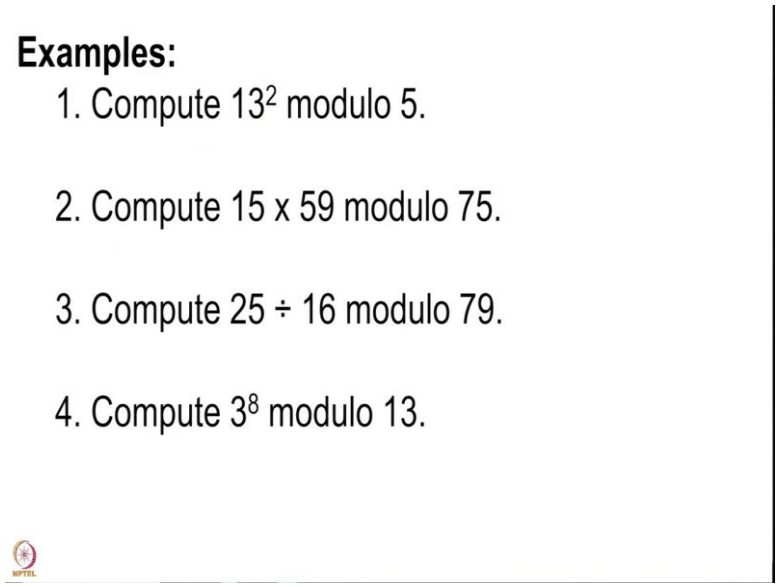
**A Basic Course in Number Theory**
**Professor Shripad Garge**
**Department of Mathematics,**
**Indian Institute of Technology, Bombay**
**Lecture no. 13**
**Solving linear polynomials modulo n – I**

Welcome back, we are discussing Congruence. This is an equivalence relation, modulo n, given a natural number 'n'. After seeing some basic properties of congruence classes, we did some very basic examples, computing products, divisions, takings powers, etcetera. Let me just remind you about that.

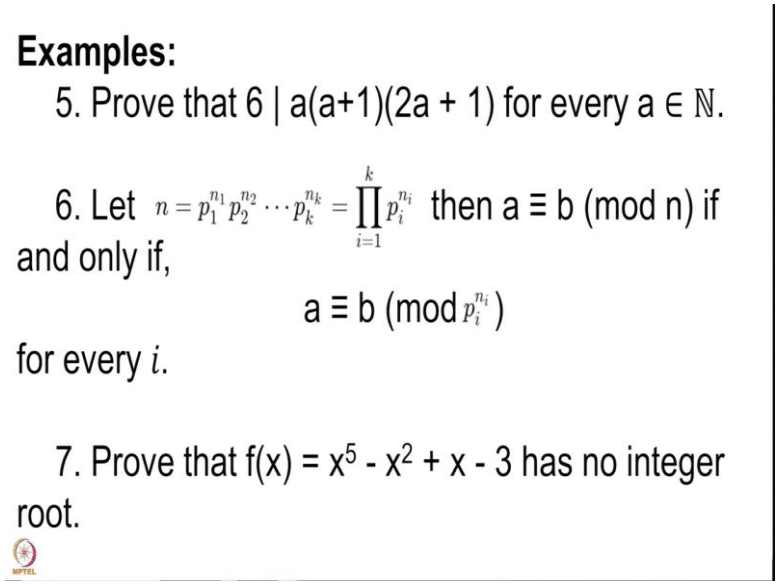
(Refer Slide Time: 0:46)




These four are the problems that we did in one of the previous lectures. 13 square modulo 5, 15 into 59 modulo 75, where if you recall we replaced 59 by negative of 16, and then 15 by 3 into 5. So that made our calculations quite easy. Then we computed 25 up on 16 modulo 79. And we observed that 16 into 5 is 80 that is 1.

Mod (75) 79, so 16 inverse modulo 79 is 5. And therefore 25 up on 16 is simply 25 into 5 modulo 79. And so that is how we did it. Then we computed 3 power 8 modulo 13, so we kept on taking various powers and saw what answer we received. These were some of the numerical problems then we also turned to some theoretical problems.

(Refer Slide Time: 1:55)




So the very first one was this one that is 6 divides a into a plus 1 into 2a plus 1, for every natural number a. We gave two proofs for this. We first considered every residue class modulo 6. There are six such classes and we verified that the product a into a plus 1 into 2a plus 1 for every such residue class, is 0. That would show that 6 divides the product a, a plus 1, 2a plus 1 for every a in n.

Later we also saw that 6 divides a number if and only if 2 divides the number and 3 divides the number. And so initially the five non-trivial classes because if a is 0 mod 6, then of course, 6 will divide the product a a plus 1 2a plus 1. That so we had to compute the values for five non-trivial residue classes modulo 6. This was reduced to computing it to three non-trivial classes, one non-trivial modulo 2, and two non-trivial modulo 3.

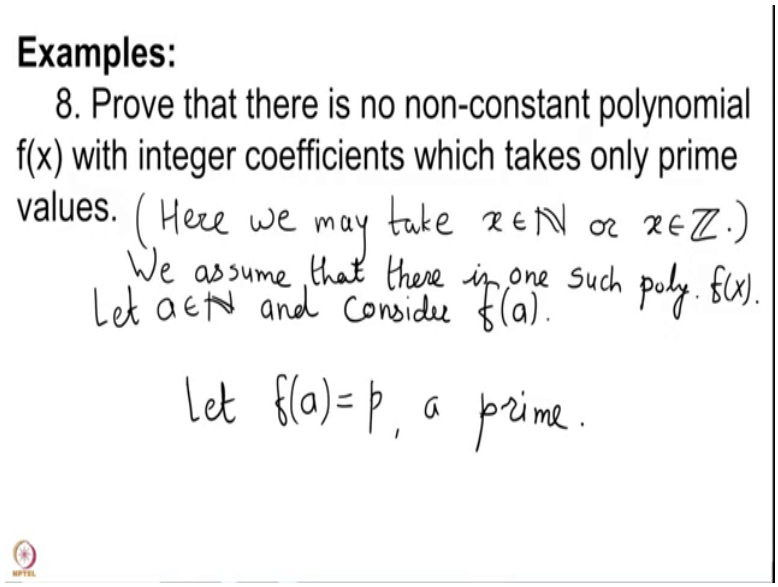
So just this basic observation that 6 divides a number if and only of 2 divides it and 3 divides it, made our computation very easy. So we went ahead with that and formulated a very general statement which is that if you have a prime factorization for n which is pi power ni, product pi power ni, then two numbers a and b are congruent modulo n if and only if a is congruent to b modulo pi power ni for every i.

That would then if you were, so the initial fifth problem was modulo 6, if it was say modulo 24, then it reduces to checking it modulo 8 and modulo 3, or if you had a problem modulo 120, it would reduce it reduce it to checking modulo 3, modulo 8 and modulo 5. So 120 would give you 190 non-trivial classes, whereas these together will give you a much smaller

number. This is how fundamental theorem of Arithmetic is very useful in doing several computations in number theory.

Finally we saw one application to show that this polynomial x to the 5 minus x square plus x minus 3 has no integer solution. We saw that if you go modulo n equal to 4, then there are indeed no solutions to this polynomial. And therefore there cannot be any solution in the set of natural numbers, or integers if you wish. So I will go one more small problem, and then we will develop some more theory or look at some more theoretical results. So this problem is as follows.

(Refer Slide Time: 4:53)



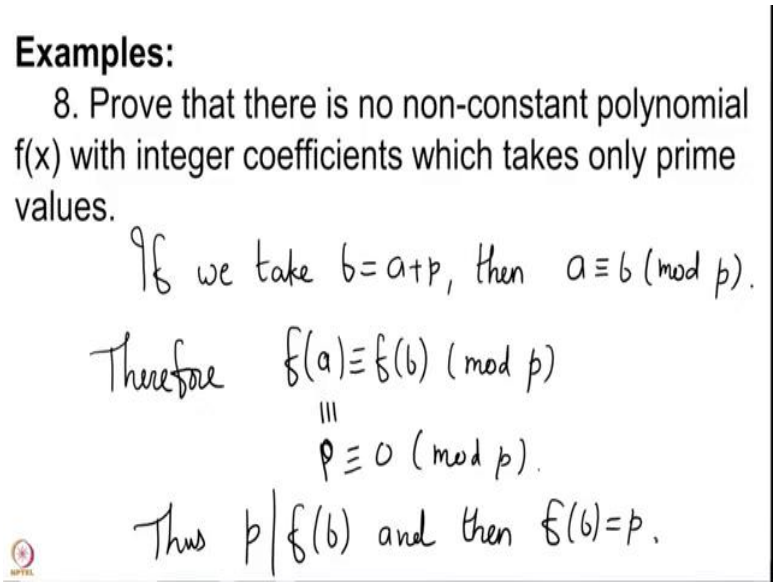

This is something that I have mentioned in when we were closing out the theme of primes and now we have techniques developed that we can use and prove this result, that if you have a non constant polynomial f of x whose coefficients are all integers, and if you say that this polynomial takes only prime values whenever you input a natural number then that is not possible, so the precise statement is that there is no non-constant polynomial fx with integer coefficients, which takes only prime values on natural numbers.

So here we may just add this statement that, we are talking about this on. Here we may take x in n or x in z. Both the possibilities will give us the solution. So how do we go about proving this? The proof is quite simple. I am not going to give you a minute this time to think about the proof. I will tell you the proof myself. So suppose you have take your favourite integer, take your favourite natural number, say 8.

So let a be a natural number and consider the function value at a. So the statement says we want to prove that there is no such non-constant polynomial so to begin with we assume that there is one, one such polynomial fx. This is our assumption. And then what we do is that we will start with the natural number n, consider the value fa and the assumption on f is that f of a is a prime.

So since, so let, f of a equal to p and we know that this is a prime. Now there is another thing that we have learnt, which is that when you take two natural numbers which are congruent modulo n, then any integer polynomial evaluated on those numbers will give you values which are also congruent to modulo n.

(Refer Slide Time: 8:06)

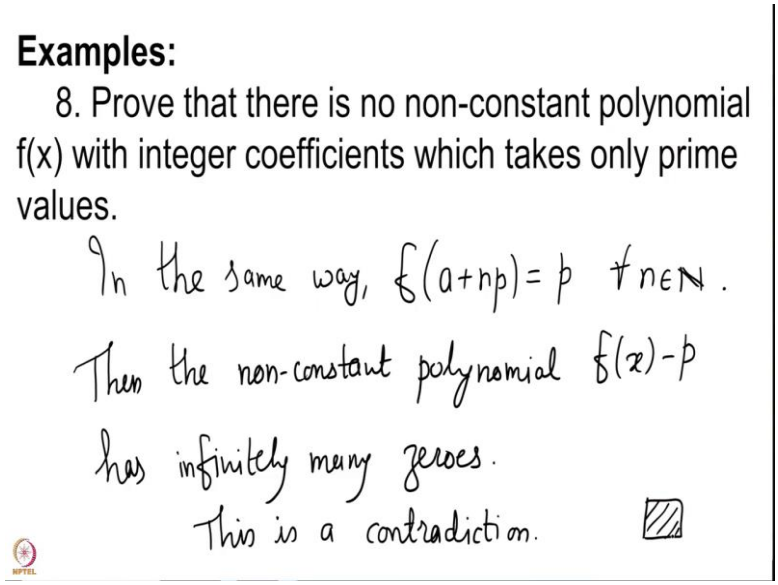



So, if we take b to be a plus p, then a is congruent to b modulo p, because the difference is divisible by p. So b is congruent to a mod p. And then what we get is that fa has to be congruent to fb mod p. But this is 0 mod p, because this is actually p, so since this is p, this is congruent to 0 mod p. And you can do this for every natural number which is congruent to a mod p. So we get, so thus p divides f of b, but f of b should also be a prime because a plus p is a natural number after all.

So f of b should also be a prime and here p divides it, p is a prime if f of b was not equal to p, then we would get a contradiction, because we would have the number fb which would have one fb as its two divisors, and then here we are getting one more divisor, in that case fb cannot be prime. So the only way that f of b can be a prime is that it b equal to p. So now if I

take any further integer so b plus p, b plus 2p, b plus 3p and so on all those values will be equal to p.

(Refer Slide Time: 10:10)




We repeat it by the same way so. In the same way, f of a plus n p is p for every natural number n. and what it tells us is that then the non-constant polynomial fx minus p has infinitely many zeroes. So we have that f of a is p, f of a plus p is p, f of a plus 2p is p, and so on, f of np is going to be b, and since the polynomial fx is non-constant, by subtracting p from that we will still get a non-constant polynomial.

If fx minus p becomes a constant polynomial then fx will be p plus that constant polynomial and therefore fx would be constant. So since fx is non-constant, fx minus p will remain non-constant and now we have infinitely many zeroes for such a polynomial. A polynomial of degree n can have at most n roots, at most n zeroes in complex numbers.

And since we are getting infinitely many zeroes here, this polynomial has to be a constant polynomial equal to zero. And that tells us that fx has to be equal to p, for all x, which says that f has to be a constant polynomial. So this contradiction proves the result, which completes the proof. So let me go through this proof again. What we did was simply we took any integer a, evaluated the polynomial at a.

That gave us a prime number because the non-constant polynomial should give us a prime, for every integer or for every natural number, whichever set you are working with. Once you get f of a equal to b then we will look at f of a plus p, call that b. Now this b is congruent to a,

modulo b, therefore, the function value the value of the polynomial f at a and a plus b will be congruent to each other modulo p.

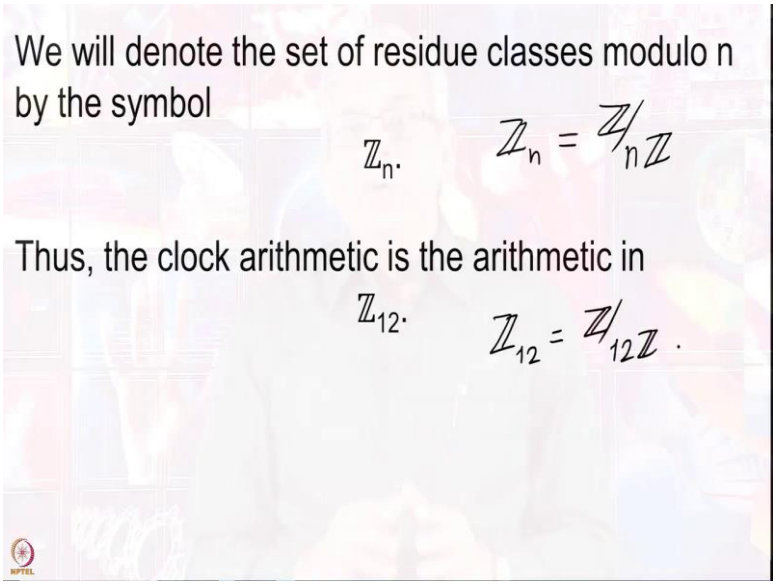
This is where we are using that the function, the polynomial has integer coefficients that is an important thing here, so p will divide f of a plus p, but f of a plus p, f of b that should also be a prime and if a prime divides another prime then both the primes better be equal otherwise we get some contradiction, so f of a plus p is p.

So f of 2p will be p, by the same method and so on, that gives us that there are infinitely many natural numbers of the form, f a plus np, such that the polynomial f evaluated at all these infinitely many values will give us the same constant p. And that is the contradiction, because the non-constant polynomial number one can have only finitely many zeroes and therefore, it can have only finitely many points where same value is taken there.

It cannot happen that a non-constant polynomial takes infinitely many, take one value at infinitely many points, because you can just subtract that value and get a contradiction. So, what we have done so far, after having defined the congruence and so on, have studied several possibilities for solutions modulo the congruence and we also proved that one polynomial does not have a root in integers, because we do not have roots for that modulo 4.

So the next question comes, when do we get roots? Modulo and integer n, or modulo a natural number n. But before we go on, we should begin, we should set up the notation so sometimes I may use this.

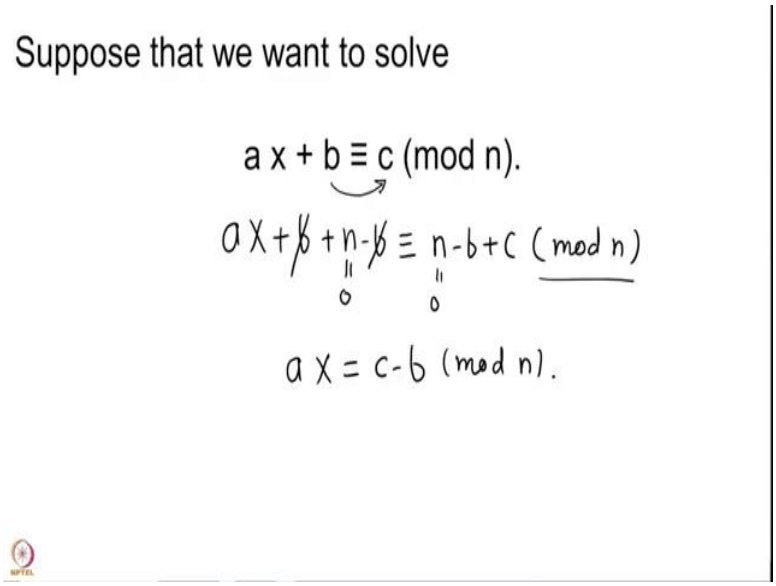
(Refer Slide Time: 15:07)



We have been working with this arithmetic of residue classes modulo n and the residue classes modulo n will be denoted the set of all of these, will be denoted by z, which stands for integers subscript n. So I will just call it zn, if you know a little bit more about algebra, maybe the group theory or the ring theory, and so on.

Then you will immediately notice that this zn is nothing but the quotient of z modulo n z, whether you are looking at it from group theoretic point of view or ring theoretic point of view, it is all the same. So now we go towards finding conditions which will guarantee that there are solutions to congruency equations. Before, we go to higher degree let us first look at degree one.

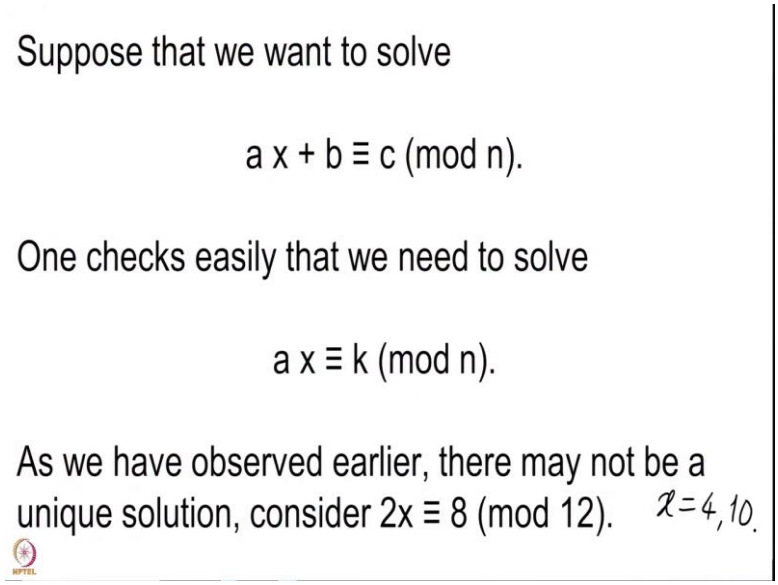
(Refer Slide Time: 16:11)




So suppose we want to solve the congruence relation, the congruence equation, of the type ax plus b is equal to c modulo n. So we are working in zn and we want to solve ax plus b equal to c. In that set, in the set of residue classes modulo n. Now here the b can be put on the other side. You can add n minus b to both sides, and that will tell you that ax plus b plus n minus b, this is going to be congruent to n minus b plus c modulo n.

So these b gets cancelled because you are allowed to do the addition and subtraction, and the n is anyway zero because you are going modulo n, this n is also zero modulo n, so we get ax equal to c minus b mod n. What we have done simply is that, we have moved this b to the other side with a negative sign that is all that we have done. So this says that we need to be able to solve the linear congruence ax plus b congruent to c mod n, that b is really superfluous.

(Refer Slide Time: 17:41)

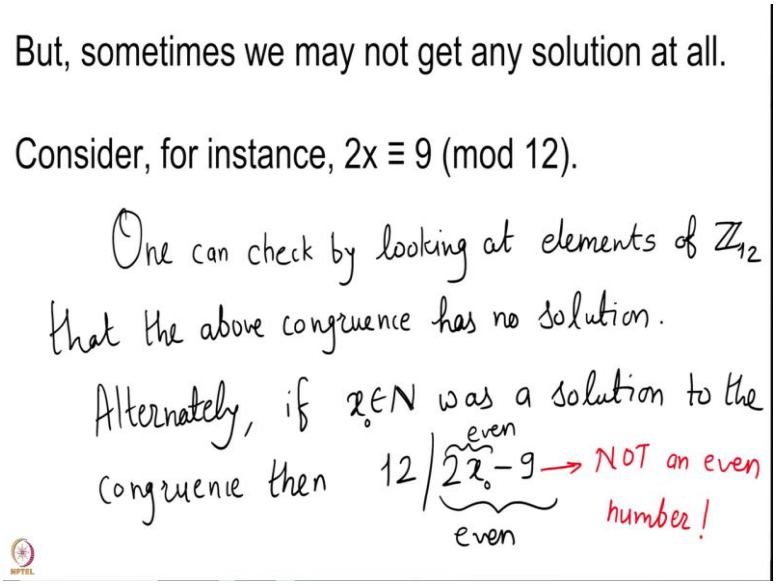



You can solve for ax equal to k modulo n. It is enough to solve for this. So we will take various possibilities of k, various possibilities of a, having fixed an n. And we want to know when we can have a solution, when we can have a solution to this linear congruence, when there can be a root to the polynomial ax minus k, or when there is a solution to x equal to k modulo n, this is what we want to do.

Now there are two problem as we have seen earlier that first of all there need not be a unique solution. This is something that we have seen earlier already in the clock arithmetic, we have seen. So there may not be a unique solution, you may have multiple solutions. For instance 2x congruent to 8 modulo 12.

So if you remember x equal to 4, and x equal to 10 these were the two solutions that we obtained. So this is one type of a problem that we may not get a unique solution. But at least we have a solution there may be another type of a problem that you may not get even the solution.

(Refer Slide Time: 19:14)




Sometimes we may not get any solutions at all. How can this happen so, let me give you an example. So consider for an instance this 2x congruent to 9 modulo 12, so what do we want to have here. We want to have is of, you can of course check. One can check by looking at elements of z12 that the above congruence has no solution. This is of course something that you can do, of course you have to just multiply by 2.

There are twelve possibilities; there are 12 elements inside 12. So you simply compute 2 into x for each of them and check whether you are getting 9 as the answer. But there is another simpler method, which is as follows. If x in n was a solution to the congruence then 12 divides 2x minus 9. So this number has to be even, because it is a multiple of 12.

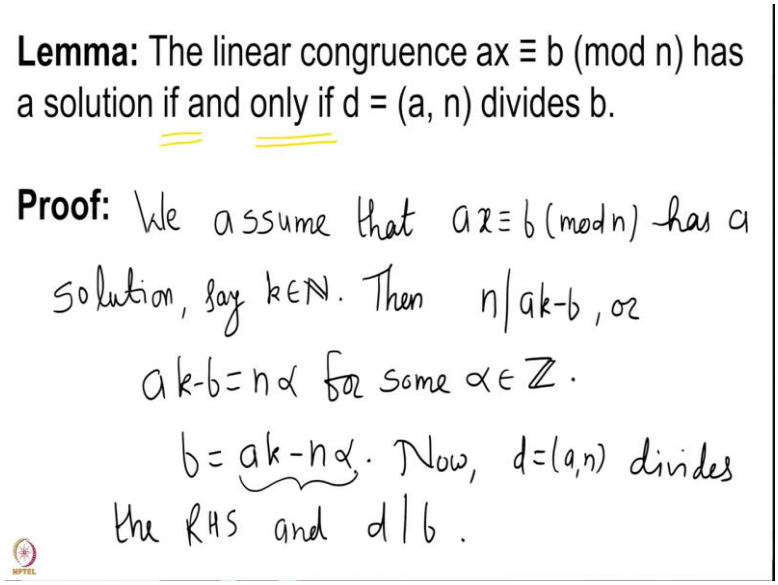
2x minus 9 is the solution, you know if you are getting confused with the x, being taken to be the same elements. Let us take it to be x naught, so 2x naught minus 9 is an even number because it is divisible by 12 and 2x naught is of course even, which gives you a contradiction because 9 is not an even number at all.

So this is a simpler solution and this works without having to do all those 12 computations that we would have needed to do otherwise. So what is going wrong here, the thing that is going wrong here is that there is a common divisor of 2 and 12, which is 2, and this divisor should divide 9, the problem is that 2 does not divide 9.

9 is an odd number, so because 2 does not divide 9 we are not getting a solution, so when we are looking at the common divisor of two numbers dividing yet another what we are really

looking at is the GCD. So we can formulate the condition and prove it, which will guarantee exactly when we are going to have a solution to the linear congruence. So that comes in the next slide.

(Refer Slide Time: 22:54)




So here is the Lemma, the linear congruence ax congruent to b mod n, has a solution if and only if d which is the GCD of a and n divides b. So once again let me remind you that here we have two parts, the part one is if and the part two is only if. So what we would be proving is that if d which is the GCD of a, n divides b then we get a solution for the linear congruence, this is something that we will prove.

And we will also prove that if there is a solution then d should divide b. This is the part which says only if. So you get a solution only if d divides b. Otherwise you would not get a solution. If d does not divide b, then you would not get a solution. If d divides b, then you get a solution, so these both the directions need to be proved. So we will begin with the only if condition and we will try to prove this.

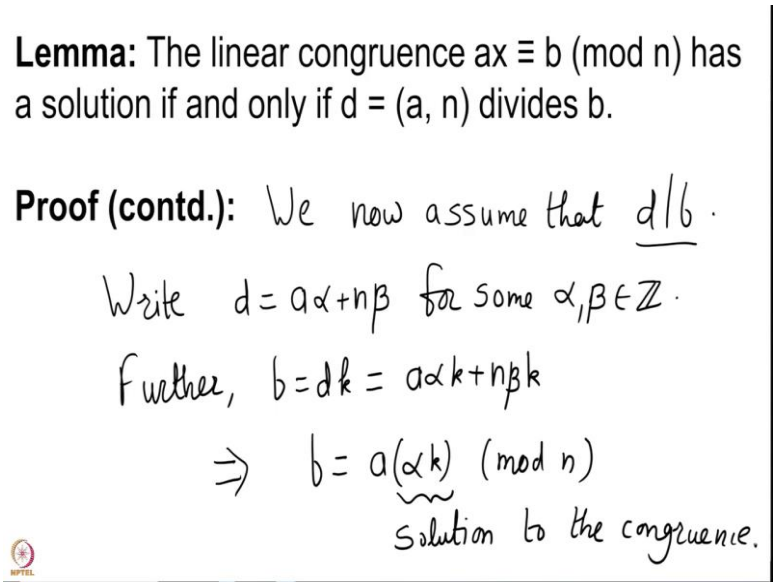
So we assume that ax congruent to b mod n has a solution, say k, in the natural numbers. So we assume that there is a solution to the congruence ax congruent to b mod n, then what we get is that n divides ak minus b or ak minus b is n into alpha for some alpha in z. So we have that ak minus b is a multiple of n.

And we can rearrange these terms to get b to b minus b will be ak minus n alpha, we will put be to the n alpha side to make it plus and then, n alpha (com) comes to this to become

negative. So b is ak minus n alpha. Now, d which is the GCD of a and n divides the LHS and hence it should also divide the RHS. That completes our proof.

We assume that there is a solution say k, then we can write b as nk minus n alpha for some alpha coming from integers, and now d being the GCD of a and n, should divide the RHS and not the LHS sorry. The right hand side, this is where d divides and then d should divide b. This was quite simple, we now go to prove the other side that we assume that d divides b and we want to get a solution to ax congruent to b modulo n.

(Refer Slide Time: 27:06)




So d remember is the GCD of a and n, and we also know that this GCD can be written as a alpha and n beta, for some alpha beta coming from integers. Further d divides b, so b is d into k and therefore, this is a alpha k, plus n beta k, because d is a alpha plus n beta, we have that d into k which is b is a alpha k plus n beta k, which implies that b is a times alpha k modulo n, so we got a solution to the congruence.

Of course, this may not be natural number, if you really want a natural number you can keep adding multiples of n, to this and you will get. So alpha k plus a suitable high enough multiple of n will give you a natural number and then a into alpha k plus a into that high enough multiple of n will be same as d modulo n, and then you will have a solution in the set of natural numbers we will see more of this in the next lecture so see you until then, thank you.