equals qn plus r. b equals q prime n plus r.

Now what happens when we subtract them? Well, then we get a minus b equals n times q minus q prime plus r minus r. And this is 0. So now the difference is a multiple of n. So by our definition, a and b are congruent. Does that make sense to everybody? Yeah?

AUDIENCE: Can [INAUDIBLE] examples of a, and b in certain regular numbers?

BRYNMOR CHAPMAN: Oh, so some examples of a, n and b?

AUDIENCE: Yeah.

BRYNMOR CHAPMAN: OK. So, for example, 17 is congruent mod 5 to 12. Because 5 divides the difference. If you subtract them, you get 5. 5 is a multiple of 5. So they're congruent.

17 is also congruent to, say, 32. If you subtract these, you get negative 15-- same deal. It's not congruent to 33. If you subtract those, you get negative 16, which is not a multiple of 5. Any other questions? Yeah?

AUDIENCE: [INAUDIBLE]?

BRYNMOR CHAPMAN: So this is only half the proof. We're proving one direction. So we are assuming that the two remainders are the same. And we're trying to prove this.

So if the two remainders are the same, that's from the division theorem. We've got the same r in both cases. So we're going to write both numbers in that form. So a is qn plus r. b Is q prime n plus r prime. But we established that r is equal to r prime. So we're just writing that as q prime n plus r.

And now in order to show that a and b are equivalent, we have to subtract and see whether the difference is a multiple of n. So in this case, when we subtract them, the r's cancel. The n factors out, and we get n times q minus q prime. So that is indeed a multiple of n. And so n divides the difference. So they're equivalent, congruent. Yeah?

AUDIENCE: Can you just please repeat how you worked [INAUDIBLE] that notation with congruencies?

BRYNMOR CHAPMAN: How we say this?

AUDIENCE: Yeah.

BRYNMOR CHAPMAN: a is congruent to b mod n. Or a is congruent mod n to b. There are several different ways of saying it.

What about going in the other direction? Suppose a is congruent mod n to the b. Now we want to prove that the remainders, when you divide by n, are the same. How do we do that? Yeah?

AUDIENCE: We know that we might say for [INAUDIBLE], some k times n. Could we add that difference to one of them? Could we take b minus n [INAUDIBLE] and add that to b. Then we should get a, then n, I think-- and then we'll have a equals [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah. So the last step here is now to use the division theorem again. So if we apply the division theorem, I guess, to b is probably going to be the most useful. We can write b equals-- let's do the same form that we had there, q prime n plus r.

Now, a is b plus kn. So that's going to be q prime plus k times n plus r. And now the division theorem says that this q prime plus k and r, those are unique. So that q prime plus k is the q that we need. And the r is the same. So both of them have the same remainder. Does this make sense to everybody? Yeah?

AUDIENCE: I'm just wondering how you want to show that a is-- a is congruent to n, the n mod [INAUDIBLE].

BRYNMOR CHAPMAN: a congruent to b mod n?

AUDIENCE: Yes.

BRYNMOR CHAPMAN: So what we're trying to prove in if and only if here, so for one direction, we're assuming one side and trying to prove the other. And for the other direction, we do the opposite. So this is one direction. We're assuming that the remainders are the same. And we want to prove that they're equivalent, they're congruent.

For the other direction, we assume that they're congruent. And then we want to prove that the remainders are the same, so two separate proofs. Any other questions?

In some sense, we can consider the n different numbers, like 0 through n minus 1, to be the only numbers we care about when working mod n. Everything else is going to be equivalent to one of those. It's going to be equivalent to its remainder.

So I'm going to take a moment here to talk about notation. So the remainder, which we've called rem a, comma n-- so our convention. Is that even if n is negative, this remainder should always be positive. Not everybody uses this convention.

So in particular, when you're dealing with programming languages, most have some operation that looks like this. It may be denoted differently in different languages. Sometimes, it's a percent sign. Sometimes, it's actually rem or mod, or something like that. And sometimes, it'll behave the same as how we defined it.

Sometimes, it'll be allowed to be negative. So if n is negative, the remainder might be negative or something like that. And some languages have both, usually with different names, like mod versus double mod.

In this class, whenever we write rem a, comma n, we always mean the positive or the non-negative remainder. So this is always going to be between 0 and n. And perhaps even more confusing, sometimes this would be written as mod of a, comma n; or even worse, an infix notation, a mod n.

So this is why we don't like to use the word "mod" when talking about modular congruences because if you see something like, say, a equals b mod n, what does that mean? Who can tell me what that means? Yeah? Do you have a guess?

AUDIENCE: Oh, but I was thinking it was a [INAUDIBLE].

BRYNMOR CHAPMAN: And why is that?

AUDIENCE: Why? So that's just the definition.

BRYNMOR CHAPMAN: Yeah, the answer was that's just the definition. So the important distinction here is between these two things. These are very different statements. The mod here is attached to this equivalence sign.

And so this is talking about a relation between a and b. This is a function written in infix notation. So this is saying that a is actually equal to the one value that you get when you divide b by n and take the remainder. So these mean different things.

It is going to be much less confusing if you use a equals b rem n, or in prefix notation rem b, comma n for the left one, and a congruent mod n to be for the right one. So it's hopefully, much more obvious what the distinction is between these two things than between these two things. So please use the ones on the bottom until you are very comfortable with modular arithmetic.

So let's go back to the actual content now. So as I promised before, we're actually going to be talking about arithmetic. So let's start on that.

So the simple statement that we wrote up there on the left, even plus odd equals odd, in some sense, that's saying something profound. No matter which even number and which odd number you pick, if you add them together, you're always going to get an odd number.

And, more generally, if we take any a congruent to, let's say, 3 mod 5 and any b congruent mod 5 to, say, 4, if you add them, what do you know about it? What do you know about their sum? Yeah?

AUDIENCE: 2 mod 5.

BRYNMOR CHAPMAN: Mm-hmm. So their sum is always going to be congruent to 2 modulo 5. Or perhaps an easier thing to see is it's always going to be equivalent to 7. Which is, in turn, congruent to 2. So adding a and b modulo 5, you get the same result as if you add these two equivalent remainders.

So we have a theorem. Suppose that a and b are equivalent mod n. Then for all c, we have the following. I have space here. So a plus c is congruent to b plus c. a minus c is congruent to b minus c. c minus a is congruent to c minus b. And a times c is congruent to b times c.

So As. You might expect, if you want to add, subtract, or multiply modulo n, you're allowed to replace things wherever you want with something it's equivalent to. So at any point during this computation, you can replace-- oh, sorry, different a and b. This is not relevant for the theorem statement.

But if a and b are equivalent, then you can replace a's with b's wherever you want, and you'll get the same result. Does that make sense? So, question, what about a to the c and b to the c? So let's assume that c is positive for now.

Can I say anything about exponentiation modulo n? If we assume that a and b are congruent modulo n, can we say anything about a to the c versus b to the c? Yeah?

AUDIENCE: Would they be the same because the maximal value of a [INAUDIBLE] possible part from the [INAUDIBLE] part of that is the same?

BRYNMOR CHAPMAN: Yeah. So let me rephrase that slightly. You can prove it more formally by induction. So you can repeatedly multiply. Every multiplication is going to give you congruent values. So by the time you get to the power of c, they're still going to be congruent.

So, yes, this is true and the proof, by induction on c. So our base case is going to be when c equals 1. In this case, our assumption is that a is congruent to b. So a to the 1 is congruent to a. Well, it's equal to a. b to the 1 is equal to b. So this is fine.

Our inductive step, so assume that a to the c minus 1 is congruent mod n to b to the c minus 1. Now, what happens when we increment our exponent? Well, what is a to the c? Yeah?

AUDIENCE: a is [INAUDIBLE].

BRYNMOR CHAPMAN: So we can strip off a factor of a. Now we can replace each of these factors individually. So by our theorem up there, this is congruent to b to the c minus 1 times a. We can replace this factor. And now by our theorem assumption, we can replace this factor as well. Does that make sense to everybody?

What about c to the a and c to the b? So we just saw that when we're working modulo n, we're allowed to replace the base of exponents as we like. Can we do the same thing with the exponents themselves?

Show of hands for yes? Show of hands for no? No seems like it's winning out by popular vote, but not by much. There are a lot of abstentions. Can anybody give me a reason why or why not? Yeah?

AUDIENCE: My reason is just because there's one example of 2 squared is not congruent mod 5 [INAUDIBLE].

BRYNMOR CHAPMAN: 2 squared is not congruent mod 5 to what?

AUDIENCE: 2 cubed.

BRYNMOR CHAPMAN: 2 cubed. OK, that is a true statement. Does that--

AUDIENCE: In this case, it would be, if you want to prove [INAUDIBLE] it'd have to be proof by induction. That's the thing that's false. You just need one counterexample.

BRYNMOR CHAPMAN: Yeah. So you are correct that we only need one counterexample. Is this a counterexample? So let's see. So the claim is that if a is congruent to b mod n, then c to the a is congruent to c to the b. We haven't satisfied our precondition here. 2 is not congruent to 3 mod 5.

So you have the right idea. We do want to find a single counterexample that will suffice to disprove this. We're going to need a different counterexample if we want this to work. Does anybody else have an idea for a counterexample? Or failing that, does anybody have a proof? Yeah?

AUDIENCE: I could if it's a's, but you could split up c to the b's in smaller components and then show that it's [INAUDIBLE].

BRYNMOR CHAPMAN: OK. What are the smaller components, factors of c?

AUDIENCE: Yeah, basically.

BRYNMOR CHAPMAN: OK. So what do you want to do with those factors of c? I suppose we could strip off, say, a is smaller than b. We could strip off a of them.

AUDIENCE: And then whatever's left over, if that's mod whatever that is. That's true. And then we know [INAUDIBLE] the whole truth is true.

BRYNMOR CHAPMAN: OK. So you want to divide out a bunch of factors of c until we get something like this?

AUDIENCE: Yes.

BRYNMOR CHAPMAN: OK. How do you divide mod n? Let's look at a concrete example. So let's keep trying to look at 5. Let's say b minus a is also 5. Is this a true statement? Sorry, did somebody-- is this true for all c?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: So I claim that minus 1 is not going to work here. Yeah?

AUDIENCE: Anything to the 0 power is 1 is true.

BRYNMOR CHAPMAN: Yeah. So anything to the 0-th power is 1. That's fine. The problem is we're subtracting a from both of these exponents. So if, say, you have b equals 5 plus a, you're going to end up with 5 on the right-hand side.

So our counterexample is going to be-- maybe we could have something like c to the 1 and c to the 6. And in particular, we're going to want c to be minus 1. Ah, n was five-- that's right. So this is our counterexample. We've exhibited a specific a, b, and n, where our purported theorem statement fails.

It is not the case that minus 1 to the 1 is congruent mod 5 to minus 1 to the 6. The left-hand side is minus 1. The right-hand side is positive 1.

So when exponentiating, we have to be careful. We are allowed to replace the bases of exponents. We're not allowed to replace the exponents themselves.

So we will see in a little while how we can get around this to some degree. We can do something with the exponents. It's just not this. Well, why don't we take a look at an example first.

So suppose x is 11335 to the 11111 multiplied by 6 plus 7799 to the 5,000. How might we compute the remainder of x after we divide by 100? How can we use the two terms that we did prove to compute that efficiently? What might our first step be? Mm-hmm?

AUDIENCE: We try to distribute, separate out the 1,000 times 6 plus 11,000 times the 7,000?

BRYNMOR CHAPMAN: So the answer was distribute this across this addition. I claim that that's going to make our lives harder, not easier. So what was the theme of the two theorems that we just proved? If we want to do computations modulo n, we can replace things by other numbers that are easier to work with and which are congruent.

So computing the remainder when we divide by 100, that's looking for a computation modulo 100. So we can replace these values, modulo 100, and make them easier to work with. Are any of these values that I've written down congruent to anything nice modulo 100? Anyone? Yeah?

AUDIENCE: Is the first term that you're multiplying the 11,000-- 11,335 to the 11,000 whatever? Can you write that is congruent to 35 to the--

BRYNMOR CHAPMAN: Yeah.

AUDIENCE: 11,000 whatever.

BRYNMOR CHAPMAN: Yeah, so we can just get rid of these. That's congruent to 35. What else can we do? Yeah?

AUDIENCE: Can you explain again why that-- we just get rid of that?

BRYNMOR CHAPMAN: So we're computing modulo 100. We're looking for the remainder when we divide by 100. So we know that 1-- whoops, 11335 is congruent to 35 modulo 100.

AUDIENCE: [INAUDIBLE] over the last two digits?

BRYNMOR CHAPMAN: Yeah. So we're getting rid of the first three digits and only looking at the remainder after we divide by 100. So basically, the idea is that we can do this division at intermediate steps. We can take remainders in the middle of our computation. That's what these two theorems are telling us.

Anything else that we can simplify? No? Does somebody want to do that computation by hand? No, nobody? Yeah. OK.

AUDIENCE: So we do the same thing with the 7,000 [INAUDIBLE].

BRYNMOR CHAPMAN: OK.

AUDIENCE: It'd be 99.

BRYNMOR CHAPMAN: OK, yeah, we can do the same thing here, turn that into just 99. I claim that we can take that a step further. 99 is not particularly easy to work with. I claim that there's something else that's equivalent to that that is. Yeah?

AUDIENCE: 0?

BRYNMOR CHAPMAN: Not 0.

AUDIENCE: Negative 1

BRYNMOR CHAPMAN: Negative 1, yeah. So we can replace this 7799 with negative 1. Negative 1 is easy to work with. So now what happens? Yeah?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah. So let's exponentiate this negative 1. So we end up with 6 plus 1, which is 7. Now what do we do about 35 to the 11,111? Well, we don't really know how to do anything with exponents, right?

So let's just try to start exponentiating it and see what happens. So what's 35 squared? Well, that's going to be-- well, if we actually compute it, it'll be 1,225, I think. Is that right? 1,175? 1,225. So that's going to be congruent to 25.

35 cubed? Well, it's going to be 25 times 35. So that's 875. So that's going to be congruent to 75.

35 to the fourth? Well, 35 to the fourth is going to be 35 squared, squared again, so 25 squared. 25 squared is 625. So that also has a remainder of 25.

So what's going to happen after this point? What happens is we continue multiplying by 35? Mm-hmm?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah. The answer was it'll alternate between 75 and 25. Whenever we have an odd power, as long as it's greater than 1, when we exponentiate 35, it's going to be 75. Whenever we have an even power, it's going to be 25. We can prove that formally by induction. I'm not going to do that here.

But the point is 35, we've got an odd exponent here. So we can replace this with 75. And now 75 times 7 is going to have a remainder of 25. So does that make sense to everybody?

We perform the computation, but instead of just doing it over the integers and then reducing mod 100, we're reducing mod 100 whenever we can. We're always trying to replace intermediate values with things that are easier to work with. And that simplifies our computation considerably. Yeah?

AUDIENCE: How did you know 75 is [INAUDIBLE] 25?

BRYNMOR CHAPMAN: You can perform the computation. 25 by 21 is possibly an easier one to do. Any other questions? Yeah?

AUDIENCE: I think there was a step where we went from 6 plus negative 1 to the 5k to 7.

BRYNMOR CHAPMAN: Yes.

AUDIENCE: I was just wondering what happened there.

BRYNMOR CHAPMAN: So we had 6 plus negative 1 to the 5k. So we are exponentiating this negative 1 over the integers. Negative 1 to any even power is going to be 1.

AUDIENCE: k is even?

BRYNMOR CHAPMAN: Sorry?

AUDIENCE: Do we know k's even?

BRYNMOR CHAPMAN: Oh, sorry, 5k, 5,000. Sorry, it's not actually-- yeah, my bad, this kind of k. Sorry. That's my bad. Any other questions? Yeah?

AUDIENCE: So [INAUDIBLE].

BRYNMOR CHAPMAN: Pardon?

AUDIENCE: Will all phases exhibit a pattern?

BRYNMOR CHAPMAN: Oh. So the question was, is there always going to be a pattern like this? So this is kind of touching on stuff that we will see later. But yes, there will always be some pattern. It may not be this easy to find.

But the basic idea is that there are only 100 different values that it could take, modulo 100. So if you have more than 100 powers, something's going to have to collide. And At that point, it'll start repeating.

Here, it happened to be quite nice. It started repeating very quickly. And the period is only two. That may not always be the case, though. but we will see, in a moment, something more about what we can say about that.

So we've seen how to add, subtract, multiply, how to change the bases of exponents. What about division? Are we allowed to divide modulo n? So suppose we have 3x is congruent to 3 modulo 6.

So if we had this over the integers, say, or over the reals-- I guess reals are a better example-- if we just had 3x equals 3, how would we solve this for x? It's not a trick question, I promise. Yeah?

AUDIENCE: Divide by 3.

BRYNMOR CHAPMAN: Yeah, you just divide both sides by 3. You can cancel off this 3, and you just get x equals 1. So now the actual question is, can we do that modulo n? Can we do that modulo 6? Are we allowed to just cancel these 3's and conclude that-- oops-- x is congruent to 1 modulo 6? Yeah?

AUDIENCE: I think so because the [INAUDIBLE] multiplying by 1/3 [INAUDIBLE].

BRYNMOR CHAPMAN: OK. So the answer was yes, because it's the same as multiplying by 1/3. So remember that 1/3 is not really something that we can-- it doesn't really make sense modulo, modulo n, or at least, not modulo 6. Sometimes it might make sense. Sometimes it might not. We'll see more about that in a moment.

But what is a third? We're talking about integers. Yeah? Sorry?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: So other way around, multiply instead of dividing?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: OK. So the suggestion was instead of dividing by 3, let's try multiplying by something, so that we get 1 here. So let's try to multiply this, multiply both sides by some a. And this should end up being 1, if we choose our a appropriately. What a do we choose? Does there exist such an a? Yeah?

AUDIENCE: The original claim is false because if we set x equal to 3, 3x is [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah. So the original claim is false. The counterexample is that we could take x's 3 here. 3 times 3 is 9. That is congruent to 3. But x is not congruent to 1. So the answer, I guess, to the followup question is that no, there is no such a. We cannot divide by 3 or multiply by something to get 1.

And this is basically the same thing that we were doing last week. We're looking for a solution to 3a is congruent to 1 modulo 6. If we unpack what this actually means, 6 divides 3a minus 1. Is there a solution to this? No.

So basically, that's asking if we can write 1 as a linear combination of 6 and 3. But 1 is not a multiple of their gcd, so we cannot. So does that make sense to everybody? So we cannot always divide. Are there circumstances under which we can divide? Yeah?

AUDIENCE: Oh, I was thinking you divide the 6, as well?

BRYNMOR CHAPMAN: Oh, OK, so the idea was to divide the 6 as well. Yeah, I suppose you could do that. But we're specifically trying to do arithmetic modulo 6. So that may or may not make sense.

But I mean, yeah, I suppose you could say 6 divides 3x minus 3a. And so you could factor out a 3 and say that x is at least odd. And in fact, that does characterize the solutions to the original problem. It's just that may or may not be what you're actually looking for.

So under what circumstances are we allowed to divide? So we just saw that we can't divide here, because there's no solution to this equation. What if there is a solution? What if instead of modulo 6, we had modulo 5? Would we be allowed to divide here?

If we have 3x is congruent to 3 modulo 5, can we then conclude x is congruent to 1 modulo 5? Seeing some nods. Why? Well, basically, exactly the same reason, this exactly characterizes when what we described will work.

If the modulus and the coefficient we're trying to divide by are co-prime, if their gcd is 1, then we'll be able to divide. So more formally, let's write out what we mean. So let's start with the definition.

So we'll say that a multiplicative inverse of-- let's call it x-- modulo n, which we will denote x to the negative 1 is a number which, as you might expect, satisfies the following congruence. So just as we have multiplicative inverses over the reals-- so x times x inverse should be equal to 1, in that case-- we are defining something analogous when we're working mod n. So does that definition make sense to people?

So as an example, 1 inverse, so 1 is a multiplicative inverse of 1. Maybe I should write it like that, mod anything. 2 is a multiplicative inverse of 3 mod 5 because 2 times 3 is 6. 6 is congruent to 1 modulo 5. So 2 and 3 are modulo inverse, modulo inverses of each other, modulo 5.

AUDIENCE: Can you explain that again, the last part of it?

BRYNMOR CHAPMAN: The last part? Yeah. So what this is saying is that 2 times 3 is congruent to 1 modulo-- oops, I should write it like this. So 2 times 3 is 6. 6 is congruent to 1 modulo 5. So that means that 2 and 3 are multiplicative inverses of each other modulo 5 because when you multiply them, you get 1. Does that make sense?

So when do multiplicative inverses exist? Can anybody finish this theorem statement? Can anybody characterize this? When is a invertible modulo n? Yeah?

AUDIENCE: Then you [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah, when the gcd of a and n is 1. And why is that?

AUDIENCE: It wasn't 1 [INAUDIBLE] multiply a by the numbers you could [INAUDIBLE].

BRYNMOR CHAPMAN: OK, yeah, so that's good intuition. If their gcd were not 1, like, say, the gcd is 2, so both a and n are even-- multiplying a by anything is going to give you an even number. That's never going to be congruent to 1 modulo another even number. So more formally, so a has an inverse mod n if and only if there exists a b-- so this is just the definition-- such that ab is congruent mod n to 1.

Now, how do we characterize when this is true? Well, let's unpack this definition here. So this means that n divides their difference.

So-- oops-- why don't I write this as ab minus 1. So we're saying that n divides ab minus 1. We're looking at what that division actually looks like, what the factor of n is. So there's some q such that qn is ab minus 1.

Now we can rewrite this. So 1 equals ab minus qn. So we're saying there exists b and q such that 1 equals ab plus minus q times n. So this is just saying that 1 is an ILC of an. And as we saw before, this happens if and only if their gcd is 1. So does that make sense to everybody?

So if two numbers have a gcd of 1, then we can divide by 1 when working modulo the other. So if we have, say, 7x is congruent mod 30 to 14, then we are allowed to divide by both sides because the gcd of 7 and 30 is 1. So we're allowed to divide both sides by 7. So we are allowed to conclude that x is congruent mod 30 to 2.

I suppose more formally, we want to find a multiplicative inverse of 7. And I think 13 is such an inverse, 7 by 1391. Yeah. So if we multiply both sides by negative 13, we'll get a coefficient of 1 over here, and we'll get 2 on the right-hand side. So sometimes, you can divide, but not always.

So let's use that now to figure out what more we can say about exponentiation. so the following is a theorem, which is attributed to Fermat, as many things are. It's often known as Fermat's Little theorem, not to be confused with Fermat's Last theorem, which Fermat-- I feel like that one should not be attributed to him at all, because he didn't prove it. Or I think he thought he knew a proof and was like a complete fuck up, but whatever.

Fermat's Little theorem is a different story. It is much more elementary. He did actually prove it. It states the following. So if p is prime, and a is not a multiple of p, so a not congruent mod p to 0, then a to the p minus 1 is congruent mod p to 1.

So if you think about what this is saying a little bit, it's similar to what we were trying to do with exponents earlier. But instead of getting rid of multiples of p in an exponent when we're working mod p, we're instead going to get rid of multiples of p minus 1. So basically, we can always factor out an a to the p minus 1 without changing the end result. Yeah?

AUDIENCE: [INAUDIBLE]?

BRYNMOR CHAPMAN: Sorry. Thank you, Zach. I promise I'm awake. Yeah, if a is congruent to 0, then clearly, this theorem is false. a should not be congruent to 0. If a is congruent to 0, then a to the p minus 1 is also 0.

So how could we prove this? Any ideas? It's a bit of a weird proof idea. Let's consider the following set. So a, 2a, 3a, all the way up to p minus 1 times a, now what can we say about this set if we reduce everything in it modulo p?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah. So the answer was that this is basically equivalent to-- this is abusing notation a bit. The claim is that all of these are distinct modulo p, and none of them are 0. Why is that?

Well, first, probably the easier part, why is none of these 0? That's basically saying, why is none of them a multiple of p? Well, all of the coefficients on a are less than p. So p doesn't divide any of those. p also doesn't divide a, by assumption. and p is prime, so it doesn't divide any of these products. So none of these is 0. Why are they all distinct modulo p? Yeah?

AUDIENCE: If we think of a being a different system and modulo p, then they're all some constant from 1 to minus 1 times that n. And none of those will be the same or [INAUDIBLE].

BRYNMOR CHAPMAN: OK. Let me try and rephrase that. So if you look at two different values, like two different coefficients, you said, so suppose for contradiction, a times i equals a times j. So we're actually going to use a instead of n. Or sorry, this should be small p. What is this telling us? Yeah?

AUDIENCE: So p prime and a and b are co-prime.

BRYNMOR CHAPMAN: That's right.

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: Yes.

AUDIENCE: So i equals j.

BRYNMOR CHAPMAN: Yes. So the answer was p is prime. So a and p are co-prime, right? So a has an inverse. We can cancel it. So this tells us that i is equivalent mod p to j.

The two coefficients are equivalent. The two coefficients are coming from the set 1 to p minus 1. So if they're congruent mod p, they're actually equal. OK? So that means that all of these values are going to be distinct modulo p. None of them are 0. So they're these particular values.

What happens when we multiply everything in S together? Well, if we multiply everything in this set, what do we get? Yeah?

AUDIENCE: So is it p minus 1 and then the [INAUDIBLE]?

BRYNMOR CHAPMAN: Yes, p minus 1 factorial, that's what it's called. So we take the product of both sides. We have the product of this-- or sorry, the product of this one is going to be equal to p minus 1 factorial.

What about the other one? Well the other one is going to be the same, except we've got a bunch of factors of a. How many factors of a? Yeah?

AUDIENCE: [INAUDIBLE].

BRYNMOR CHAPMAN: Yeah. So this will be a to the p minus 1 times p minus 1 factorial. So p minus 1 factorial is equivalent to p minus 1 factorial times a to the p minus 1. What does that tell us? Yeah?

AUDIENCE: Again, because p is prime, none of numbers from 1 p minus 1 [INAUDIBLE] p. So p minus 1 factorial is [INAUDIBLE].

BRYNMOR CHAPMAN: OK. So the answer was that because p is prime, none of these numbers are a multiple of p. So their product is not a multiple of p. So p minus 1 factorial is not a multiple of p. So it has an inverse.

So that means that we can cancel it from both sides. And we end up with 1 is congruent to a to the p minus 1. So we have p minus 1 factorial is congruent mod p to p minus 1 factorial times a to the p minus 1. These cancel. And we have 1 is congruent to the p minus 1. And that's the result that we were looking for.

So if we're working mod n, we cannot generally reduce exponents mod n. But if n is prime, we can instead reduce mod n minus 1. Does that make sense to everybody?

So as an example, so if we wanted to, say, find the remainder of 7 to the, say, 95 modulo, let's say, 13, how might we do that? Well, 13 is prime. So instead of computing 7 to the 95, let's reduce that mod 13 minus 1, so modulo 12.

So this is going to be the same as 7 to the, what is it, 11? mod 13? Now what can we do? What is 7 to the 12? Sorry? Did somebody give an answer? No?

AUDIENCE: It's 1.

BRYNMOR CHAPMAN: 1, yes. So 7 to the 12 is 1. 7 to the 11 times 7 is 7 to the 12. So this is the modular inverse of 7 modulo 13. What can you multiply 7 by to get 1 mod 13? Yeah?

AUDIENCE: 2.

BRYNMOR CHAPMAN: 2. So that's all we have time for today. I will see you on Thursday. And if you have any questions, feel free to come up and ask.