PROFESSOR: So welcome to this week. We are going to talk about number theory. Actually, before I forget, there are some handouts at the very back. Please raise you hand if you don't have any, then one of us can actually come over and hand you out this sheet, which contain some facts about the visibility. Thanks a lot. And we will be using these throughout the lecture.

So today we're going to talk about number theory. And this is a really different way of thinking, actually. But we will use the same concepts as you have learned before, like induction, and invariance, stuff like that, to prove whole theorems. So what is number theory?

Well, first of all, it's a very old science. One of the oldest mathematical disciplines. And only recently it actually got to have some more practical applications. So what this number theory-- it's actually the study of the integers. And what are the integers? Well, these are the numbers 0, 1, 2 3, and so on. So number theory got-- Oh, there's some more over here. Another handout over there.

So number theory got used actually in cryptography only about 40 years ago. And at the end of the second lecture, we will be talking about this application into cryptography. There are many application in cryptography. But we'll be talking about one of them to show you how useful this actually is.

Now cryptography is the study and practice of hiding numbers. So you can imagine how important that is. We have like medical data that we need to store outside in the cloud. Right? So, gee. Do we really want that? We actually want to hide our information. We do not want others who are not allowed to see my private information to see it. So this art of hiding information is extremely important, especially nowadays. And number theory actually will help us with this.

So number theory is something, you'll be very surprised, that can be used to save-- oops. I

have to put this on. To save New York City in the *Die Hard* number 3, I believe. So let me start up again.

So let's see where it plays.

Maybe not.

[VIDEO PLAYBACK]

-Yeah, go ahead and grab it.

-You're the cop.

-Simon said you're supposed to be helping with this.

-I'm helping.

-Well, when you going to start helping?

-After you get the bomb.

Careful.

-You be careful.

-Don't open it.

-What? I got to open it. And it's going to be all right.

[BEEPING]

[ELECTRONIC CHIRPING]

Shit.

-Shit! I told you not to open it.

[PHONE RINGING]

[PHONE RINGING]

-I thought you'd see the message. It has a proximity circuit, so please don't run.

-Yeah, I got it. We're not going to run. How do we turn this thing off?

-On the front there should be two jugs. Do you see them? A give gallon, and a three gallon. Fill on of the jugs with exactly four gallons of water and place it on the scale, and the timer will stop. You must be precise. One ounce or lower less will result in demolition. If you're still alive in five minutes, we'll speak again.

-Wait! Wait a sec.

I don't get it. You get it?

-No.

-Get the jugs.

Obviously, we can't fill the three gallon jug will four gallons of water, right?

-Obviously.

-I know. There we go. We fill the three gallon jug exactly to the top, right?

-Uh-huh.

-OK. Now we pour that three gallons into the five gallon jugs, giving us exactly 3 gallons in the five gallon jug, right?

-Right. Then what?

-Now, we take the three gallon jug, fill it a third of the way up--

-No, no. He said be precise. Exactly four gallons.

-Every cop in 50 miles is running his ass off, and I'm out here playing kids games in a park.

-Hey. You want to focus on the problem at hand?

[END PLAYBACK]

[LAUGHING]

PROFESSOR: All right. You can imagine what we are going to do right here, right? So. You can imagine what's below this table is a bomb.

[LAUGHING]

You guys have to save 6042.

[LAUGHING]

So we have the fountain here. Each tennis ball is one gallon of water. We have a big jug, five gallons and three gallons. So you all got to help me out here. So who has an idea of what we can do? So.

AUDIENCE: [INAUDIBLE]

PROFESSOR: All right. Let's first do that. Fill up the three gallons.

AUDIENCE: And pout it into the five.

PROFESSOR: Let's pour it into five. Maybe someone else can-- can continue. Over there.

AUDIENCE: If we do the same again, we'll end up with just one gallon in the three gallon.

PROFESSOR: Uh-huh. So, let's do that. Because that's true, right. You can only fill it up to five gallons. So only, at more, two gallons can add to this, exactly two gallons. And one gallon is left. All right, next one. You? Would you like to--

AUDIENCE: Take out the five.

PROFESSOR: Take out the five. All right.

And then what?

AUDIENCE: Pour the one over there.

PROFESSOR: Pour the one over here?

AUDIENCE: [INAUDIBLE]

AUDIENCE: Then fill the three gallon, and put it into the five.

PROFESSOR: All right. That's great. And I fill it up right here. Fantastic. So we actually have four gallons here. And luckily, they are safe. Right? So you say, thank god. 6042

So we can continue.

So this is actually pretty amazing, though. How can we get four gallon out of three gallon jug, and a five gallon jug? And that's what we are going to talk about in more generality, actually. And if you would just change it a little bit, right? Then things would get more difficult. For example, if you would change the five gallon jug into a six gallon jug, can we still get four gallons? No. Why not?

AUDIENCE: [INAUDIBLE]

PROFESSOR: Everything has to be multiples of three. That's exactly right. This is a multiple of 3. 1 times 3. This is 2 times 3. So if I do combinations with those, like pouring one into the other completely, or emptying, of filling up, we always will have a multiple of three gallons in either one of those, or both.

So we can never have four gallons. So this is something that we would like to analyze a little bit more. And to do that, we're going to first a all start with a definition. Actually you can put up the screen over here. So let me take that out.

Can someone up there pull up the screen? Maybe not? Maybe later.

All right. So let's go with a definition.

We say n denote by m and a bar, and a, we mean m defines a. And how do you define this? Well, we say that n defines a, if and only if there exists an integer k, such that a can be written as some multiple m, mainly k times m. So if you look at this definition we, for example, have that 3 divides 6, like what we just discussed. There's something interesting going on. Suppose a is equal to 0. Well, any integer will define a, will define 0. Why is that? Because I can't take k to be equal to 0, so this is equal to 0 times any integer m. So m defines 0 for all integers. So

this is kind of the exception, right?

And we are going to use this to set up a theorem, and analyze this whole situation over here. Now in order to do that, we will need to sort of define what we can do with all this. So there are states. We will define a state machine. We will see what kind of possible transitions we can have. And once we have modeled all this very precisely, we can start proofing stuff.

Now let me first of all write out what our assumptions are. So suppose we have an a gallon jug. So in our case, a equals 3. And we have also b gallon jug.

And in our case, b equals 5, right? And we issue that a is at most b. That is sort of the situation that we are working with. And he would like to prove a theorem. Exactly what we notice over here, that three defines both. The three gallon jug, and the six gallon jug, we would like to prove something like this. If m defines a, and also m defines be, well, then m should define any results that I can get with the pouring, and emptying and filling those jugs. So this is the theorem, if you'd like to prove. And we can only do that if you start to have a proper model for this.

So let's go for that. And--

And, well, the state machine that we're going to use here looks like this.

First of all, the states that we have are the number of gallons that are in these two jugs. So we will denote those by pairs.

Pairs x, comma y. And x denotes the number of gallons in the a gallon jug. The number of gallons m m that we abbreviate as by the a jug, and y is the number of gallons in the b jug.

So these are the states. And the start state it exactly as it is right there. We have nothing in either of the jugs.

So that's the pair 0, comma 0. So now we start to build up some mathematics here, right? So we express the state of this whole situation by a pair of number. Now we need to find out what they can do with it. So what are the transitions?

The transitions are, as we have seen, right? We can just fill one of the jugs. We can empty those. And the other possibility is that we can pour one jug over into the other one as much as we can. So let's write all of those out.

We can do emptying. Well, how does that change the state?

If we have x gallons in this jug, and y-- and y gallons in that one, we can transition this into, for example, emptying the a gallon jug. So be y of 0. Or we can empty the b jug.

Well, filling is something similar.

But now we are actually pouring more water from the fountain, essentially. Right? All those tennis balls here. And we can fill up say the a gallon up to a gallons, and leave the b jug as it is. Or w we can fill up the b gallon jug, and leave the a gallon jug as it is. So these are these two transitions. And the pouring of one-- of one jug into the other is actually a little bit more complex. So let's have a look.

So how does pouring work? Well, suppose we start with x and y. So let's have a look here. Um, I don't know. Suppose we have 2 balls in here, and 2 balls in here. Well, in that case, I can say pour all of these over in here. Right? So that's easy. But there's also another possibility, better when I pour all of these over in here. But hey, I can only put in 1 ball, because it's only a three gallon jug. So I'm left with only 1. A gallon in this jug.

So these are two-- these are two situations that we need to explain. So let's first do the first example that I just did. I pour everything over into the other jug. So we have 0 gallons left in here, and x plus y gallons left in the other jug. And this can happen if there's sufficient space, right? So this can only happen if x plus y is at most b. Which is the capacity of this b gallon jug. Now if that's not the case, then I can pour in just a little bit, like just say 1 ball. Like just one of these can go in here. So that's the other case.

So x, y we'll actually go to-- well, let's just see how this works. How many gallons are left in this b gallon jug to fill up? Well, we have b minus y gallons left, right? Space left. So we can take b minus y gallons out of this one to fill up this one. So let's do it.

We take b minus y gets out of the a jug, and put it all in here, and it makes it completely filled

up. So we have b gallons over here. So this is really equal to x plus y minus b, comma b. And this only is possible if-- if you are essentially in the complimentary case. So we have that x plus y is at least b, such that there is enough gallons in the a jug to be poured over to fill up the b jug.

So these are the two kinds of cases. And, of course, by symmetry we can do also the pouring from the other jug into the first. So let's write all those out, as well. So x, y can actually go to x plus y, comma 0. I pour everything from here to there. And this only holds if x plus y is at most a.

The other possibility is where, exactly as in this case, we can only pour a minus x gallons over from y into this particular jug. And then this one is completely filled up. And then I have a few gallons left over here. So how does that look? Well, we completely fill this up to its capacity. And what is left this is y minus-- how much did we have to pour in here? Well, that's a minus x.

And we again have a similar formula. But it now looks a little bit different. X plus y minus a. And this is only for the case where x plus y is at least a.

OK. So these are all the cases. So maybe there are some questions about this. Is this clear, that we have these different possibilities? Like when we look at these jugs we can either empty them, filling them up. Or we can pour say only 1 ball over up to the full capacity of this jug. Or we can just pour everything over into, say, this jug.

So those are the different cases that are now fully described by this state machine. So now we can start to prove this theorem over here. So how do we go ahead? How are we going to use what you've learned like induction, and invariance? So let's do it.

But before, actually, we do this, let's take this example that we had and see how we can describe all the transitions that we just did, as far as I remember them. So we have that a equals 3, b equals 5. Right? We start with empty jugs. We need to filled up the five gallon jug, right?

Then we started pouring the five gallon jug as much as we could into the three gallon jug. So it's one of those rules. We've got 3 into 2. Then we emptied the three gallon jug. We got 0 and 2. Then we did-- What did we did next? Oh yeah, we poured everything into this one. So we have 2, 0 as the next state. We filled up-- actually I forgot exactly what we did next. But I think

we filled up the five gallon jug. And then we simply poured over as much as he could from the five gallon jug. And we got 3 and 4, and here we are. We got 4 gallons.

So what we just did is fully describe this state machine. So let's not try to prove this theorem.

So as I said, we're going to use induction.

So you always would like to write this out if you solve your problems. What are we going to assume? Well, we assume actually that m defines a, and m defines also b. That's the assumption of the theorem, and now we need to prove that defies any result that you can achieve in this state machine. So what's the invariance that we are thinking about?

Invariance is going to be--

Oops.

It's a predicate. And it says something like, if the state xy-- if this is the state after n transitions--

Then we would like to conclude that m the fights both x, and m defines y. So this is our-- our invariance. And we like to use this to prove our theorem. So how do we start usually, right? So we always start with-- with a base state. Great. So let's do it.

The base case is-- well, we start with the all 0s, like the empty jugs. It's-- well, and we also-- have paid a little bit of extra attention to what we mean by division over here. We said that all integers actually divide 0. So in particular, m. m divides 0. m, 0. So the very initial state, 0 comma 0, is indeed complying to is particular invariant. So let's write it out. So we have the initial state 0, 0. We know that m divides 0. And therefore, we know that p 0 is true. So that's great.

So the inductive step. How do we start the inductive step-- step all the time?

And we will assume, actually, p of n, right? So lets assume that. And now we would like to prove p, and then n plus 1. So what do we really want to do? We want to say, well, we know

that we reached a certain state x comma y, for which m divides x, and m divides y. Now we would like to show that if we transition to a next state, we again have that same property, that m divides the number of gallons in both jugs once more. And then we can con-- can conclude p, n plus 1. So that's how we always proceed. So let's see where we can write it out in a bit more formal way.

OK. So how do we go ahead? Suppose that x, y is the state after n transitions.

Well, what can we conclude? Well, we have the predicate pn, the invariant. So we know that n divides x, and n divides y. And we concluded that because pn is true.

So after another transition-- what happens after another transition? So we can conclude that the jugs are filled by the different types of numbers that we see here this is state machine. So let's write them out. So after another transition, um, each of the jugs is actually filled-- Um, are filled with-- well, either if I've emptied it, say a 0, 0 gallons, a, b, x and y. I see appearing over here. And I also notice that I see x plus y. And x plus y, minus b. And x plus y, minus a. Those are all the different number of gallons that can be in jug. Yes, please?

AUDIENCE: [INAUDIBLE]

PROFESSOR: In our example-- Yeah, that's a good question. So in our example problems of 3 and 5, it turns out that the only number that divides 5 both the three gallon jug, and the five gallon jugs is actually one. So in our example, we would have that m equals 1. So over here we have that only 1 divides a, as well as 1 divides b. So m equals 1 in our case. But for example, in the three gallon jug, and the six gallon jug-- Right? We have that m equals 3, like 3 divides 3, And 3 divides 6. So those are the two cases that you sort of look at right now. But you put into a much more general setting, right, we are distracted away from the actual numbers. And use a and b as representations.

Are any other questions?

So after another transition, each of the jugs are filled with, well, either 0 gallons, if we have a completely emptied them. Or we have filled the first a gallon jug, or it can be b. We also noticed that it can be-- it can be of x, of course. It can be y, because that's the state that we are in. And we can have x plus y, minus a, which appears over here. And x plus y, minus b.

So these are all the different number-- possible number of gallons.

The x plus y. That's also present. Is that true? Yeah. That's right. x plus y. So we also have x plus y. Actually, it's good to check that again. So we have 0, x, y, a, b. Got those. X plus y, and x plus y, minus p, and x plus y minus b. Yeah.

So now we can start using our-- our assumptions. So what our they? We have that in order to prove this-- right? At the top over here, we assume that m divides, and m divides b. So we know that first of all, m divides 0, of course. But we know that m divides a. We know that m divides b. We have concluded that m divides x. And also m divides y.

So if you now use some facts about divisibility on your handout, which we will not prove now. But I think most of them will be on your problem set, actually. We can conclude that also linear combination of a, b x and y will be divisible by m. In particular, m will divide x plus y. m will divide x plus y minus a, and also x plus y, minus b.

So we will conclude that m actually divides any possible results. So divides any of the above. And now we're done. Why is that? Because we have shown now that after the next transition-- after we have reached x, y after n steps, then in our n plus 1-th step, all that you can achieve is divisible by m. So that's exactly the invariance. So we conclude that p, n plus 1 is true. And so now we're done.

Are any questions about this proof? So this is like the standard technique that we tried to use all the time here in this class. We will use it in all the other areas, as well. In graph theory, in particular.

And especially in number theory, will also use it, especially in this class.

OK. So let's apply this to theorem. Let's I think about this movie that we saw, this *Die Hard* number 3. *Die Hard* number 4 came out. And then the cast got stuck in *Die Hard* number 5. There's was a problem, because the rumors were that in *Die Hard* number 5, they had like a 33 gallon jug. That's a lot. And a 55 gallon jug.

So Bruce has in training his muscles, because you can imagine those are pretty heavy. So if you want the pour one into the other, my goodness. So-- but the question is, is he training the right muscles? So can we apply this theorem now, and showed that--

Oh, I should to tell you what is the problem. Well, again, he has to get say 4 gallons out of this-- out of these two jugs. So is that possible? It's not. I see someone shaking his head. Do you want to explain why?

AUDIENCE: A and b are both divisible by 11.

PROFESSOR: Yeah.

AUDIENCE: So any other configuration will also have to be divisible by 11. And 4 is not divisible by 11.

PROFESSOR: Exactly. 4 is not divisible by 11, so the whole cast got blown up in *Die Hard* number 5. And so we have no *Die Hard* number 6, as well.

OK, so-- so now all of this stuff actually helps us to define a new concept, as well. So let's do that. I'll put it up here.

We will use the terminology GCD of a and b as being the greatest common divisor of a and b. So, for example, if we are looking at a equals 3, and b equals 5, well then the GCD of 3 and 5 is actually equal to 1. There's no other larger integer that divides both 3 and 5. In other examples are, for example, if we have the GCD of say 52 and 44. Well, what's this equal to? Well, this actually is 4 times 13. This is 4 times 11. So 4 divides both this, and both this one. But nothing larger can divide both of those. So we have that this is equal to 4.

We will have a separate definition that talks about this very special case where two numbers-- if you look at their greatest common divisor-- when that greatest common divisor is equal to 1, we actually define those two numbers to be relatively prime to one another. So let's put that out over here.

So that's another definition. We say that a and b are relatively prime if the greatest common divisor is actually equal to 1.

Now today we will not really use his definition so much, but it's actually very important. And we'll come back to this next lecture.

So if we now look at this particular thing them over here, can we see a nice corollary of this? Like a result, if you think about this greatest common divisor. Well, the greatest common divisor off a an b divides both a and b. So the greatest common divisor of a and b will divide any result that we can generate by playing this game with the jugs. So the corollary here is that the GCD of a and b divides any result.

OK, so that's really cool. So this already tells us quite a bit about this game that we have here. So now what we would like to do is to find out what exactly we can be reached? We have a property that we have shown here. But what else can we do here?

Now it turns out that you can say much more, and we would like to prove the following theorem to make-- to analyze this whole thing much better. I don't think I need the state machine anymore. So let's take that off.

The theorem that we would like to prove is that any linear combination of the-- let's change this into the 3 and 5 again. Any linear combination of 3 and 5, I can make with these 3 and the 5 a gallon jug. So let's write it out. So any linear combination l, which we writes as some integer s times a, plus some integer t times b. So any linear combination of a and b, with-- well, of course, the number of gallons should fit the largest the jug. So with 0 is, at most l. Is it mostly can be reached.

So this theorem we would like to prove now. And in order to do that, we would like to already think about some kind of a property that we have. So when we talk about linear combinations, the s and the t can be negative, or positive. We really don't care. So for example, we could have like, I don't know, minus 2 times-- so for example, 4 is equal to minus 2, times 3, plus-- actually, is that true? Yeah. Plus 2, times 5. So here we have s to be equal to minus 2, and t is equal to 2. And of course, a is equal to 3, right? And be is equal to 5. So 4 is a linear combination of these two. And according to the theorem, we can create that number of gallons in this jug. And we already saw that, because we did it.

But for our theorem, in order to prove this, we really would like s to be positive. So how can we do that? If anybody has an indea what we could do?

AUDIENCE: Let's assume that b is greater than m.

PROFESSOR: Yeah. We have still that a is supposed to be-- We will assume that throughout the whole lecture. Thanks.

So in order to prove this, we really would like to have s to be positive. So let's just play around a little bit with linear combinations to get a little bit of feeling for that. How could we write 4 differently, as a linear combination of 3 and 5, such that we have actually a positive number over here? Does anybody see another way to see that?

AUDIENCE: [INAUDIBLE]

PROFESSOR: Yeah, that's true. 3 times 3, minus-- minus 5. So-- and how did we do that? Well, we can just say 5 times 3 to this one, and then subtract the same again, minus 3 times 5, over here. And if he adds those things together, he will see 5 minus 2, is 3 times 3, as you said. And we have minus 3 plus 2 is actually minus 1 times 5. And this will be a different linear combination of 4.

So what we can do here, we can sort of play around and make this s over here, which we now say call s prime, is positive.

Actually, it's larger than 0.

So let's start the proof for this theorem. It's pretty amazing to me, actually, that you can do so much a game like this, and see so much happening. So let's figure out how this works. OK.

So let's first formalize this particular trick over here. And how do we go ahead with it? Ah, well, notice that we can rewrite L, which is equal to s times a, plus t times b. s, you know, we can just add a multiple of b over here. n times b, say m times a. And we can subtract the same amount over here, minus n times a, times b. So do you see what I did over here? I have added n times b, times a, and subtracted n, times a times b. And we did something similar over here, not exactly the same. But that's what we did.

And you can imagine that we can choose m, such that s plus n times b will be larger than 0. We can do that. So essentially this proved to us that there exists an x prime, and also the t prime, such that L can be rewritten as a linear combination, s prime, times a, plus t prime, times b. But now with you extra property, that s prime is actually positive.

Now this is really important, because we're going to create an algorithm of playing with those

jugs that can achieve this particular linear combination. And that's how we're going to prove this theorem. So let's assume that 0 is less than L, is less than b. I know that we, in the theorem, we also consider the case is L equals 0, and L equals b. But those are obvious, right? You could either empty the jugs, or just fill up with the bigger one. So we will consider just this case.

All right. So what's the algorithm going to do for us?

The algorithm is going to repeatedly fill and pour our jugs in a very special way. And miraculously we will be able to get the desired linear combination every single time. And of course, we're going to use induction again to prove this property.

OK. So how does the algorithm work? Well, to obtain L gallons we're going to repeat s prime times, which is the number that we have over here. The following algorithm-- we first of all, we will fill the a jug. This one. After we have done this, we are going to pour this into the b jug. So how do we go ahead? We pour- oops. This into the b jug.

And when this b jug becomes full, we are going pour it out. So let's write it out. So when it becomes full, it will actually empty it out. And we will continue pouring the a jug into the b jug. So we'll continue this process.

So let's take an example to see how that works. So we keep on doing this until the a jug is actually empty. So let's take an example.

So let's see. Let's do that over here.

Actually we can do the tennis balls, too. Let's do that first. See how that works. So essentially, in order to get 4 gallons, we just fill up the three gallon jug. We empty it all in here.

We fill it up again. You pour in as much as we can. That's-- that's it. We have to empty this one. Oops. We have to keep on pouring. Put this in here. Fill this one up, and then pour over into the five gallon jug. And now we've got 4 gallons over here. So what did we do? So let's write it out.

So for our special linear combination over here, we have that 4 equals 3, times 3, minus 1, times 5. So we need to repeat this process three times. So let's do that. In our first loop we will do the following. We start with the start state, the pair 0, 0. We're going to fill up the very first jug all the way up to its capacity, 3. And we put it all over into the b jug.

What happens in the second loop?

The second loop, we again fill up the a jug. So we have-- we start at 0, 3. We fill it up. We get 3, 3, the pair 3, 3. We pour everything in here, as much as we can. That give us 1, 5. Only 2 gallons are poured into the bigger gallon. We empty the bigger gallon, the bigger jug. We get 1, 0. And we keep on pouring, and you get 0, 1.

So now in the third loop-- and that's where we should get the 4 gallons.

We start off with 0,1. Um, we fill up the a jug. We pour everything over into the bigger jug, and we get 0, 4. And that's the end result.

So this algorithm seems to work for this particular example. Of course we would like to prove it for the general situation. So how do we do it?

Well, we're going to just to analyze the algorithm in the following way. We can notice that in this algorithm, we fill up s prime times the a jug, and we essentially pour everything out into the b jugs, and we sometimes empty the b jug. So let's try to think about this a little bit, and see how we could try to formalize this.

So let's write it out. We have filled the a gallon jug s prime times. We also know that the b jug has been emptied a certain number of times. So let's-- let's just assume-- suppose that the b jug is actually emptied, say, u times.

I do not know how many times. But I say, well, let's assume it's u times, and try to figure out whether we can find some algebraic expression. So at the very end of the algorithm, let r be what is in the b jug. So let r be the remainder, in the b gallon jug.

So now we can continue. We know if r is what left in the b gallon jug, well, we know already some property of it. Actually, let's put that on the next board. We know that 0 is at most r, and

at most b, because that's what's left in the b gallon jug, right? So we know these bounds. We have assumed that 0 is less than L, is less than b, which we put over there. We know that r must be equal to what kind of linear combination of s prime, and u?

So-- Well, we have been filling of s prime times. So this is what we added in water to the whole system, you can say, s prime times a. And we poured out water. Well, we did that u times from the b gallon jug. So we poured out u times b gallons. So this is the remainder that this left in this bigger jug, right? So are there any questions about this? So-- OK.

So we also know that L is equal to s prime, times a, plus t prime, times b. And this is the linear combination that we would try to prove of, that it is left at the very end. So what we want to show is that r equals L.

So how do we do that now? How are we going to show that r can be expressed in L, in a special way. So let's have a look. So these are all tricks in the sense that I'm giving you this proof, but how do you come up with this yourself? Sometimes you play a lot with these kinds of things, and you get a feeling of what kind of-- sort of pattern exists, and what kind of intuition you need in order to write down a proof like this.

So let's rewrite this. I'm going add t prime times b. And I'm going to subtract it again. So I have s prime times a, plus t prime times b. I subtract it again, and I still have this amount left open here.

So what is this equal to? Well this part is equal to L. So this is equal to minus-- and I have a multiple of b, which is t prime, plus u times b.

Hm. Now this is very interesting. Does anybody see how we could continue here? So we have r expressed as L, minus a multiple of b. And I also know that L is in this range. I also know that r is in this range. So that's kind of interesting, right? So how can that be? What should be the case here? Does anybody see what kind of property t prime plus u must have in order to make that happen? So let's have a look here. We have L. It's in this range. So let's just draw an axis. So at 0, we have b. And somehow in this range, we have L. Now if I subtract like actually b, or something more than b, or I add more than b. I will jump out of this range, and I go somewhere over here, or I go somewhere over there. Right? So if I said suppose L is over here, then L minus b would be over here, which would be negative. Or if I add b, it will be over here, which would be more than b.

Now we know that this is equal to r, but r is in this range. So that's not really possible. So let's write it out. So if t prime plus u is unequal to 0, so we're actually really subtract or add a multiple of b. Then I know that r is either smaller than 0, or r is larger than b. Now we know that cannot be the case, so we can conclude that t prime plus u equals 0. Now that implies that t prime equals minus u, or maybe other way around, because that's easier to see what's happening.

So u equals minus t prime. If you plug that in here, well, we get exactly the same expression. You see? Minus, minus t prime is equal to plus t prime. And we get the exact same linear combination. So we conclude that r equals L.

And now we're done. Why is that? Well, we have shown that the very last number of gallons that is left after this procedure, after this algorithm, is actually exactly equal to the linear combination that we wanted to achieve. So now we got the proof for this theorem that tells us that any linear combination is actually-- of a and b can actually be reached by pouring gallons over and back, and emptying and filling those jugs.

All right let's continue. So there was a question over here that I would like to-- that I would like to address.

So maybe I did not make so clear what the s prime, and the t prime is over here. And in this proof, we started off with this linear combination. I would like to have an algorithm of pouring that creates L gallons in say the bigger jug. So in order to do that, I want to find, say, a linear combination that makes this L such that this s prime is an integer-- positive integer.

Why do I want to have a positive integer? Because in this algorithm, I'm going to repeat something s prime times. If s prime is negative, I cannot do it, right? So s prime has to be a positive integer. In order to create such a positive integer, I can just add like 1,000 times b times, and subtract 1,000 times a times b. That's OK I could just add a lot. And if I add enough, I can make s plus n times b positive. Even if s is, say, minus 100, well, if I add 1,000 times 5, I will get a positive number.

So that's sort of the reason this proof that we want to rewrite the linear combination to a new one, such that s prime is positive. And if we have s prime positive, then we can actually talk about this algorithm, because we can only repeat something s prime times, if s prime is say 1, or 2, or 3, or something positive.

All right. So let's-- I'll talk about say the next part. So we have gone-- We have proved two theorems. But in the end we would like to have a characterization of the greatest common divisor. That's the goal of this lecture.

So let's do it. Um. In order to do this, let's first of all look at our five gallon, and three gallon example. We know that the greatest common divisor is equal to 1. We know that 1 can be rewritten as a linear combination, as 2 times 3, minus 1 times 5. So that means that according to the theorem that we have up here, we can actually make exactly 1 gallon in one of these jugs. So that means that we can also have any multiple of those. So we can reach any multiple 1. That's very special. So this particular case, we know that any multiple of 1, any number of gallons can be reached.

So can we sort of generalize this a little bit by using the greatest common divisor? So the greatest common divisor 3 and 5 is equal to 1. And we have shown that the greatest common divisor defies any result. Can we say something more? Can we say that the greatest common divisor can be maybe written as a linear combination of this type over there? And that's how we are going to proceed now.

So let's set talk about the very special algorithm which is called Euclid's algorithm. And I think in the book it's also called The Pulverizer. And you will have a problem on this just to see how that works, and to really understand it. So let's explain what we want here.

So first of all, we know that for any b and a, there exists a unique quotient and remainder r. So let's write it out. There exists unique q, which we will call the quotient.

And r. We call this the remainder.

Such that b equals q times a, plus r. With the property that 0 is at least r, and at most a. So we're not going to prove this statement. It's actually like a theorem, right? But let's just assume it for now. And in the book you can read about it.

We're going to use this to prove the following lemma that we will need to give a characterization of the greatest common divisor, as a linear combination of integers.

Oh, before I forget, you will denote this remainder as rem of b, a. And this is the notation that

we use in this lecture.

So what's the lemma? The lemma is that the greatest common divisor of a and b, is equal to the greatest common divisor of the remainder of b and a. With a. So what did we do? Let's give an example to see how this works.

For example, let's take-- actually let's do it on this white board.

So, let's see.

For example, let's see whether we can use this to calculate the greatest common divisor 105, and 224.

So how can we go ahead? Well, according to this lemma, we can rewrite this as the greatest common divisor of first the remainder of 224, after dividing out as many multiples of 105 as possible. And 105.

So what are we going to use here? We're going to use that 224 is actually equal to 2 times 105, plus 14.

So we had the GCD of 14 and 105. Now why can I do this? Well, I'm essentially just subtracting like 2 times 135 from 224. Well, the greatest common divisor that divides 105 and 224 also divides 105, and a linear combination of 105, 224. That's essentially what we are using. And that's actually stated in this lemma, and that's what we would like to prove.

So let's continue with this process, and do the same trick once more. So we can say that we can rewrite this as the greatest common divisor of, well, the remainder of 105 after taking out this many multiples of 14 as possible, and 14. So what are we going to use over here? We are going to use that 105 is equal to 7 times 14, plus 7. So this is the greatest common divisor of 7, and 14. Now if you just continue this process, we can see that this is equal to the greatest common divisor, again, of the remainder of now 14, after dividing out as many multiples of 7 with 7.

Now this is equal to 0, 7. Why is that? Because 14 is equal to 2 times 7, plus 0. So 0 is the remainder after dividing out 7 as many possible times as possible. OK. So we have the greatest common divisor of 0, and 7. What's the largest integer that can divide both 0 and 7?

Well, any integer can divide 0. So we know that this is equal to 7. So essentially, what we have done here, we have repeatedly used this particular lemma to compute in the end, the greatest common divisor of 105 and 224.

And we have been very methodol-- we have used a specific method. We used the lemma, and we worked it out. We used the lemma again, and we just plugged in the actual numbers. Used to lemma again. Plugged in the actual numbers, and so on. And this is what is called Euclid's algorithm. And in the book it's also called The Pulverizer. And there's, I think, a few other names. But I like this one.

So this is an example of Euclid's algorithm. So now let's have to look whether we can have prove this particular lemma, and actually I will-- Yep. We're going to prove this lemma.

OK. So how do we do the proof? Well, first before we know that if- yeah. Well, how do we do this? You would like to prove that if the great-- well, if n divides a and b, in particular, the greatest common divisor divides a and b. We would like to show that it's dividing also the remainder of b, after dividing out a, and a itself. If you can show that, then we know that the greatest common divisor of this thing is at least what we have over here.

So I said a lot right now. So let's try to write it out a little bit. So suppose that m is any divisor of a. And at the same time, m also divides b.

Well, then I know that m also divides b minus, say, the quotient, q that we had over here, times a. And-- and this is actually equal to the remainder of b and a. Now we also note that m divides a. So what did we show here? We showed that if m divides, and m divides b, then m also divides the remainder of b and a. And n divides a.

So what does is prove? Well, it proves that, in particular, the greatest common divisor over here divides this one. That's interesting. That essentially means that we have shown this inequality. Because if this one divides this, well, that means that this number over here must be at least what we have over here.

OK. So let's continue.

We consider two cases. If the remainder of b and a is unequal to 0, well, what can we say now? We can say that if I know that m divides this remainder of b and a, which can be

rewritten as b minus q, times a. And I also note that-- if I also know that n divides a, then this actually implies the reverse of this statement, that n divides a, and divides b.

Now why is that? Well, we're actually using the fact that if n divides b, minus q, times a, and m divides a, then m also defies any linear combination of these two. In particular, this plus q, times a, which is b. m divides b.

So maybe I'm going a little bit fast here, I notice. This all also has to do with all the lecture handouts. You see a few facts on the divisibility. And in particular, item number three that talks about the fact that I'm using here. If a divides b on your handout, and a divides c, then I know that a divides any linear combination of b and c. So that's essentially what I'm using here repeatedly.

OK

So let's look at the other case. If the remainder is equal to 0, well, then I actually know that b minus q, times a is equal to 0. Well, if I know that m divides a, well, then since 0 equals b minus q, times a, I know that b equals q, times a. So if m divides a, I also now that m divides b. So this is one argument. This is another one. And this was-- These are the three arguments that now show that anything that divides these two also divides a and b.

So now we have the reverse argument, right? So this greatest common divisor divides this one here, and this one. And we just proved that it divides a and b, and so it must divides the greatest common divisor of a and b. So now we have shown the other inequality, and this proves equality. So you should definitely look this up in your lecture notes.

So now we can finally prove this beautiful theorem a that will help us to characterize the-- actually, let me put this over here.

So the final theorem that we prove here is that the greatest common divisor of a and b is actually a linear combination of a and b. So we're going to use this algorithm that you have over here, Euclid's algorithm. And we are going to do a proof, again, by induction. And we use an invariance.

So we use a similar kind of strategy, of course. The invariance that we are going to use says-- well, if Euclid's algorithm reaches the greatest common divisor of x and y-- so for example, it's

reach, say, 7 or 14, and 105, for example. Then, say, after n steps then both x and y are linear combinations of a and b. So then x and y are linear combinations of a and b.

And at the same time, we also know that the greatest common divisor of a and b is equal to the greatest common divisor of x and y. So this is my invariance. And the way I will go ahead is to simply do what you do always in these situations.

So we start with the base case. And we can immediately see that after 0 steps in the Euclidean algorithm, I've done absolutely nothing. So obviously after 0 steps, x equals a. y equals b. So of course, they are linear combinations of a and b. And this equality holds, as well. So for the base case--

So after 0 steps, we immediately know that p 0 is true. Now for the inductive step, we have to do a little bit more.

As usual, right? We always assume p n. And now we would like to prove p n plus 1. So how do we do this? Well, we notice that there exists a q such that the remainder of y and x is equal to y minus q, times x. So we assume p n. We have reached some state, x, y. We know that the remainder of y, x equals y minus q, times x, for some quotient q. We know that y is a linear combination of a and b, and x is, as well. So that means that this one is actually also a linear combination of a and b.

So now when we look at this , algorithm we can see that-- that if you look at the remainder that appears in here, that's still a linear combination of a and b. So after a extra step, we notice that what we have reached are still in combinations of a and b. And of course, the lemme has showed-- has shown us that what we reach is still equal-- the greatest common divisor is still equal to what we originally started out with. So this proves p of n plus 1.

So n-- let's finish this particular proof. So for the very last step, if you now look at this particular-- so if you look at the very end, we notice that in every step the remainder is getting smaller, and smaller, and smaller. Right? And you can use a similar kind of proof technique to show that after a finite number of steps, we will reach a GDP of 0, y. Something like this.

So in the very last step of Euclid's algorithm we achieve something off this form. We now use our predicate over here, and say that y is a linear combination of a and b, but the greatest

common divisor of 0, y is also equal to the original greatest common divisor that we want to characterize.

So now we have proved the theorem that says that the greatest common divisor of a and b is actually a linear combination. So now we're going to combine all those three theorems in one go. And that will show us the final result, which is that the theorem that the greatest common divisor of a and b is actually the smallest positive linear combination of a and b.

So we're going to combine all of these together. We know that the greatest common divisor divides any result. The theorem up there says that any linear combination can be reached. And also just showed-- have shown that the greatest common divisor is a linear combination of a and b. So we can combine those three to get this theorem.

So how do we do it? Well, let's just look 0 all the way up to b. Suppose these are all the results that we can reach in our problem. We know that the greatest common divisor divides all of those. At the same time, it's also linear combination that's over here. Since it's a linear combination, it can also be reached, right? By the theorem that we have. So suppose that this is the greatest common divisor. But we also know that the greatest common divisor is dividing all of these points here that can be reached. So therefore, it must be the smallest one.

And I will leave you with some homework to think about this very carefully. And you can show for yourself that you can now combine those three arguments together, and see that the greatest common divisor must be the smallest positive linear combination.

So, I will see next Thursday.