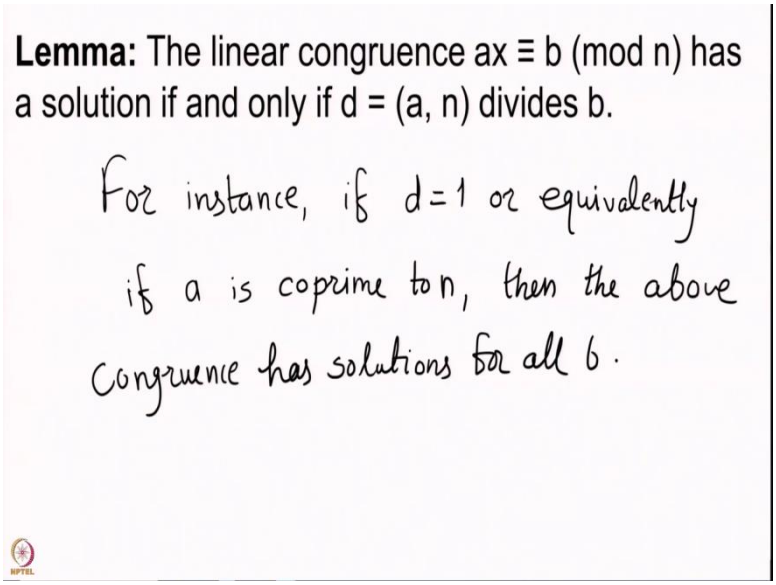
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics,
Indian Institute of Technology Bombay
Lecture 14
Solving Linear Polynomials Modulo n – II

Welcome back. We are looking at solutions of Linear Congruence equations Modulo sum natural number n. We saw that if you take this linear congruence which is say ax congruent to b mod n. Then, the solution exists exactly when you have that this GCD of a and n divides b. So, this holds that the condition really is on a and n. The condition on b is a very mild condition that you should have that this GCD d divides b. That is a very mild condition which is there on b.

(Refer Slide Time: 1:14)

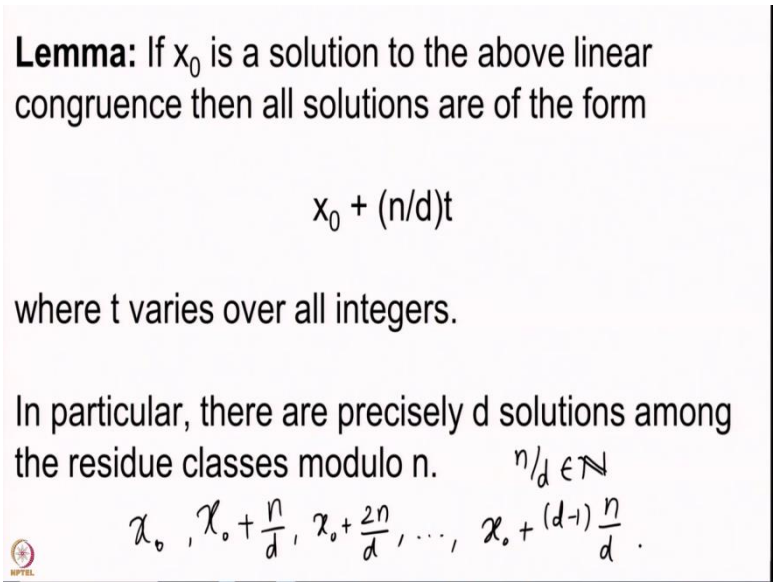


So, for instance, if d is one or equivalently, if a and a is coprime to n, then the above congruence has solutions for all b. So the only important thing here is to note that a is the only important thing. You should look at the GCD of a and n, and the mild condition on b is that d should divide b.

So, I told you in the last lecture that when you are looking at solutions to linear congruences, then there are two problems, which is that there may not be a solution. But now, we have gone modulo this problem so to say by putting a condition on the GCD of a and n. So, now we know when there may, exactly when there can be solution but sometimes there are not unique solutions as we have seen in the clock arithmetic already.

So, when there are not unique solutions, can we get the exact number of all solutions? That is the question. If there are no unique solutions, how many different solutions can there be? That is the question that we want to answer. And this question is related very nicely with the quotient of n and d. So, this is what we have in the next slide.

(Refer Slide Time: 3:29)



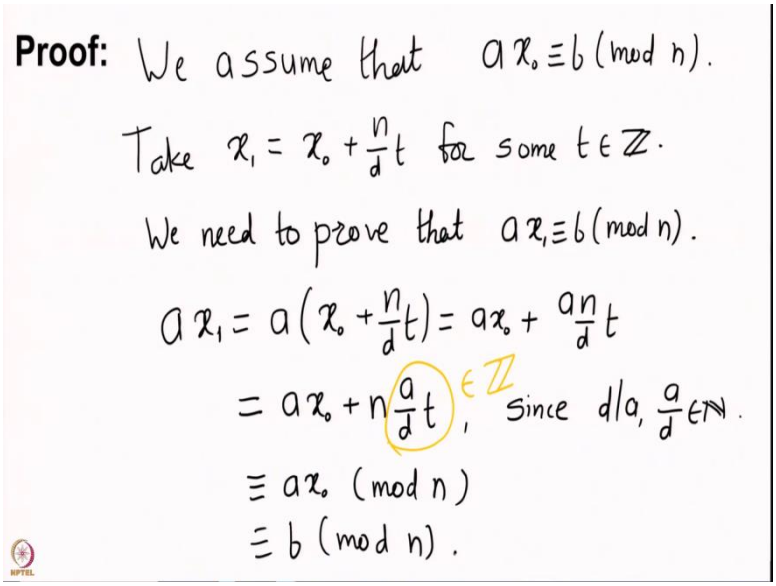
If you have a solutions x naught to the other linear congruence, so remember the above linear congruence was our ax congruence to b modulo n. if you have a solution then all solutions are of the form x naught which is one solution that you had plus n upon d into t, where t is varies over all integers. So the statement is quite simple, if you have one solution, all other solutions are obtained by adding multiples of n by d to that solution and you get all other solutions.

To show, to prove this lemma what we will have to do is to show that whenever you have, x naught to be a solution then x naught plus n by d into t is also a solution for every t. This would be one statement, one direction of proving this lemma. Second direction would be to show that any other solution is also of this form. These are the two directions that we will have to prove.

This is a very important corollary that whenever you are looking at it modulo n then you will have exactly d solutions modulo n. So, these will be given by x naught plus n by d. And before that you will have x naught, x naught plus 2 n by d. So on, all the way up to x naught plus n minus 1 into n by d. these are n different solutions. These are all different. First of all, note that these n by d is a natural number because you have d to be the GCD of a and n. So, in particular d should divide n.

Therefore, n by d is a natural number. And so, but it is a smaller number then n. And when you add that number to x naught, you do not get same elements modulo n. In fact, you do not get the same elements modulo n until you add n times this number. So, these are precisely the d solutions, you should have said instead of d minus 1, I should put, instead of n minus 1, I should put d minus 1. Because when you take the next one it would be x naught plus dn by d, which would be x naught plus n. Then, you would get the same number. Okay, let us go about proving this.

(Refer Slide Time: 6.15)



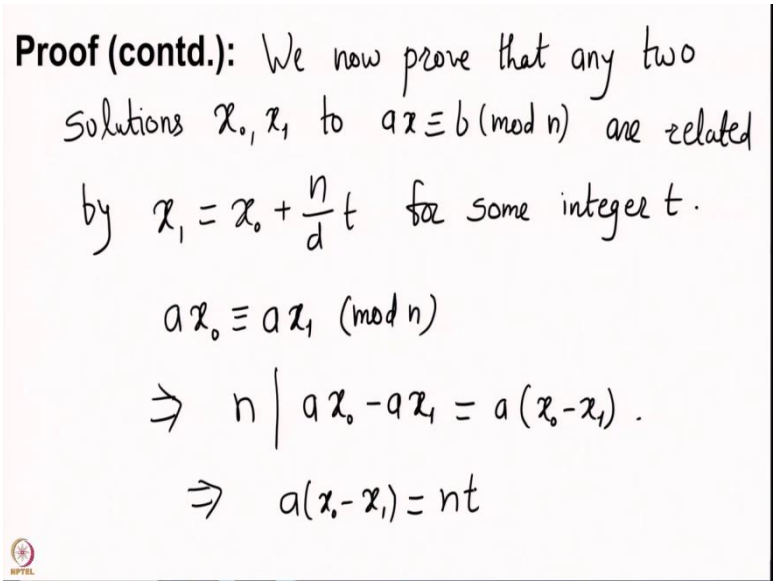
So, first of all, we assume that ax naught is the solution a x naught is congruence to b mod n. So, x naught is assumed to be a solution to this linear congruence and take x 1 to be x naught plus n by d into t for some t in integers. You can take it to be any t. Now, it is very simple. What we just want to prove is that a x 1 is congruent to b mod n. This is the only thing to prove. So, we need to prove that a x 1 is congruent to b mod n. This is all. Let us go about proving it.

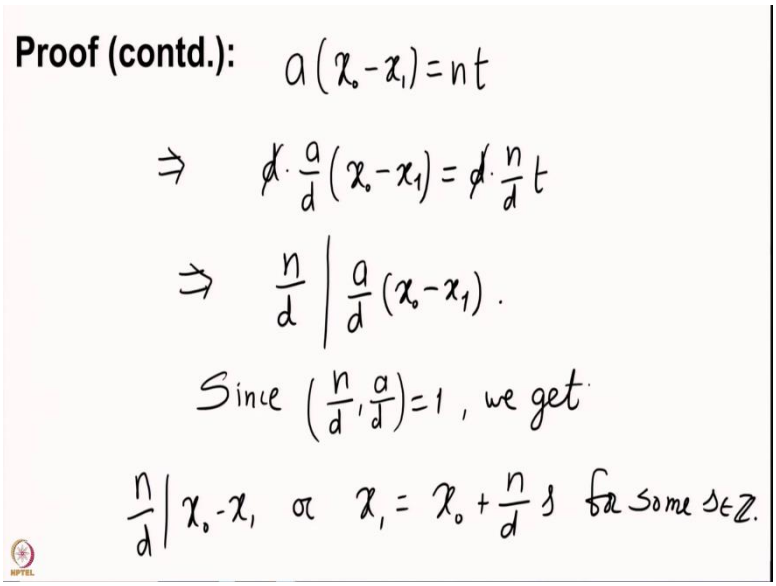
So, a x 1 is a x naught plus n by d into t which gives you a x naught plus a n by d into t but note the d being the GCD of a and n, d divides a as well. And therefore, this is congruent to a x naught modulo n because now we have that all these elements are integers. So, we have written a x 1 to be equal to a x naught plus n times an integer and therefore, we get that a x naught is congruent to a x 1 modulo n and thus we get it to be congruent to b mod n

So, one side was quite easy. We assumed that x naught is the solution and then we proved that any x 1, which is given by x naught plus n by d t is also a solution. Now, we have to

prove the other direction. Which is that, we will start by assuming that there are two solutions and we will prove that the other solution is equal to the first solution plus an integer multiple of n by d. This is what we need to prove.

(Refer Slide Time: 9.37)





We now prove that any two solutions x, naught x 1 to a x congruent to b mod n are related by x 1 equal to x naught plus n by d t for some integer t. This is what we want to prove. So, let us begin. So, we have that a x naught is congruent to a x 1 modulo n because both are congruent to b mod n.

So, we get that a x naught is congruent to a x 1 mod n and which further implies that n divides a x naught minus a x 1, which we can write as a into x naught minus x 1. Now, we

have that d the GCD divides both n and a, so we can cancel out GCD from this equation or alternately we have that a into x naught minus x 1 is say n into t.

Because n divides this difference a into x naught minus x and we have that a x naught minus x 1 is n into t, which further gives us we have that a x naught minus x one is n into t and this gives us that d into a by d, x naught minus x 1 is d into n by d t. So this d's can be cancelled to get that n by d divides a by d into x naught minus x 1. So, here we have two integers one is this a by d. And the other is n by d.

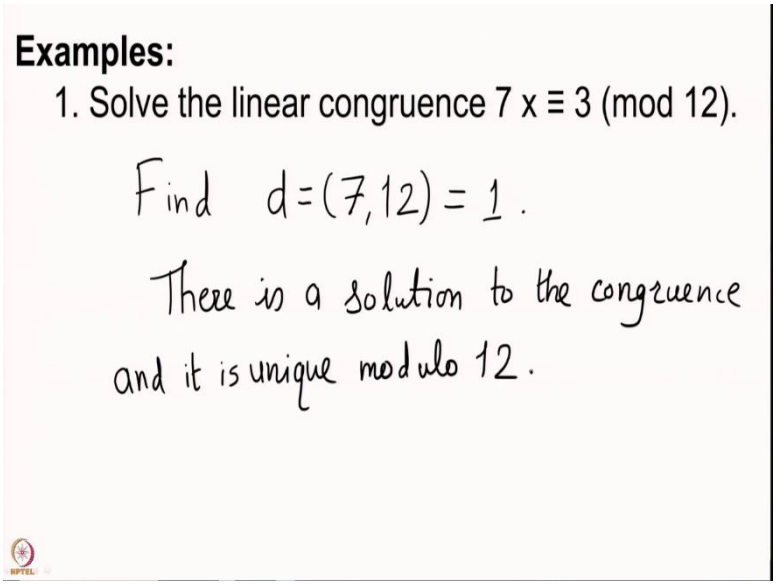
And we have that n by d divides a by d into x naught minus x 1. The GCD that was there for both a and n has now been cancelled on both sides. Therefore, the GCD of a by d and n by d is equal to one. There is no common prime factor between n by d and a by d. So, all the prime factors of n by d would go and divide the difference x naught minus x 1 with all the powers that it would divide n by d. It would divide the difference x naught minus x 1.

So, what we therefore get is, so since, this GCD is one. We get n by d divides x naught minus x one. Or x 1 is x naught plus n by d into some s. So, what we have proved here is that any two solutions to the congruence a x congruent to b mod n differ by a multiple of n by d. And therefore, when we saw the example in, earlier about the (clot) clock arithmetic where we had 2 x congruent to 8 modular 12, the GCD of two and twelve was two.

And so we got exactly two solutions. Therefore, 4 into 2 is 8, similarly 10 into 2 is also 8. And n by d, remember n is 12, d is 2. So, n by d is 6 and indeed 4 and 10 differ by six. That was the only difference between 4 and 10. So any two solutions differ by a multiple of n by d and if you have got one solution, any other solution is obtained by adding a multiple of n by d.

So, this is where we get a complete description to the solutions to the linear congruence, a x congruent to b mod n With this let us go and do some simple examples to get hang of this correctly.

(Refer Slide Time: 15.01)

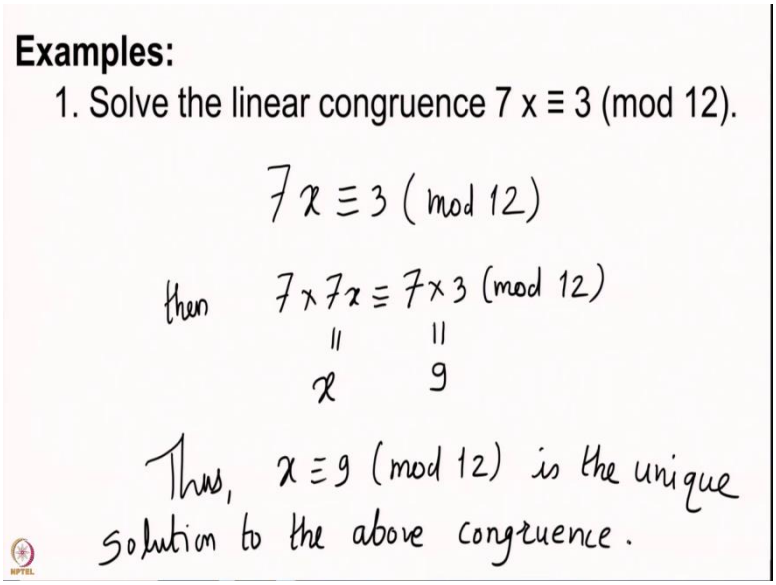


Suppose we are asked to solve the linear congruence 7 x congruence to 3 mod 12. So, first of all what we do is to find the GCD. In this case, this GCD is one. So, we always have solutions, so there are solutions to the congruence and it is unique modulo 12. So, to find this solution we invert 7. It is like 7 x is 3 in some space of numbers. And to compute x, we need to multiply by the inverse of 7. This is what we want to do.

So what is the inverse of 7 mod 12? So, we go about multiplying by all numbers modulo 12 to 7 and see when we get one. So 7 into 1 is seven. 7 into 2 is 14. That gives us two modulo 12. 7 into 3 is 21. 7 into 4 is 28. 7 into 5 is 35. 35 is minus one modulo 12. And therefore, so we have 7 into 5 equal to minus one modulo 12.

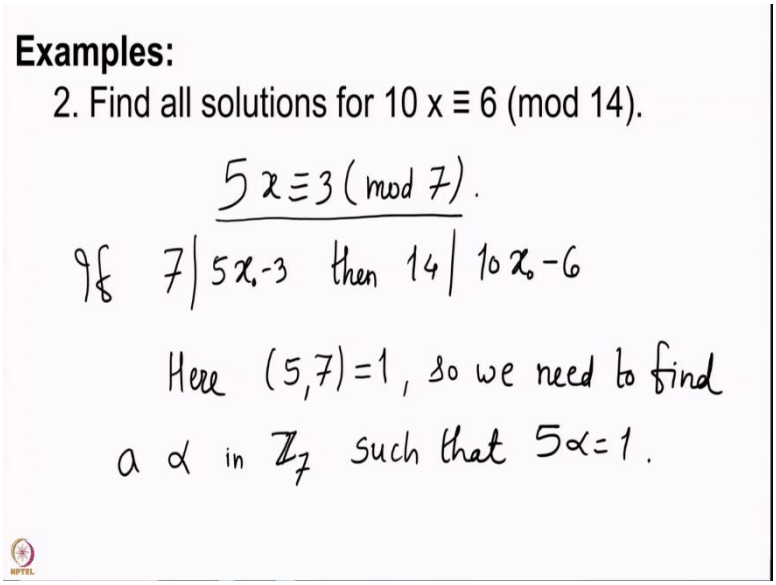
So, if I multiply both sides by minus one, I will get 7 into minus 5 equal to 1 modulo 12. So minus 5 is the multiplicative inverse of 7 modulo 12. What is minus 5 in 12? Minus 5 is same as 12 minus 5 which is again 7. So, 7 ka inverse is 7. Therefore, to find the solution for 7 x congruent to 3 e simply multiple both sides by 7.

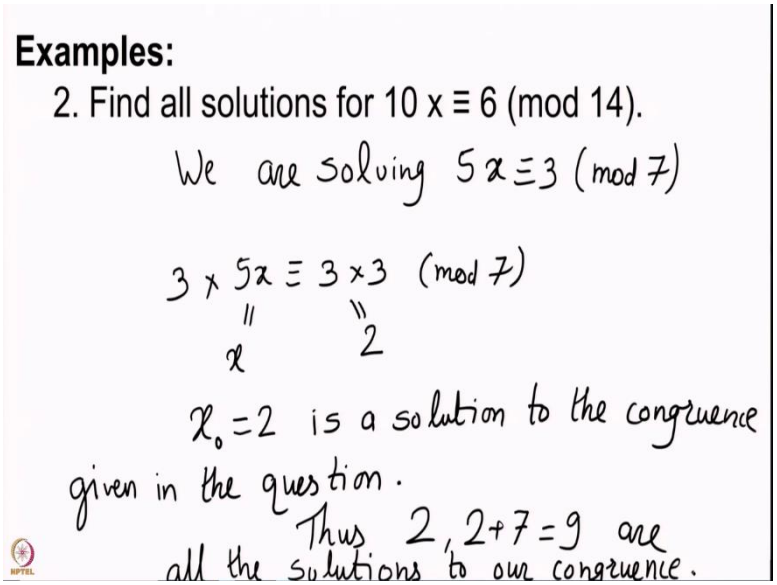
(Refer Slide Time: 17.34)



7 x congruent to 3 mod 12, then 7 into 7 x is congruent to 7 into 3 mod 12. This side is 21 or 9 modulo 12. And this side we simply get 49, which is simply x. So thus, x congruent to 9 mod 12 is the unique solution to the above congruence. You can simply check this by putting the value of x equal to 9 in the equation. So you have 9 into 7 which gives you 63. And 63 is indeed 60 Plus 3. 60 zero modulo 12 so you get 3 modulo 12. So this is how one would solve linear congruence's. Let us also see one more problem where we have multiple solutions when we do not have a unique solution.

(Refer Slide Time: 19.14)





So, the question now is to find all solutions to 10 x congruent to 6 mod 14. We are doing some other number than the 12 which has been our favourite number so far. So, first of all we check whether there is a solution at all. We first check there is a solution. And we know how to do this. D which is the GCD of 10 and 14. Now, it should be a simple matter to compute GCD's. This GCD is two and 2 divides 6.

So, we do have a solution, at least one solution. So since d is not one, we do not have a unique solution but d is two so we are going to get two distinct solutions. So, we are going to get two solutions modulo 14. Now there should be a nice algorithmto solve such equations. Such congruence relations. We will see whether there is such an algorithm but let us just try our hand and solve this problem.

What we want to do first of all is to solve for 10 x congruent to 6 mod 14 and we observe that it is enough to solve, it is enough to solve 5 x congruent to 3 mod 7. Why is this enough to solve? This is because if you had a x naught such that. So, if 7 divided 5 x naught minus 3 then 14 will divide 10 x naught minus 6.

We are just multiplying by two both the sides, so that would tell us that whenever you have the GCD, you can simply cancel out by the GCD throughout the equation, including the natural number by which you are going modulo. Including the n such that you are working in Z n, you can cancel d throughout the linear congruence. So, we want to now solve this.

Here, the GCD of 5 and 7 is one. So indeed, we should have a solution that was no surprise because we already know that there is a solution but what we do is, so we need to find a

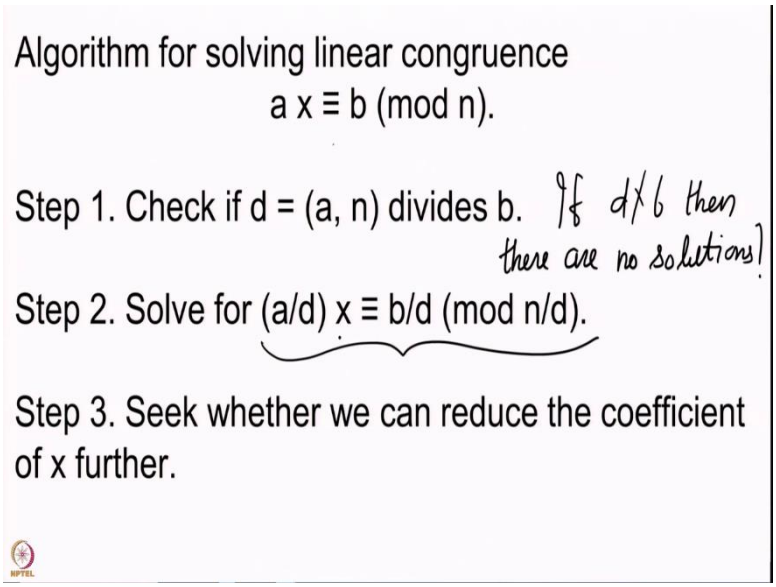
number alpha in Z 7 such that 5 into alpha is one. This is what we need to do. We need to be able to invert 5 and this is possible because we have that the GCD is one. So, 5 into 1 is 5. 5 into 2 is 10, which is not 1 modulo 7. 5 into 3 is 15 which is 1 mod 7.

So, alpha is 3. So we need to multiply by 3 to both the sides so we are solving 5 x congruent to 3 mod 7 and 5 x into 3 is congruent to 3 into 3 mod 7, 3 into 3 is 9 which is 2 modulo 7. 5 into 3 is 15. 15 x is x modulo 7, so we get that x is 2 mod 7. So x naught is equal to 2 is indeed a solution to the congruence given in the question.

. Because if you put 2 in 10 x you get 10 into 2 which is 20 and 20 is indeed congruent to 6 mod 14. So, 2 is the solution, what can be the other solution? So remember n is 14, d is 2 so n by d is 7. And therefore, 2 plus 7 which is 9 that is one more solution, because 10 into 9 is 90 and 90 is 84 plus 6. 84 is a multiple of 14. And therefore, 90 is also 6 modulo 14.

So thus, 2 and 2 plus 7 which is 9 are all the solutions to our congruence. So we have solved the problem, we found all possible solutions. There are only two because the GCD is equal to 2. And whenever the GCD is one, we convert from the GCD 2 case to the GCD 1 case and then we try to invert the coefficient of x. This is what we do. And, I told you that it would be nice to have an algorithm to solve these linear congruences. So indeed there is an algorithm which we have been following up to now.

(Refer Slide Time: 26.47)



The algorithm is as follows, what we do first of all is to check whether the GCD d of a and n divides b. This is the most important case. So, if this does not happen, if the GCD does not

divide b, then there are no s solutions. And then we are done. We will just say that there is no solution. However, if the GCD does divide n then what we do as we have done in the previous case, we solve for this, a by d, x congruent to b by d modulo n by d.

And so we need to prove a small lemma that whenever there is a solution for this, there is a solution for a x congruent to b and whenever there is a solution for that, we get a solution for this. We will need to prove equivalence of existence of solutions for these both congruences and the final thing which we wanted to do was to try and invert the coefficient of x which is a by d.

Now, what happens is that a by d is co-prime to n by d and therefore, we know that a by d into x congruent to 1 mod n by d should have a solution because the GCD is one which divides by 1, which means that we should be able to invert a by d. But to invert a by d is some sense equivalent to getting solutions. Indeed inverse of a by d modulo n by d is nothing but the solution to a by d into x congruent to 1 mod n by d.

So there should be a better way to do it. And what we then want to do is to reduce the magnitude of this a by d. We will try to make it smaller and smaller by using some other tricks and then ultimately we will solve this congruence relation. So, we will see some more of these methods in the next lecture and then we will go to what is called the simultaneous congruence, which is about the Chinese remainder theorem. See you, until then. Thank you!