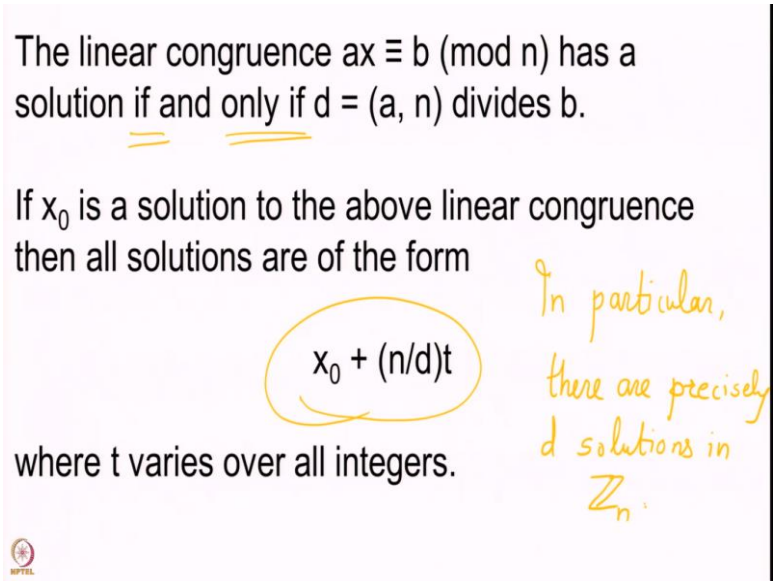
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics,
Indian Institute of Technology Bombay
Lecture No.15
Solving Linear Polynomials Modulo N-III

Welcome back, we are looking at Solutions of Linear Congruence Equations. So, this is of the type ax congruent to b modulo n and we are looking at solutions to such an equation. We saw that there is a solution precisely when the GCD of a and n call d it divides b. So, if the GCD does not divide b the then there is no solution at all.

However, if the GCD divides b then sometimes there can be a unique solution and sometimes there can be more than one solutions. So, we saw all this in our last lecture, so let us just go through that once again.

(Refer Slide Time: 01:08)



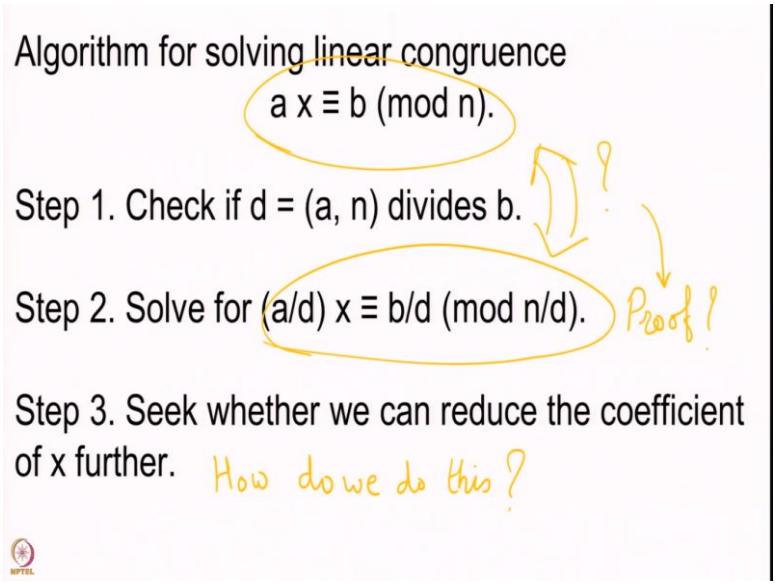
We have that the linear congruence ax congruent to b mod n has a solution if and only if d which is a, n the GCD that divides n. So, once again I would like to point it out to you that there are these two directions to proving this, the first one for if, it would mean that the congruence has a solution if d divides b. So, we will assume that d divides b and we will prove that the congruence has a solution and in the other direction the congruence has a solution only if d divides b.

So, that means when the d does not divide b the congruence does not have a solution or we need to prove that congruence has a solution then d should divide b. So, there are, these are

the two directions which we have proved already. We also then later saw that whenever you have one solution, so now you assume that d is a divisor of b, so that there is a solution and so suppose one solution is named x naught, then all other solutions in the set of integers are obtained by the formula x naught plus n by d into t.

So, this is the formula which gives us all the solutions. In particular if you are looking at solutions modulo n then there are exactly d solutions. So, in particular there are precisely d solutions in the set of residue classes modulo n. So, once this is understood. We wanted to know whether there is an algorithm for solving linear congruences. Okay and there is indeed an algorithm we saw that in the last lecture. So, let us go through that once again.

(Refer Slide Time: 03:26)



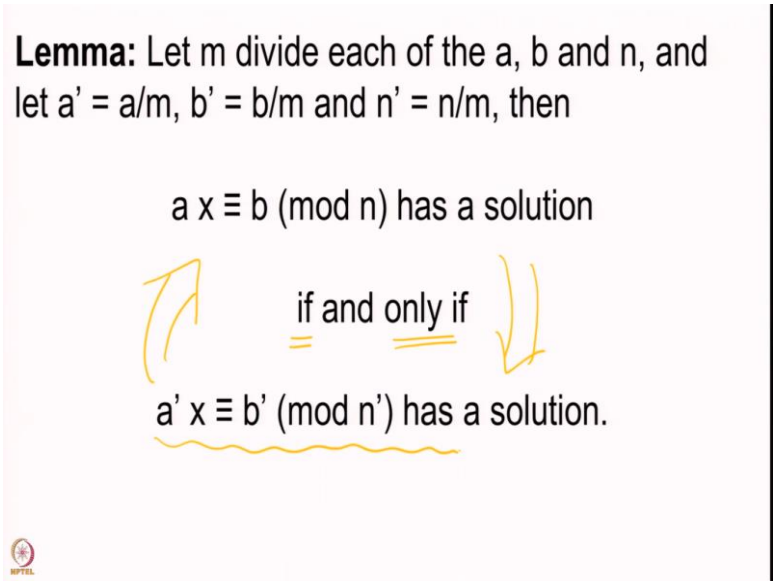
What we want to do is to solve the congruence ax congruent to b modulo n. So, a is given to us, b is given to us and n is given to us and we want to solve this congruence ax congruent to b mod n. The very basic step is to check whether the GCD of a and n divides b. If the GCD does not divide B then there is no solution and we are done. However, if the GCD does divide b that means this d divides all of the a, n and b and then we go to the next step which is that we cancel from all these numbers.

So, here I have a by d, here we have b by d and here we have n by d. We cancel d from all these three numbers and obtain a congruence for which the coefficient of x is small. Ultimately what we want to do is to cancel this coefficient of x. Make it one that is what we would want to do. If you have an equation where the coefficient of x is one, it would read like x congruent to b mod n and then that is the solution that we have.

So, that is where we are going. We are trying to reduce the coefficient of x. That is why we have divided by d throughout. And now the third step is to seekwhether we can reduce the coefficient of x further, so there are two methods to doing it, but before we go to do that we need to prove this statement that we have made here.

That when you solve this, so what we want to show is that solution to this is equivalent to having a solution to this. Are these equivalent? And this proof is needed, so we will give this proof and we will also see what so we will answer this also, how do we do this. There is one method which I will tell you and then there is another impromptu method which also will come. So, right now we are going to prove, state and prove the first part which reads as follows.

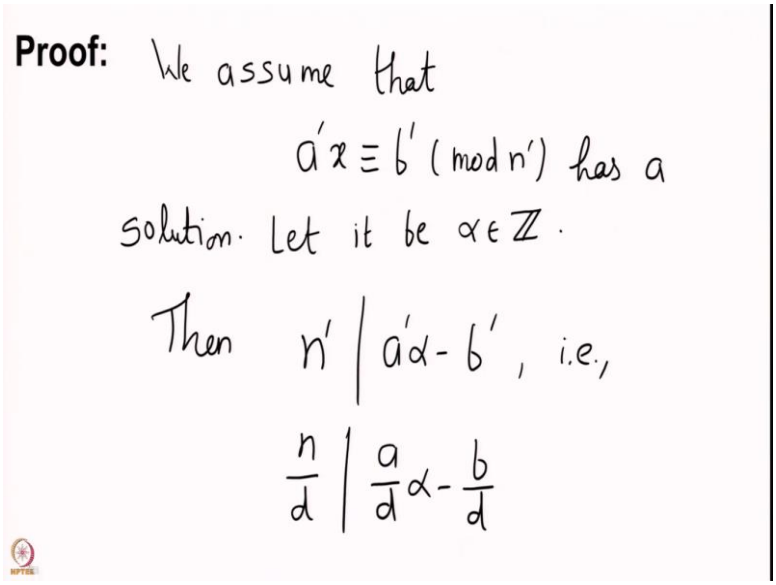
(Refer Slide Time: 06:01)



So, suppose we have that m divides each of the a, b and n and if m divides them then let us just divide them and get a smaller triple a prime, b prime, n prime, then this system has a solution if and only if this system has a solution. So, we want to say that the larger system where a is big has a solution if and only if the smaller system where a prime is smaller than a also has a solution.

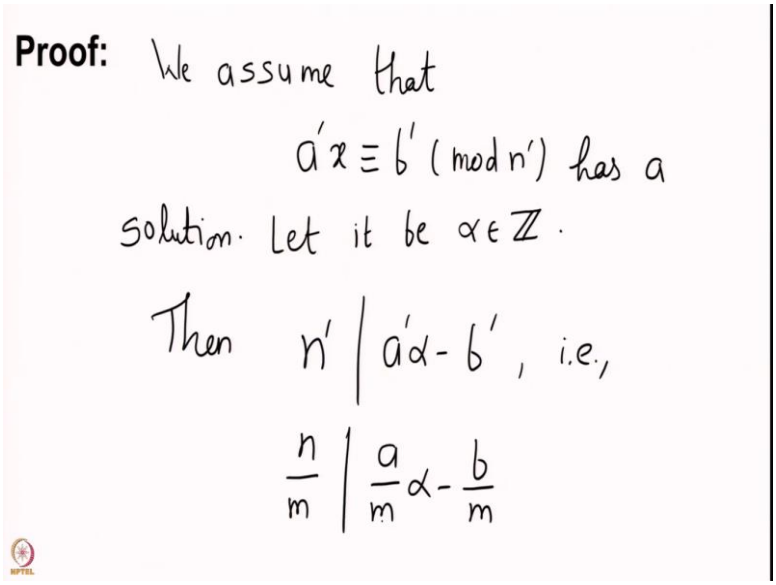
So, as I keep telling there are two parts. There are two parts if and only if. If means that we assume this and prove this and only if means that you assume that part and prove this part. Okay, so ax congruent b mod n has a solution if a prime x congruent to b prime mod n prime has a solution. Therefore, we will assume this part first and then prove this and then we will come back in the other direction.

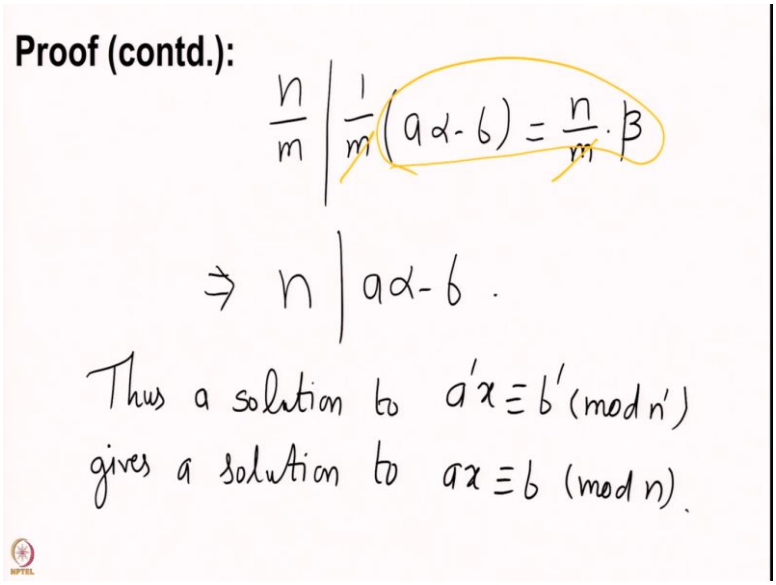
(Refer Slide Time: 07:22)



So, here we go with the proof. We assume that a prime x congruent to b prime mod n prime has a solution. Let it be alpha, so we have some solution in the set of integers, then n prime divides a prime alpha minus b prime, which is to say actually, so I should not really call this as implies but we are just going to rewrite this that n by d divides a by d alpha minus b by d. Okay, so this we are just rewriting this statement because n prime is n upon d, a prime is a upon d and b prime is b upon d or in fact there is no d.

(Refer Slide Time: 08:43)

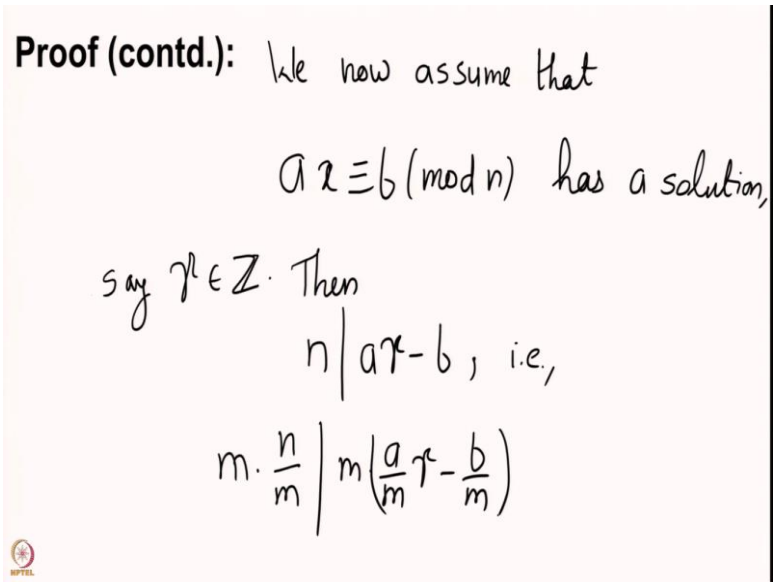




We have assume that there is an integer m, which divides all this does not have to be equal to the GCD, so we have this m coming here. But if I, you have this m you can take this m common from the right hand side so what we get is that n by m divides 1 by m a alpha minus b and this implies that n divides a alpha minus b, because I can simply write this part as n by m into some beta and then we cancel this Ms which come in the denominator to obtain this result.

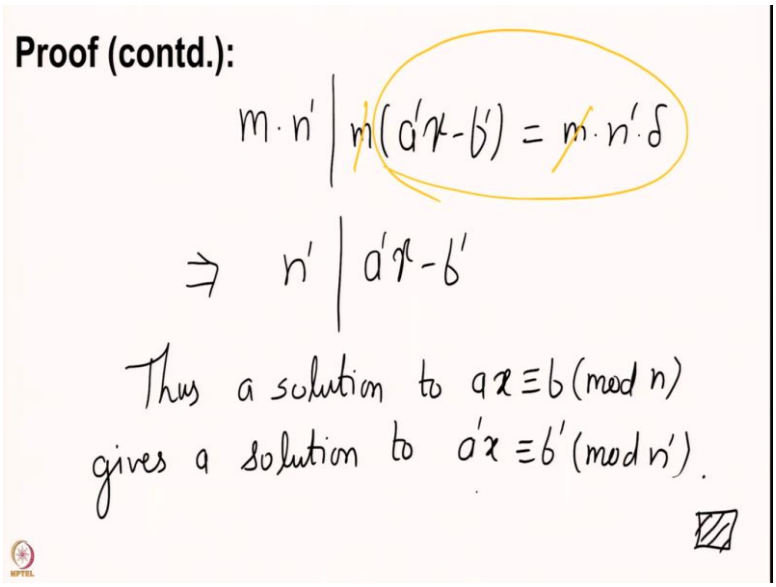
So, these get cancelled therefor we have a alpha minus b is n into beta and therefore n divides a alpha minus b, so we had started by assuming that our congruence a prime, thus a solution to a prime x congruent to b prime mod n prime gives a solution to ax congruent to b mod n. So, this was the if part which is that assuming that there is a solution to the smaller equation with smaller coefficient of x. We have proved that there is a solution to the bigger equation. Now we want prove the other way.

(Refer Slide Time: 10:37)



So, we will start with assuming. We now assume that ax congruent to b mod n has a solution. Say gamma, this is some integer and we have (equatio) this congruence has a solution, so that means n divides a gamma minus b, but now we have that m divides all of the n, a and b. So, we can then write n, m into n by m divides m into a by m gamma minus b by m.

(Refer Slide Time: 11:55)



So, what we do is that we take m common from all these terms and that gives us that m into n prime divides m into a prime gamma minus b prime which implies that n prime divides a prime gamma minus b prime because we can write this as m into n prime into some number

say delta and then we simply cancel out this m on both sides to get that a prime gamma minus b prime is n prime into delta and therefore n prime divides a prime gamma minus b prime.

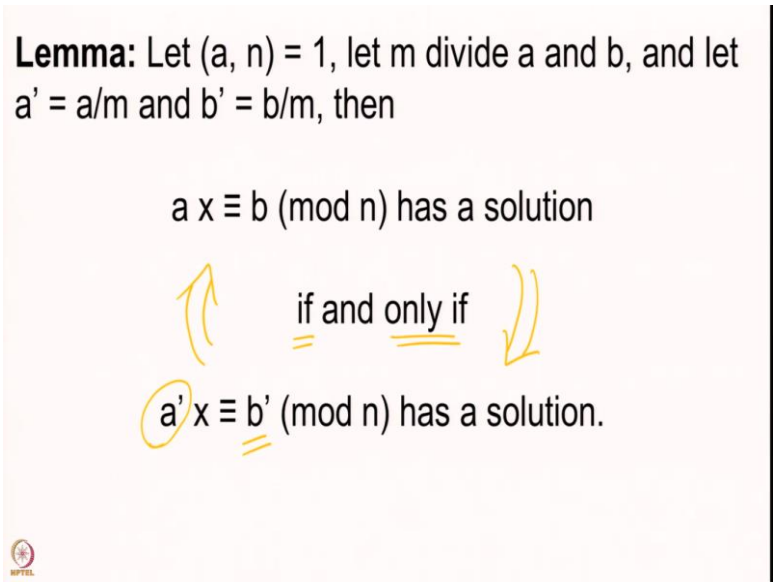
So thus a solution to ax congruent to b mod n gives a solution to a prime x congruent to b prime mod n prime, so we have proved this in both the directions. We started with assuming that there is a solution to the smaller equation and obtained a solution for the bigger equation, larger equation and then we started with a solution to the larger equation and obtained a solution for the smaller equation.

So, the existence of solutions for both of these congruences are equivalent. The existences are equivalent. The number of solutions will change because it will depend on the number n and the d. What may happen is that once you have a GCD d of a and n and suppose that it divides b and if you happen to cancel out this GCD throughout giving you a smaller equation then in this smaller equation the GCD will now become 1 and therefore in the smaller equation you will have a unique solution whereas in the larger equation you will have d solutions.

So, the number of solutions is not going to change. What, the number of solution is going to change possibly. What does not change is whether the solution exists in the very first place. Okay, so this was the first stage where you just simply cancelled out the GCD from, the GCD or a common divisor of all the a, b and n.

Now the question is, the thing that we had, we asked can you reduce the coefficient of x further and this can indeed be done, this is so what we now assume is that the GCD of a and n is 1, this is our assumption. And now we will play only with a and b and then reduce that coefficient of x which is a.

(Refer Slide Time: 15:01)

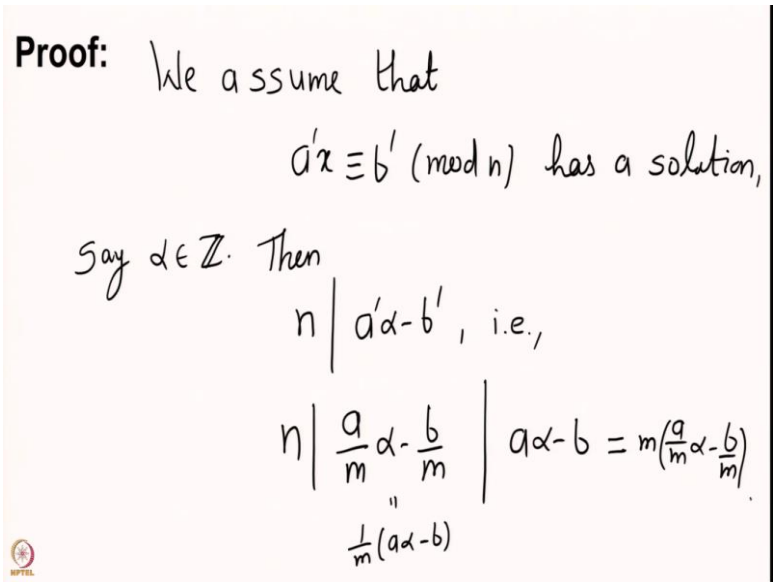


So, it goes a follows we have that the GCD of a and n is equal to 1 therefore there is a guaranty that the solution exists. In fact we are not going to get a unique solution because the GCD is 1. Suppose that m divides a and b. So, remember that we have the congruence ax congruent to b mod n. There is a number m which divides both, the coefficient of x and the constant term.

Then we divide by m to obtain a new a call that a prime which is a upon m and a new b which is b prime which is b by m. Then our original congruence ax congruent to b mod n has a solution if and only if a prime x congruent to b prime mod n has a solution. So, here we have reduced the coefficient of x by having divided it by m, of course, as a bonus we got that this also got reduced.

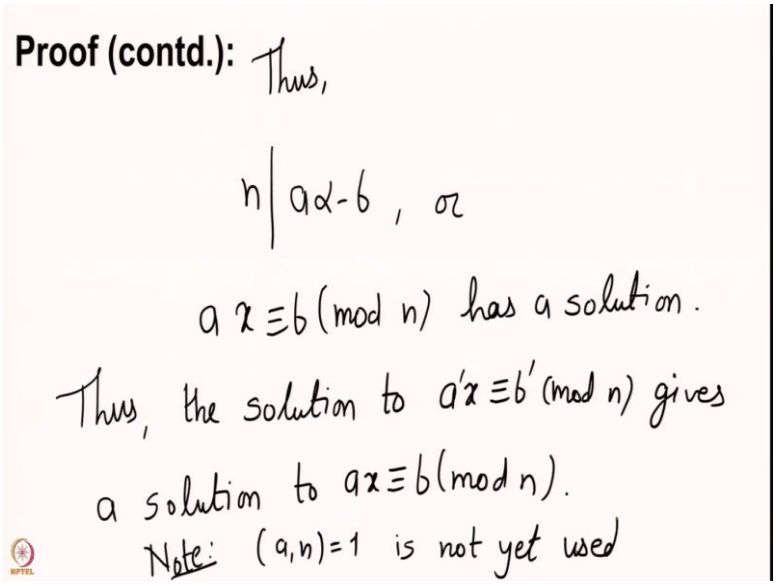
So, whenever you have a common, these n has not changed. n has remained as it is. What has changed are the coefficients of x and the constant term. So, once again we have two parts, if and only if so we will assume the a prime x congruent to b prime mod n has a solution and prove that ax congruent to b mod n has a solution, and then we prove the only if part which is to go from the larger equation to the smaller equation.

(Refer Slide Time: 16:53)



So the proof begins by assuming that, so we assume that a prime x congruent to b prime mod n has a solution, call that alpha. So what we then get is that n divides a prime alpha minus b prime, but remember that a prime was a upon m, so we just rewrite this as a upon m alpha minus b upon m and clearly this number is going to divide a alpha minus b because this is nothing but 1 upon m a alpha minus b or you may consider this as m times a by m alpha minus b by m.

(Refer Slide Time: 18:27)

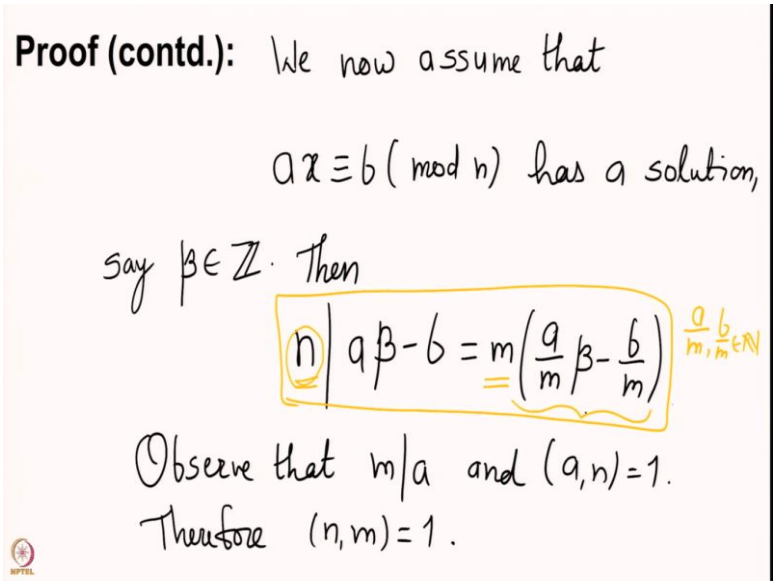


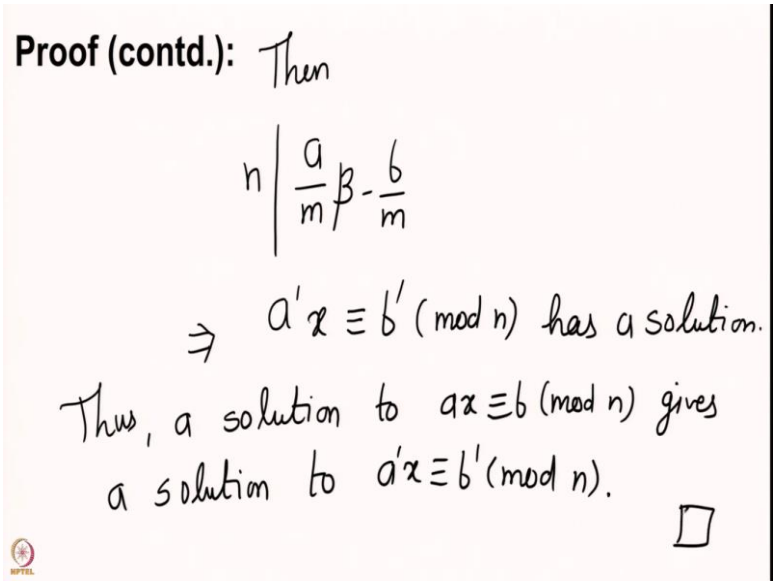
So, what we do get is that n divides a alpha minus b or ax congruent to b mod n as a solution. So, we started with this smaller equation which was a prime x mod, a congruent to b prime

mod n has a solution and we proved that the larger equation has solution, so thus the solution to a prime x congruent to b prime mod n gives a solution to ax congruent to b mod n.

We want to go now in the other directions, so we will assume that the large equation has a solution and we want to obtain a solution to the smaller equation. You would have noticed that there is something that we have not used yet which is that a comma n equal to 1 is not yet used. This is going to be used in the second part. So the second part is where will assume that the bigger equation has a solution and we will prove that the smaller equation also has a solution.

(Refer Slide Time: 20:13)





Say beta in the integers, then n divides a beta minus b but M is a common divisor a and b, so we can write this equation as m into a by m beta minus b by m. Now have come to the (equa) our assumptions observe that m divides a and a comma n is 1, which means that there is not a single prime which divides both n and a. The greatest common divisor or a and n is 1, so there is no common divisor in particular.

There cannot be any common prime divisor and here m is a divisor of a, so the prime factors of m are nothing but the prime factors of a. So, what we get is that the GCD of n and m is also 1. Here we have that n divides a product of m and some number, but n and m will have no common factors. So, every prime which occurs here will have to go and occur in the prime factorization of this number. Note that this is a number here we have that both a by b and b by m these are natural numbers.

We are not looking at rational numbers but natural numbers, so therefore what we must get is that n will in fact divide the right hand side a by m beta minus b by m which implies that a prime x congruent to b prime mod n has a solution. So, thus a solution to the bigger equation ax congruent to b mod n gives a solution to the smaller equation which is a prime x congruent to b prime mod n, keeping the modulus of the congruence constant.

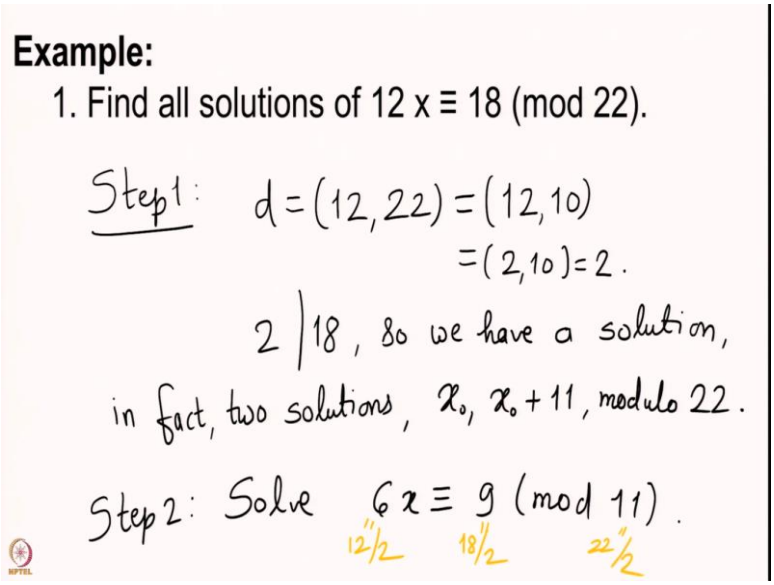
This completes the proof, so remember once again that we have carried out two steps of the algorithm after having checked that the GCD divides b. Step one was to cancel out the GCD from a, b and n and getting a solution to the smaller equation is equivalent to having a solution to the original equation, the bigger equation that was our assumption, that was the first lemma that we proved.

Then the second lemma told us that if you have anything common a and b assume that a and n have GCD 1 and further if you have anything common a and b then even that can be cancelled out. Thus, you can reduce the coefficient of x further. In both thee proofs you would have noticed that the solution that we had started with in both the situation is the solution for the other system.

In lemma one when we cancelled out m and looked at a prime x congruent to b prime mod n prime we started with a solution alpha, the same alpha continued to be a solution for the original equation ax congruent to b mod n and in the reverse direction we started with a solution gamma to x congruent to b mod n and gamma itself was again a solution for the smaller equation a prime x congruent to b prime mod n prime.

In the second lemma where we cancelled out a common factor only from a and b, the solution again did not change. We started with alpha, which was a solution to a prime x congruent to b prime mod n, the same alpha became a solution to ax congruent to b mod n and in the reverse direction as you can see here the beta which was a solution to ax congruent to b mod n continued to be a solution to a prime x congruent to b prime mod n. Now these two lemmas have enabled us to take some more steps, so let us see whether we can solve one such congruence equation in the next slide.

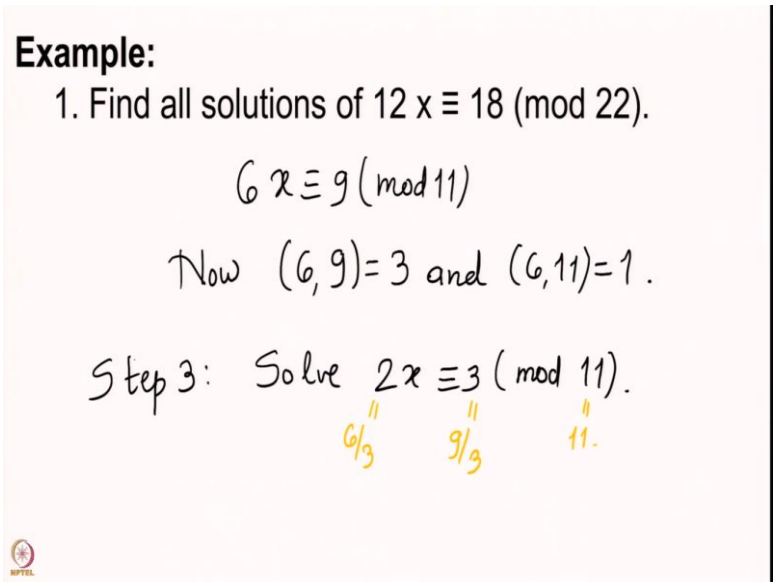
(Refer Slide Time: 26:02)



So we want to find all solutions to 12x congruent to 18 mod 22. Our algorithm says that you compute the GCD. The GCD of 12 and 22, if you want to use the division algorithm will give you the GCD to be, the GCD of 12 and 10 which is further the GCD of 2 and 10 and therefore this is 2. 2 divides 18 so we have a solution, in fact two solutions. These will be x naught and x naught plus 11 modulo 22.

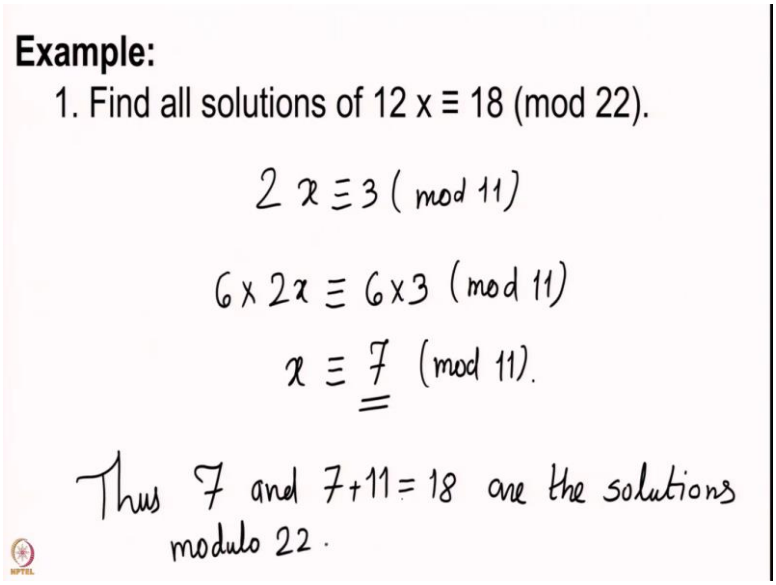
11 is 22 upon 2 so that is step one which is completed, so step two will tell us that solve 6x congruent to 9 mod 11. This is the step two that we want to now solve 6x congruent to 9 mod 11 where is 6 is nothing but 12 upon 2. The GCD is now getting cancelled. 9 is 18 upon 2 and 11 is 22 by 2, so this is an equation which we want to solve.

(Refer Slide Time: 28:02)



Let us go to the next slide and try to solve this equation, 6x congruent to 9 mod 11. Now we observe that both our, now 6 and 9 have a GCD which is 3 and of course, 6 and 11 have the GCD 1 now. So we apply this second lemma that we have proved. So step three says solve 2x congruent to 3 mod 11 because we have cancelled out 3 from both these coefficients, this remains as it is, but this is now a very simple thing 6 2x congruent to 3 mod 11 can be computed quite easily.

(Refer Slide Time: 29:08)



I will simply multiply by 6 on both sides. This is going to be 12x which is simply x. This is 18 which is simply 7. So, this is the solution that we are looking for. So thus 7 and remember

we have to add 7 plus 11 which is 22 upon 2 are the solutions modulo 22, so we have obtained a solution by applying all the steps we have learned. There is one more impromptu step which we can add but we will see this step in the very next lecture so I hope to see you again, thank you.