Discrete Mathematics

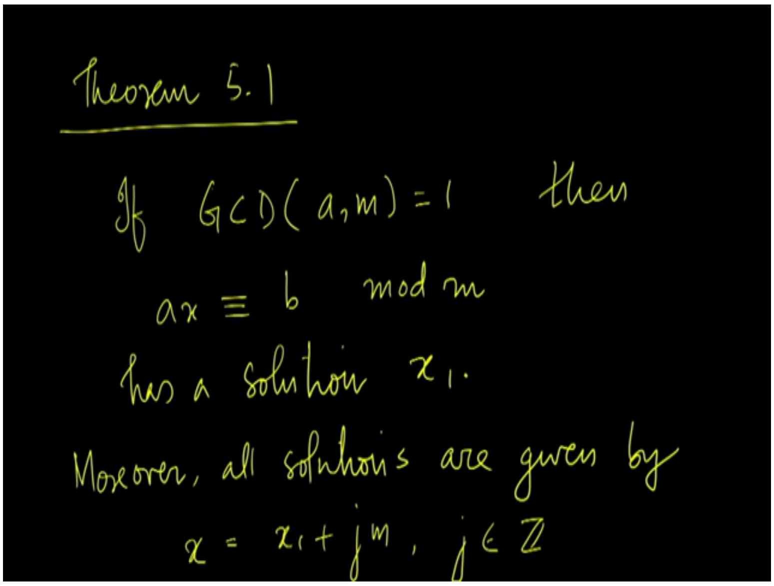
Professor. Sajith Gopalan
Department of Computer Science and Engineering,
Indian Institute of Technology, Guwahati.

Lecture 34

Solution of Congruences

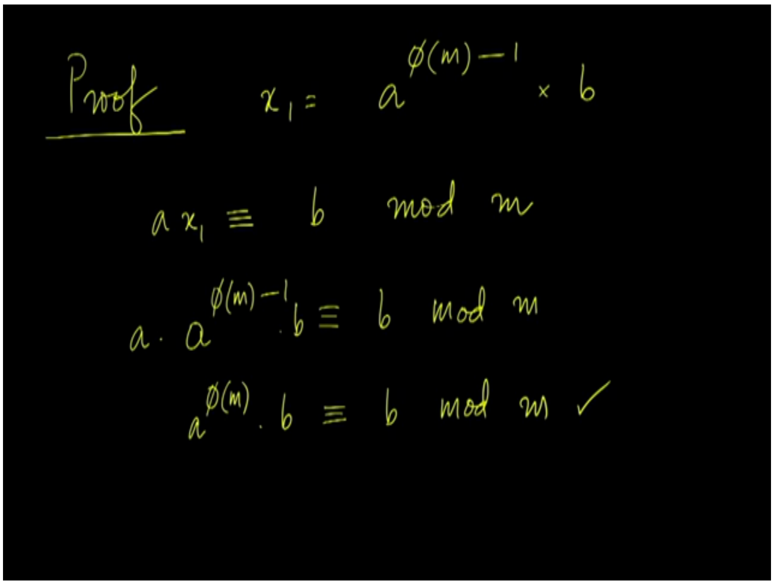
Welcome to the NPTEL mock on discrete mathematics this is the fifth lecture on number theory.

(Refer Slide Time: 00:40)



So let us begin with the theorem this is called theorem 5.1 let a say GCD of a and m is 1 then the congruence ax equals b mod m. has a solution x 1 more over all solutions are given by x equals x1 plus jm where, j is an integer. In other words, there is a solution x1 and every other solution is congruent do x1 modulo m. So that is what the theorem states.

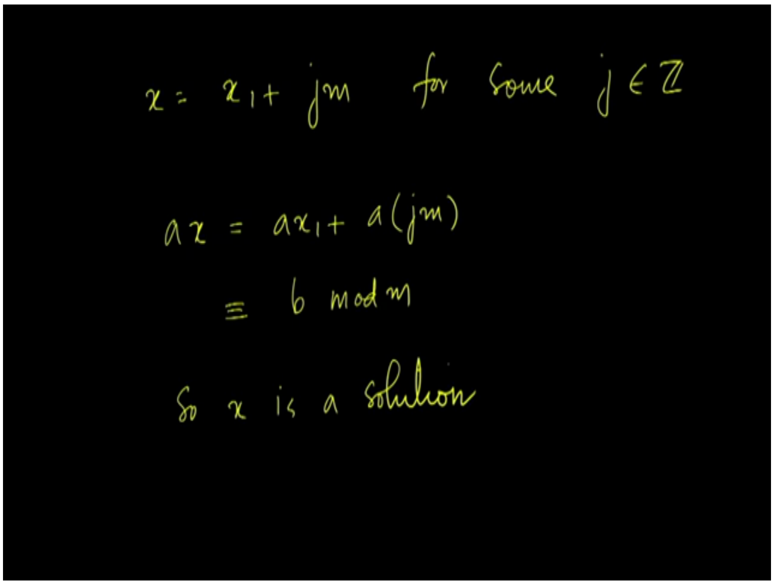
(Refer Slide Time: 01:51)



So let us proof the theorem, the theorem follows from the generalization of Fermats theorem let us say x1 is a power phi of m minus 1 times b where, phi of m is the totient of m then plugin x1 into the congruence we have the congruence says a x1 is b mod m, then we have a times a power phi of m minus 1, is congruent to this times b is congruence to b mod m if x1 is indeed a solution so let us check.

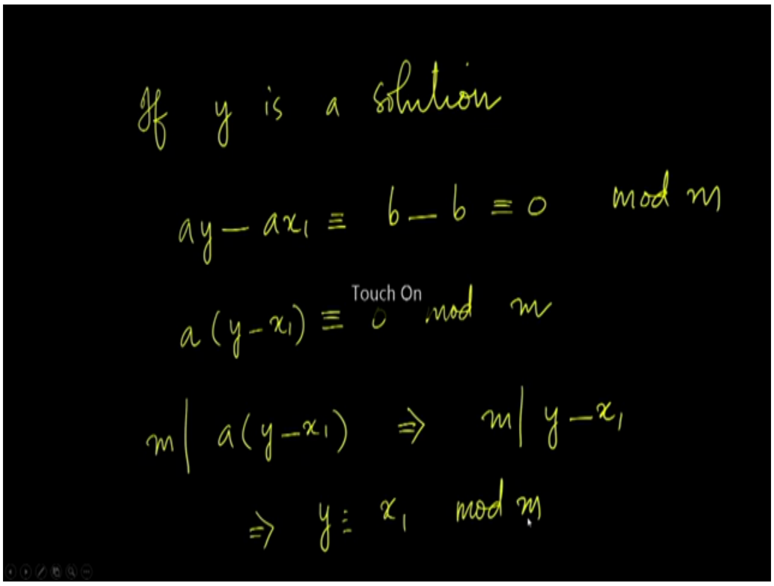
We find that a power phi of m times b is indeed a solution because by the generalization of Fermats theorem a power phi of m is 1 mod m so 1 into b is indeed b mod m. So the congruence is satisfied so if you plugin x1 as a power phi of m times b1 the congruence holds good, so x1 is indeed a solution of the congruence.

(Refer Slide Time: 03:26)



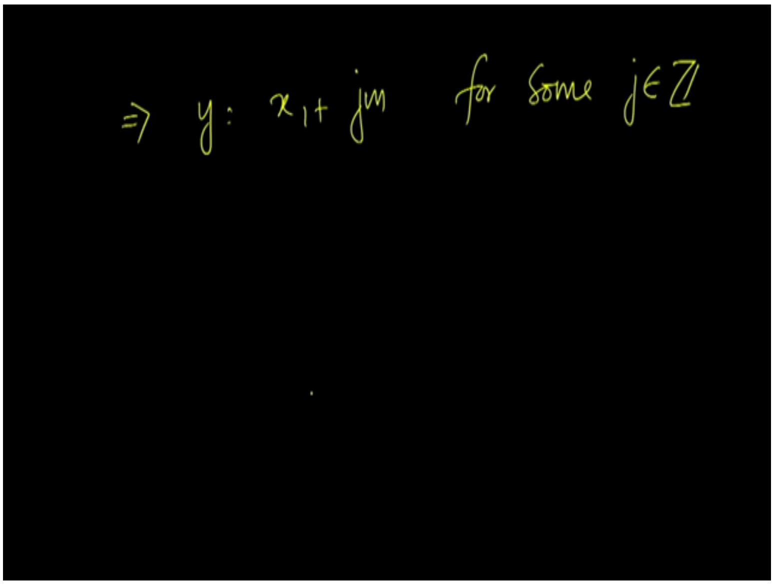
Let x equal to x1 plus j into m for some j which is an integer, plugin this x in we find that ax is equals ax1 plus a into jm this is congruent to b mod m so x is also a solution. So all numbers that are congruent to x1 modulo m of solutions. But, are this the only solutions,

(Refer Slide Time: 4:21)



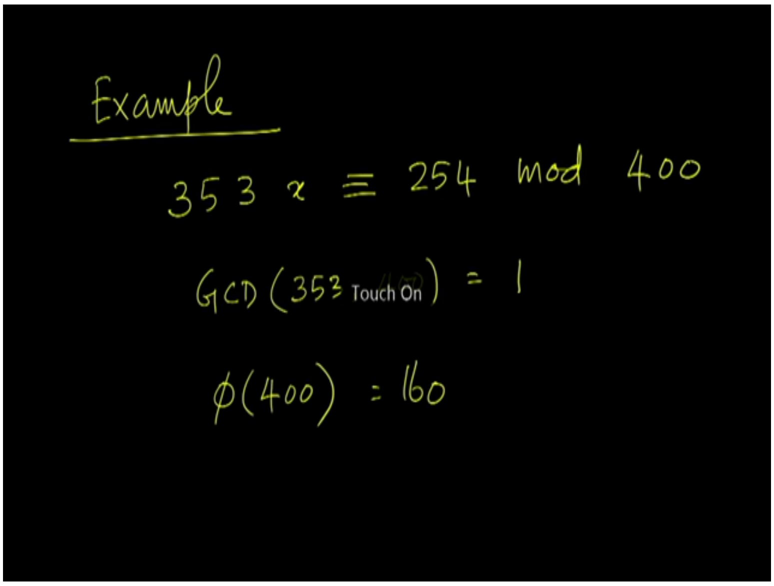
Suppose y is some solution if y is a solution, then ay minus ax1 is congruent to b minus b which is congruent to 0 mod m. Y is a solution, so ay is congruent to b mod m x1 is a solution, so ax1 is b mod m therefore, when you subtract we have a times y minus x1 is 0 mod m. or in other words m divides a times y minus x1 but, since, a and m are relatively prime they do not have a common factor therefore it must be that m divides y minus x1 which means y is congruent to x1 modulo m.

(Refer Slide Time: 05:26)



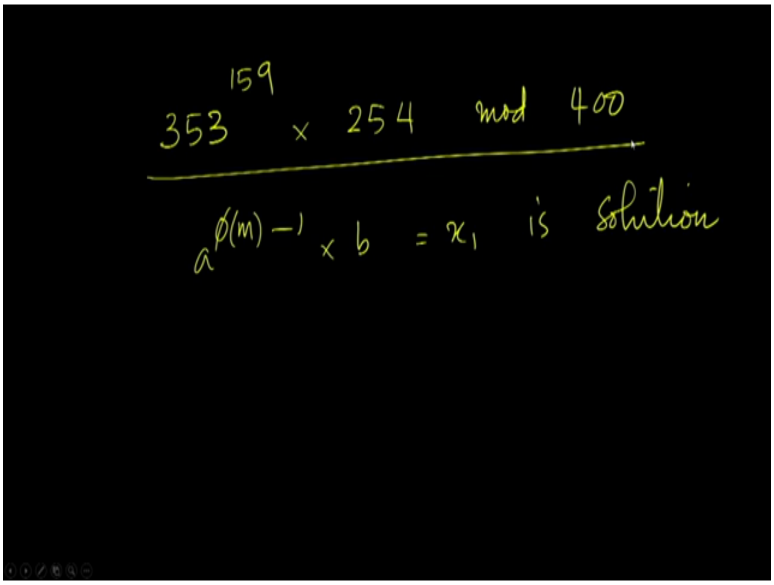
Or in other words y is equal to x1 plus jm for some j which is an integer, therefore we know that every solution of the congruence is congruent to x1 modulo m and these are the only solutions. So let us consider one example.

(Refer Slide Time: 05:48)



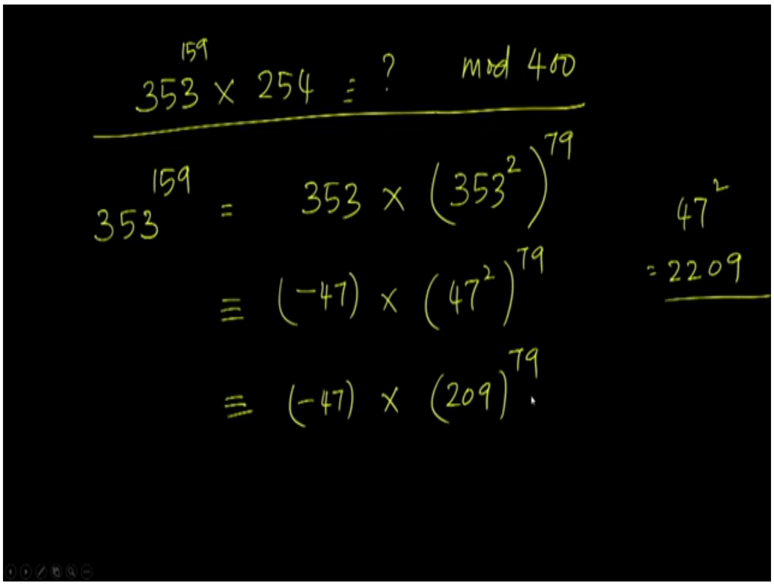
Let us say this is what we want to solve, 353 x is 254 mod 400, 353 is a prime so GCD of 353 400 is 1, and we also know that phi of 400 is 160. We will see a close form expression for phi later on, so from that we will be able to calculate phi but a manual verification will in any case show that phi of 400 is 160.

(Refer Slide Time: 06:42)



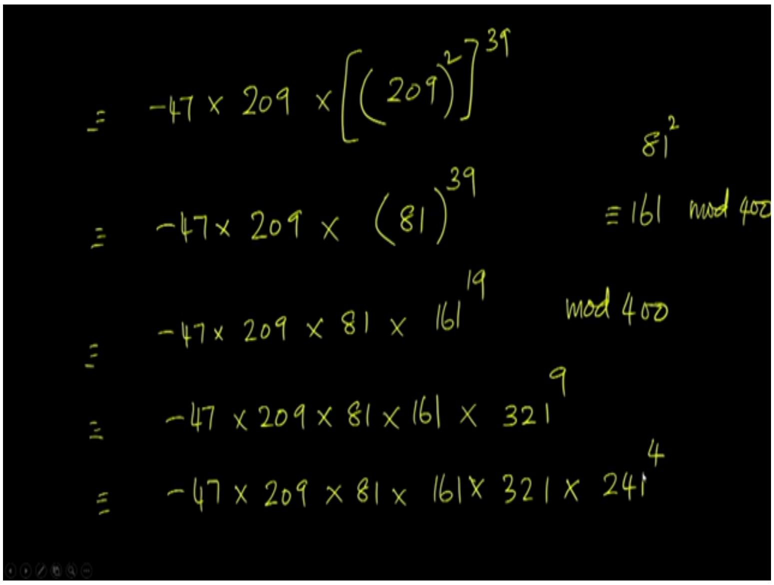
So 353 power 159 whereas phi of 400 minus 1 into 254 as the clearance shows a power phi of m minus 1 times b equal to x1is a solution. therefore, this would be a solution but how much would this b.

(Refer Slide Time: 07:20)



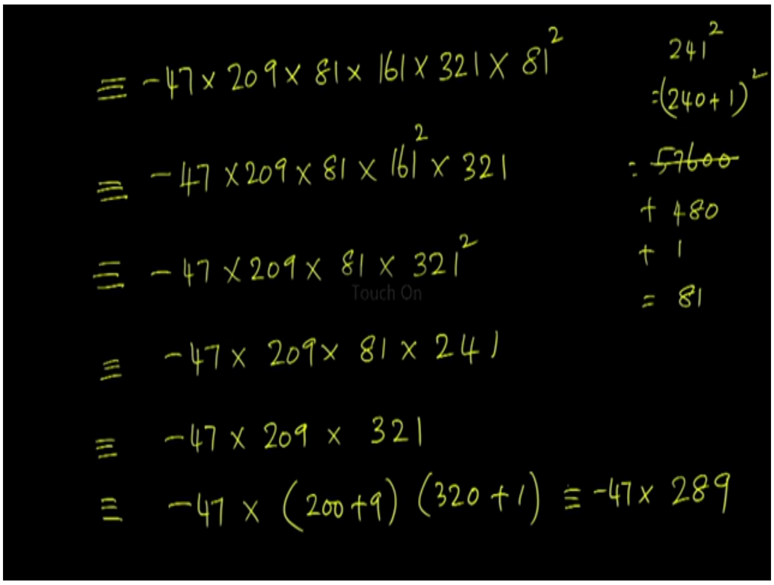
350 power 159 times 254 is what we have to calculate, of course mod 400. First let us calculate 353 power 159 this can be written as 353 times 353 square power 79, but this, mod 400 can be written as minus 47 into 47 square power 79 but, 47 square as you can verify is 2209 therefore, 47 squared is 209 mod 400 so modulo of 400 you can write this as 209 the whole power 79.

(Refer Slide Time: 08:35)



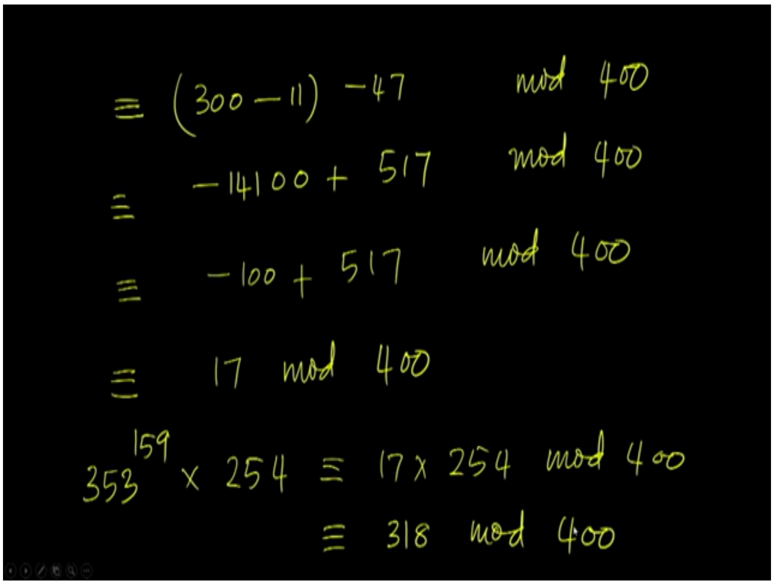
Which is minus 49 into 209 into 209 square the whole power 39, but then 209 square is 81 mod 400 therefore this is writable in this form but, 81 square is 161 mod 400. 80 squared is 0 mod 400 2 into 80 into 1 is 160, plus 1 is 161. So the equation becomes this, 161 power 19 is what we need to find, all mod 400. So this were all congruences, which can be further written as take 161 out then we have 161 power 18 which is 321 power 9 because 161 square is 321 mod 400. And then we have 321 power 8 since, 321 squared is 241 mod 400 we can write this as 241 power 4.

(Refer Slide Time: 10:45)



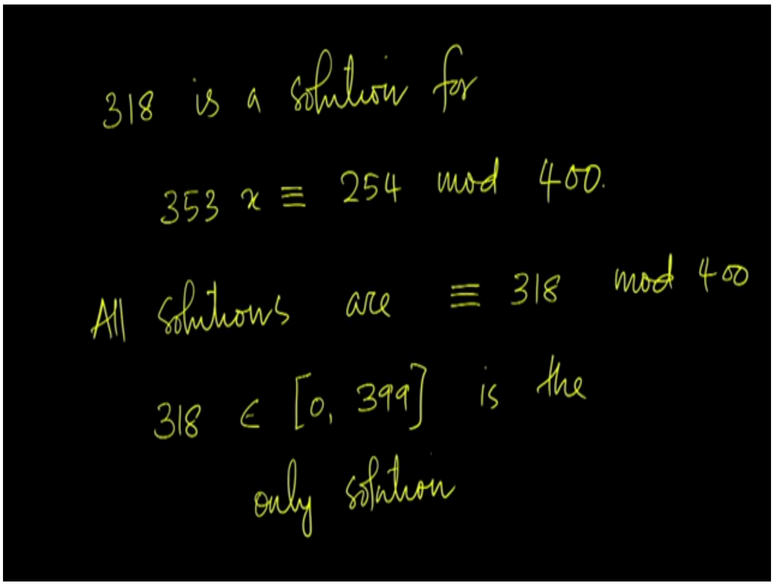
But, 241 we find this, which is of course 0 mod 400 so we need not consider it so we have 480 plus 1, which is 81 again, so this is 81 squared we have already seen this, 161 since, 81 squared is congruent to 161 this is congruent to this expression but we have already seen that 161 squared is congruent to 321 and we know that 321 squared is congruent to 241 and (()) (12:16) 241 into 81 240 into 80 is 0 mod 400 so we need not count that so this is 321 once again. Which can be written as 200 plus 9 into 320 plus 1 which is minus 47 into 200 plus 320 is a multiple of 400 therefore that does not feature in the answer and 9 into 1 is 9 so we have 9 into 320 plus 200 which comes to 289. So the expression now reduces to minus 47 into 289.

(Refer Slide Time: 13:13)



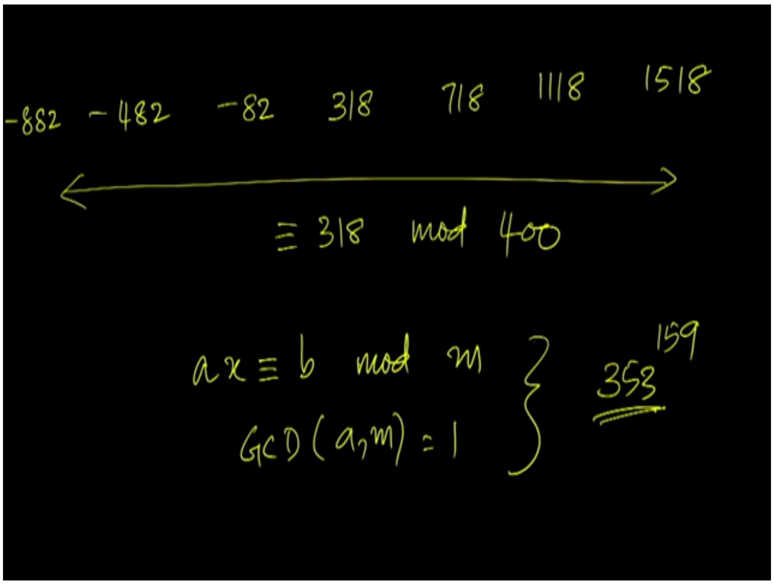
289 is 300 minus 11 that into minus 47 is minus 14100 plus 517, 11 into 47 is 517 300 into 47 is 14100, but 14100 is minus 100 modulo 400 all this is modulo 400 so we have but, 517 is 117 mod 400 so this is 17 mod 400. Which is 353 power 159 but, what we need to find is 17 into 254 so thus, 353 power 159 into 254 is 17 into 254 mod 400 which you can verify is 318 mod 400.

(Refer Slide Time: 14:39)



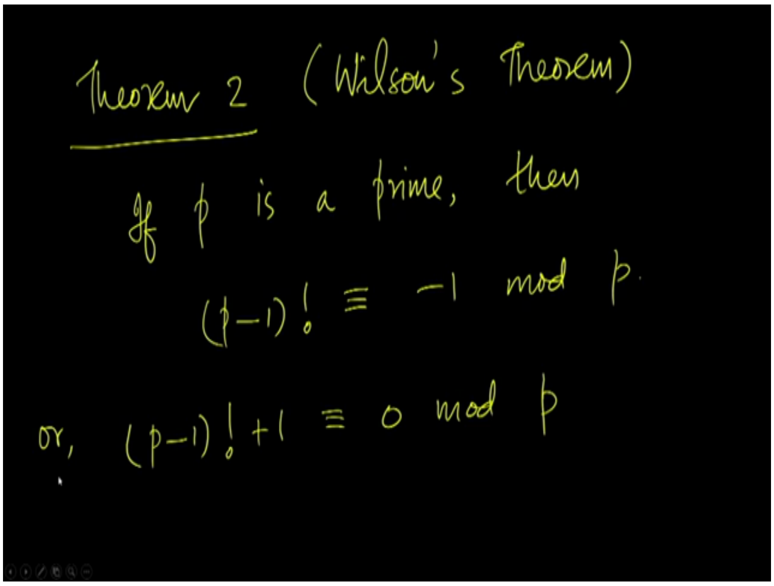
So 318 is a solution for 353 x is 254 mod 400, and we know that all solutions to this congruent are congruent to 318 mod 400, in other words 318 intersect 0 to 399 is the only solution, in the integral 0 to 399 318 is the only solution.

(Refer Slide Time: 15:30)



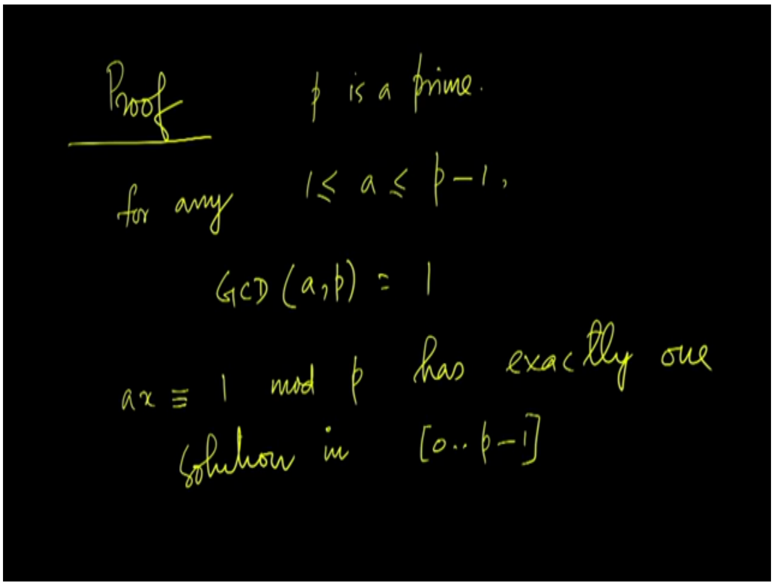
The other solutions are obtained by moving forward and backward at modulo m. So 718 1118 1518 are all solutions moving backwards 318 minus 400 would be minus 80 to minus 480 to minus 882 these are also solutions. So there is an infinite numbers solution but all solutions are congruent to 318 modulo 400. So this is one way of finding solutions for congruences of the form ax is congruent to b mod m, with GCD of am equal to 1, but it involves finding exponents of this form which is a long interious process so this is not exactly practical.

(Refer Slide Time: 16:40)



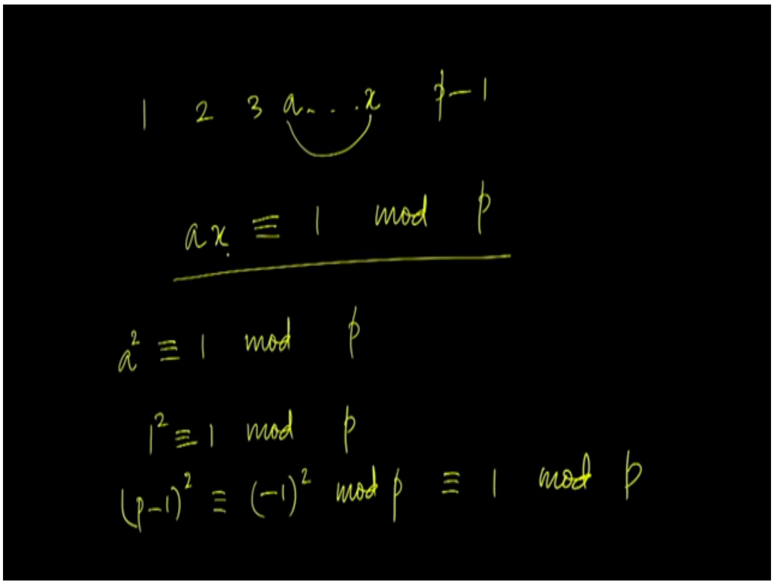
We will see an easier method later on the lecture now, let us see another theorem which is called Wilsons theorem what Wilsons theorem asserts is this p is a prime then p minus 1 factorial is minus 1 mod p or in other words p minus 1 factorial plus 1 is divisible by p. so let us proof this theorem.

(Refer Slide Time: 17:30)



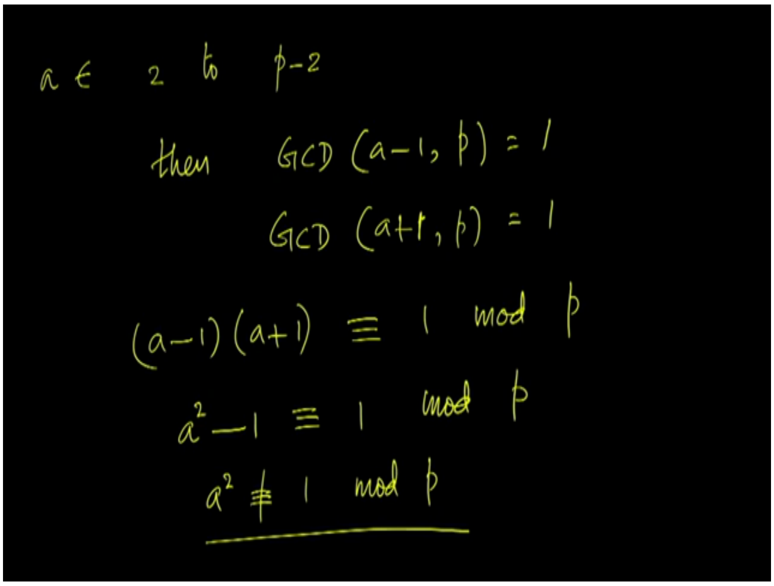
The proof goes like this for any a with a varying from 1 to p minus 1 where p is a prime we assume that p is a prime, then for any a in the range 1 to p minus 1 GCD of a, p equal to 1, a and p do not have any common factor, a prime does not have a common factor with any non-negative integer any positive integer less than that. So ax equals 1 mod p has exactly one solution in the interval 0 to p minus 1 this is what we have seen in theorem 1, ax equals 1 mod p has exactly one solution here we have taken b as 1 and m as p.

(Refer Slide Time: 18:49)



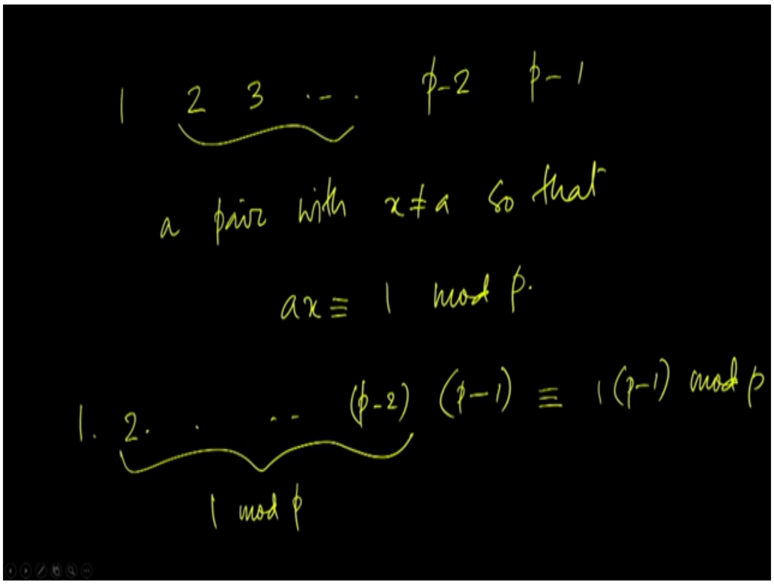
So if you consider the integers 1 to p minus 1 in this sequence we have a and the solution x of ax equals to 1 mod p. So we can think of a and x is being paired of we want to consider a and x so that ax equal to 1 mod p, but then could a and x be the same if a and x are the same we have a squared equals to 1 mod p there are two a’s which satisfy this for example 1 squared is 1 mod p, p minus 1 the whole square is minus 1 to whole square mod p which is 1 mod p. So in this we find that 1 and p minus 1 pair with themselves there is 1 into 1 is 1 mod p now a day's p minus 1 into p minus 1 is 1 mod p.

(Refer Slide Time: 20:01)



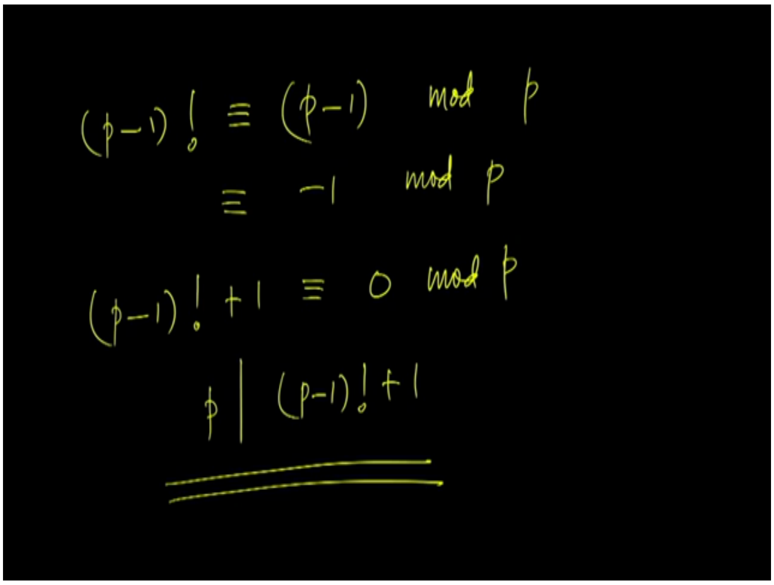
But what about the remaining if you consider the numbers in the range 2 to p minus 2 if a is in this range 2 to p minus 2 then we know that GCD of a minus 1 p is 1, p is a prime similarly, GCD of a plus 1 and p is also 1. A plus 1 can be at most p minus 1, therefore a minus 1 and a plus 1 are both relatively prime to p a minus 1 and a plus 1 therefore must be congruent to 1 mod p which means a squared minus 1 is 1 mod p or a squared is not congruent to 1 mod p, therefore no a within the range 2 to p minus 2 we will have this property a squared will not be 1 mod p and here we were seeking all the a’s so that a squared is 1 mod p we found that 1 squared is 1 mod p and p minus 1 the whole squared also 1 mod p so 1 and p minus 1 do pair with themselves.

(Refer Slide Time: 21:48)



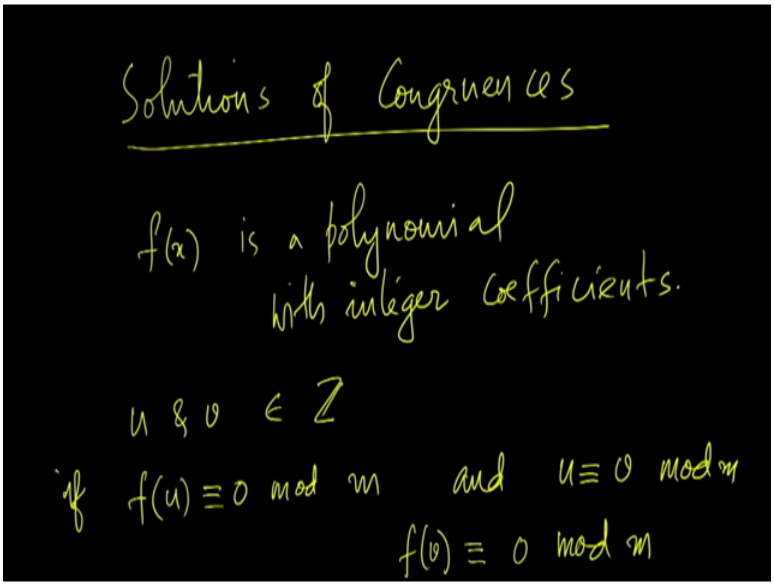
But, then if you consider the other numbers in the range 2 to p minus 2 we find that this do not pair with themselves so there they pair with some other so any a here will pair with x not equal to a so that ax equal to 1 mod p. Now let us consider this product p minus 1 factorial, consider the integers in the range 2 to p minus 2 we know that all of them pair with each other for every a in this range there is an x within this range that is not equal to a so that ax equal to 1 mod p, therefore the product of all these together is 1 mod p therefore this entire product which is p minus 1 factorial can be written as 1 into p minus 1 mod p.

(Refer Slide Time: 23:06)



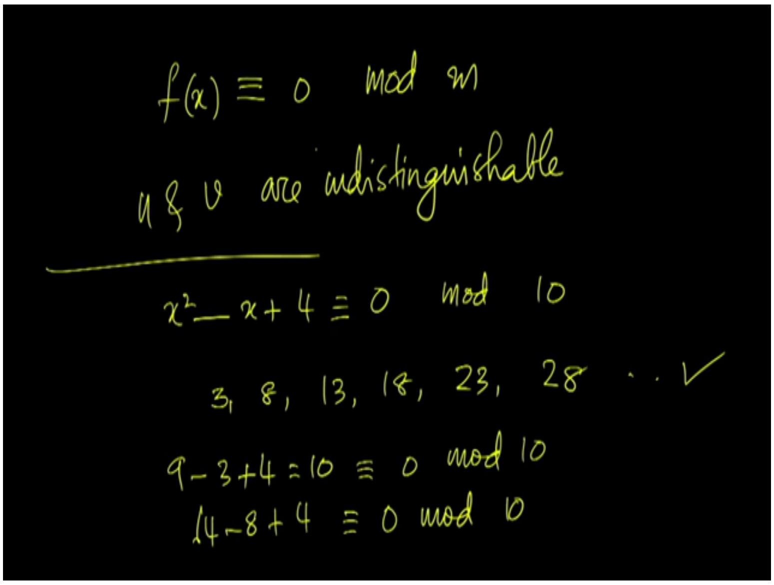
Or in other words p minus 1 factorial, is p minus 1 mod p but p minus 1 is minus 1 mod p moving minus 1 to this side, we have p minus 1 factorial plus 1 is 0 mod p or p divides p minus 1 factorial plus 1 which is what the theorem asserts Wilsons theorem asserts that p minus 1 factorial is minus 1 mod p.

(Refer Slide Time: 23:53)



Now, let us talk about solutions of congruences, suppose f of x is a polynomial with integer coefficients let a say u and v are integers if f of u is congruent to 0 mod m and u is congruent to v mod m you can readily verify that f of v is congruent to 0 mod m.

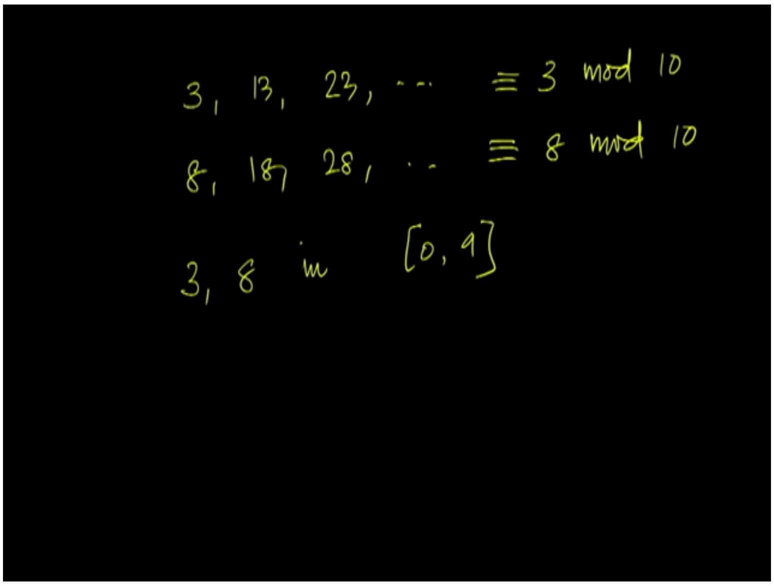
(Refer Slide Time: 24:56)



Therefore, when we talk about solutions of the congruence f of x congruent is 0 mod m we assume that u and v are undistinguishable they are congruent to each other mod m so we essentially assume that they are same solutions so we do not count them as separate solutions modulo m. For example, consider x squared minus x plus 4 equal to 0, its solutions are this is congruent to 0 mod let us say 10 it's solutions are 3, 8, 13, 18, 23, 28, etc.

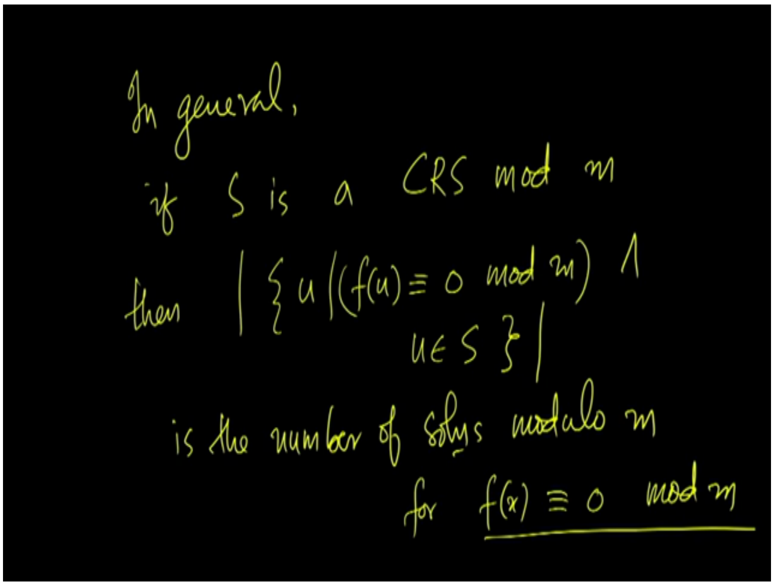
For example, substituting 3 in this we have 9 minus 3 plus 4 which is 10 this is 0 mod 10, substituting 8 here we have 64 minus 8 plus 4 which is 60 which is again 0 mod 10 so, these are all solutions. And you can also verify that if x is a solution then x plus 10 is also a solution.

(Refer Slide Time: 26:23)



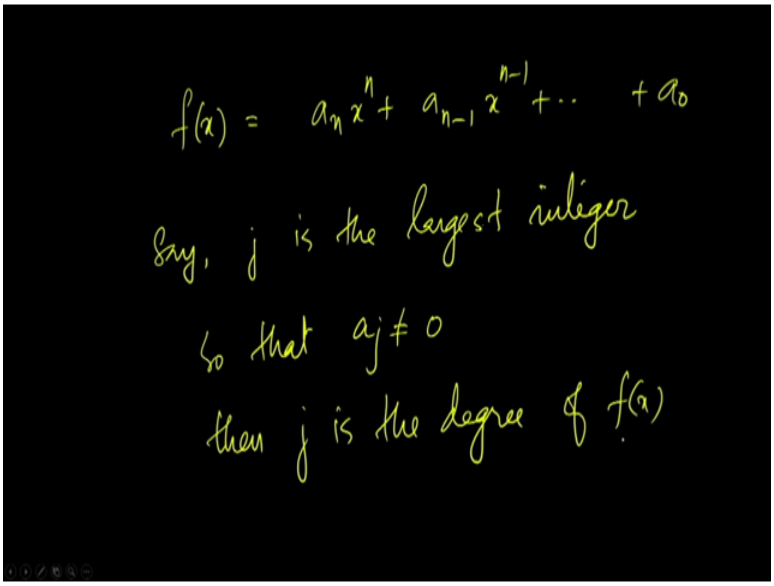
But then, 3, 13, 23, these are all congruent to 3 mod 10, similarly 8, 18, 28, these are all congruent to 8 mod 10. Therefore, we do not consider them distinct solutions we say that we have only two solutions in 0 to 9 that is we have only two solutions modulo 10 for this congruent.

(Refer Slide Time: 26:56)



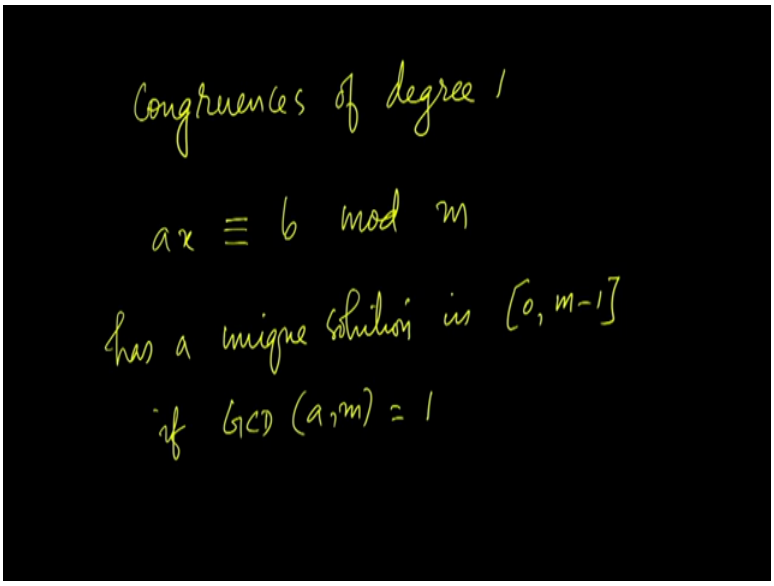
In general, is s is a complete residue system modulo m, then every u such that f of u is congruent to 3 mod m, and u belongs to s such u are what we consider solutions so the size of this set is the number of solutions, modulo m for f of x equal to congruent to 0 modulo m so we say that this congruent has these many solutions so within the CRS we consider all u that satisfy the congruence and the number of them is the number of solutions that we say the congruence has.

(Refer Slide Time: 28:22)



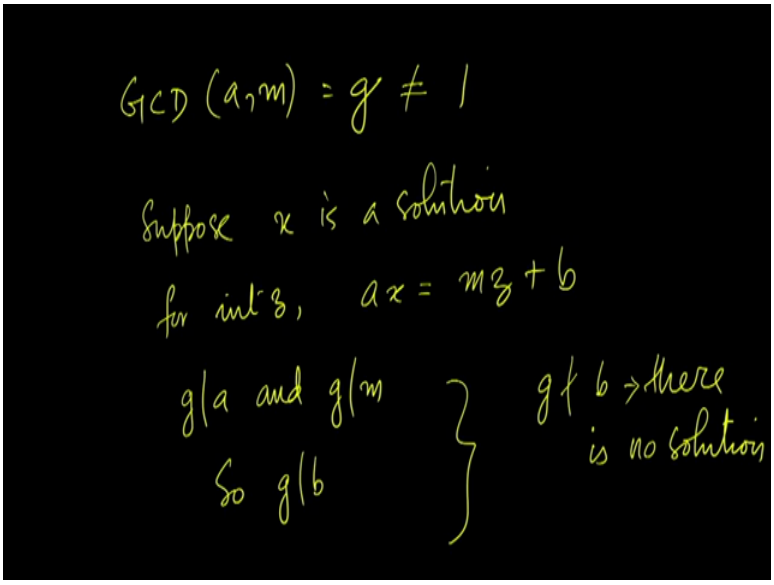
When we consider the polynomial of this form, say, j is the largest integer so that aj is not equal to 0, then j is the degree of this polynomial.

(Refer Slide Time: 29:04)



So let consider the congruences of degree 1, there is a congruence of the form ax equals b mod m so by the first theorem of today we showed that this has a solution, this has a unique solution in 0 to m minus 1 in the interval 0 to m minus 1 if GCD of a, m equal to 1.

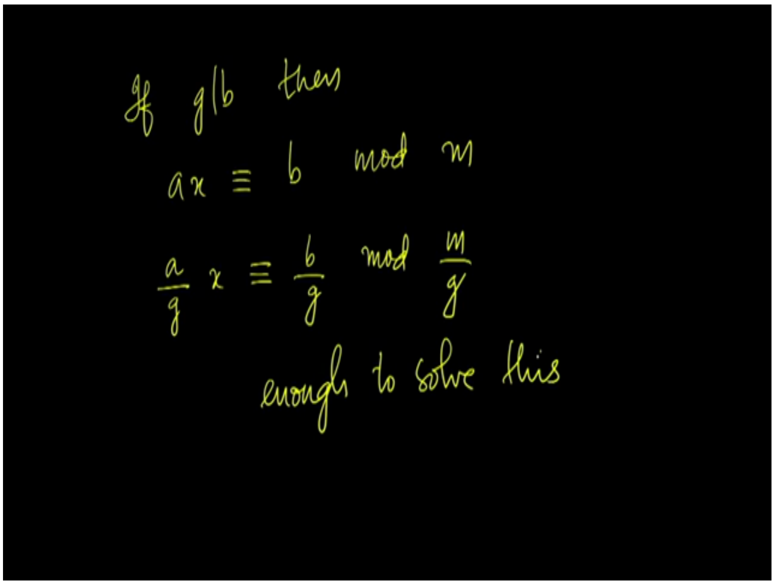
(Refer Slide Time: 29:50)



But now, let us assume that GCD of a, m is small g which is not equal to 1, so a and m have common factors, suppose x is a solution of the congruence ax congruent to b mod m then for integers z so some integer z ax equals mz plus b as ax is congruent to b modulo m ax must be b plus m z so some integer z now g is the GCD of a and m so g divides a and g divides m.

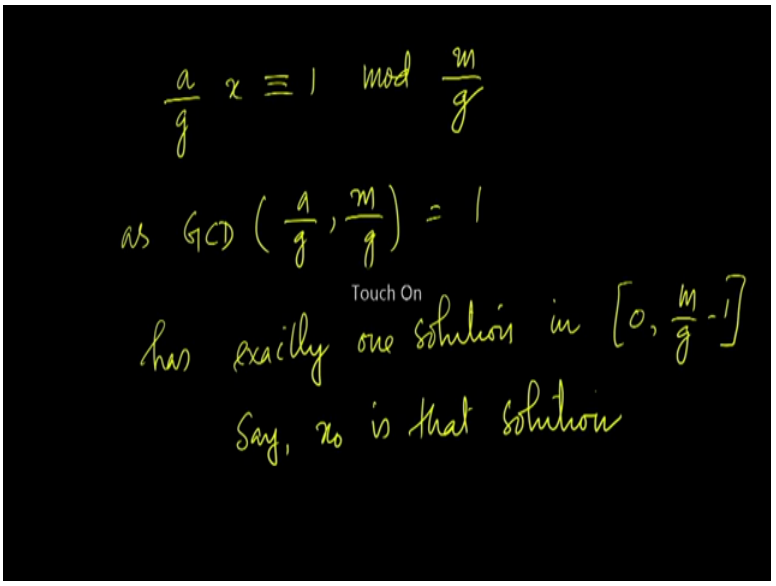
Therefore, g must divide b2, in other words of the after finding the GCD of a and m we find that g does not divide b, then there is no solution, once again the argument is if GCD of a, m is g which is not equal to 1, and the congruence has a solution x then ax must be mz plus b for some integer z since, g divides a and g divides m g must divide b to, conversely if g does not divide b, there can be no solution.

(Refer Slide Time: 31:36)



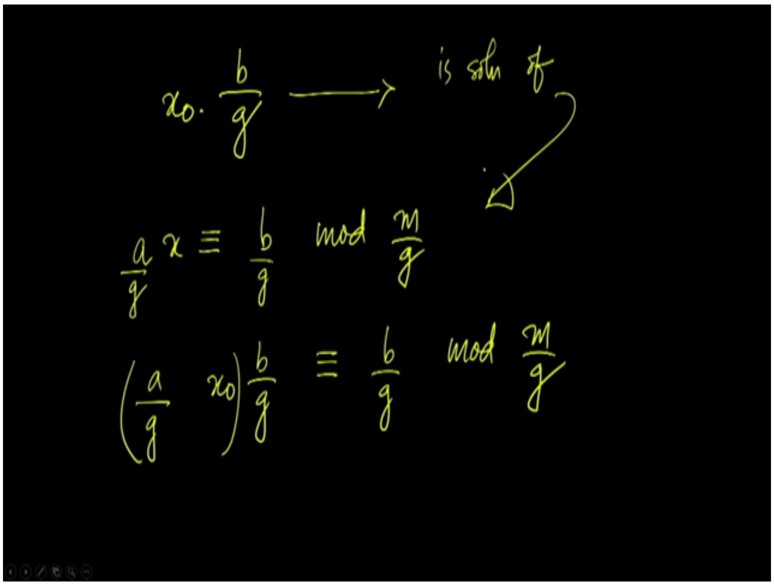
So let us assume that g divides b if g divides b then ax congruent to b mod m can be simplified g is a common factor of a, b and m in fact it is the GCD of a and m so dividing by g, I can rewrite this congruent in this fashion a by g x is congruent to b by g mod m by g but the theorem that we saw in the previous lecture so, it is enough to solve this congruence.

(Refer Slide Time: 32:25)



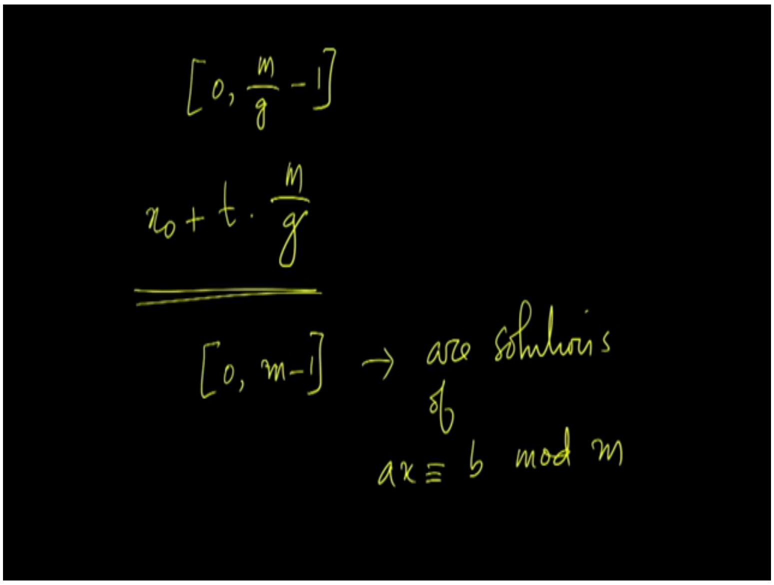
So solve this congruence first let us consider a by g x is 1 mod m by g we know that GCD of a by g, m by g is 1, they are relatively prime GCD of a and m is g so when you divide both a and m by g then the resolving numbers are relatively prime to each other, GCD of a by g, m by is 1, so this has this congruence has exactly one solution in which interval, 0 to m by g minus 1, in this range this congruence has exactly one solution say, x not is that solution, so x not is a solution of a by g, x congruent to 1 mod m by g.

(Refer Slide Time: 33:37)



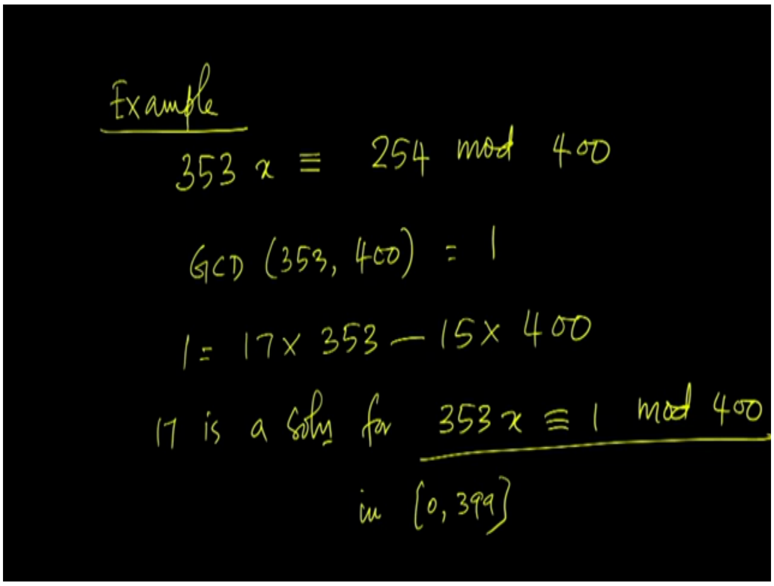
Then let us consider x naught times b by g and substitute this in the original congruence which is ax congruent to b a by g, congruent to b by g mod m, mod m by g. So we find that a by g, times x naught because by g is congruent to since x naught is a solution of a by g, x naught congruent to 1 mod b by g we find that a by g, x naught is 1 mod b by g. So this is b by g mod m by g, therefore x naught b by g is a solution of a by g, x solution of this congruence.

(Refer Slide Time: 34:54)



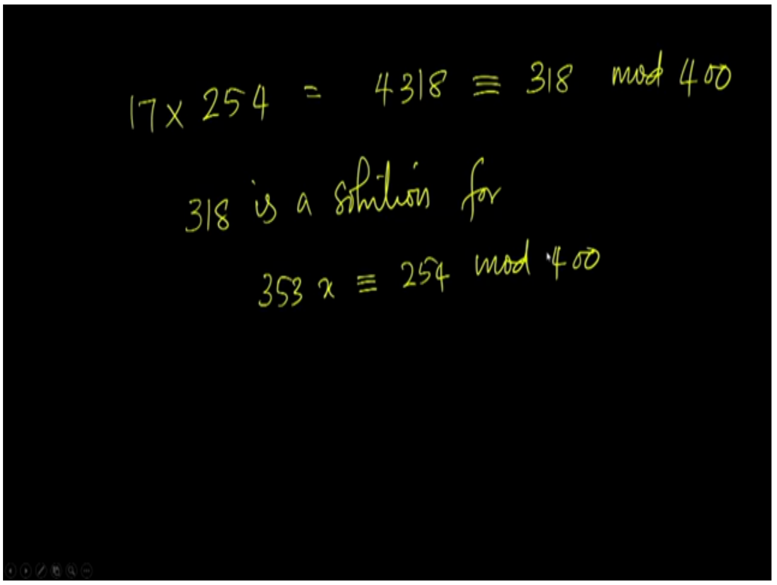
So this is the only solution of that congruence in 0 to m by g minus 1 and every solution to that congruence would be x naught plus t times m by g, consider all congruences of this form in the interval 0 to m minus 1 there all solutions of a ax equals b mod m so ax equals b mod m has multiple solutions in the range 0 to m minus 1 and although solutions can be found this way. There is but, the GCD of a and m is not 1 there are multiple solutions for this congruence in the interval 0 to m minus 1. So let us consider our previous example once again.

(Refer Slide Time: 35:58)



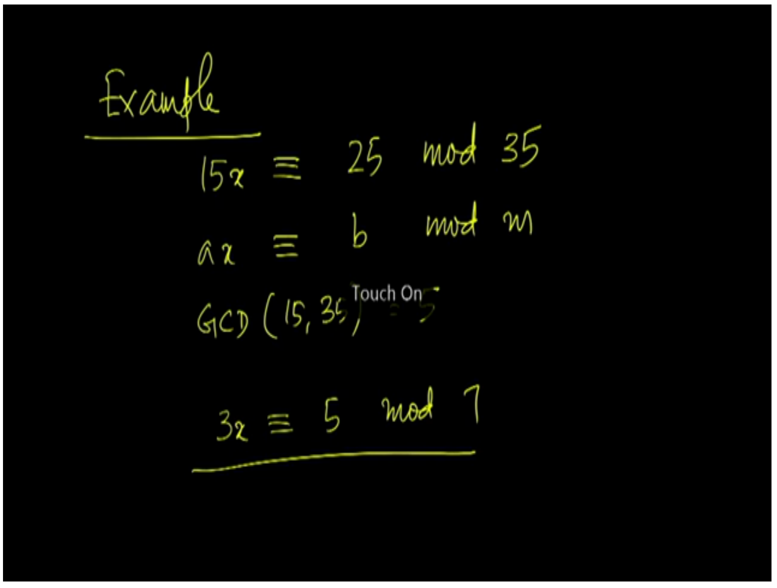
Where we want to solve 353 x equals 254 mod 400, we know that GCD of 353 and 400 is 1 353 is in fact a prime therefore one can be expressed as a linear combination of 353 and 400 using Euclid's algorithm we find that 1 is 17 into 353 minus 15 into 400, taking modulo 400 on both sides we have a that 17 is a solution for 353 x equals 1 mod 400. In other words, 17 is the only solution for this congruence in 0 to 399 but what we want to say solutions for 353 times x is congruent to 254 mod 400 instead of 1 so if you multiply this solution with 254.

(Refer Slide Time: 37:28)



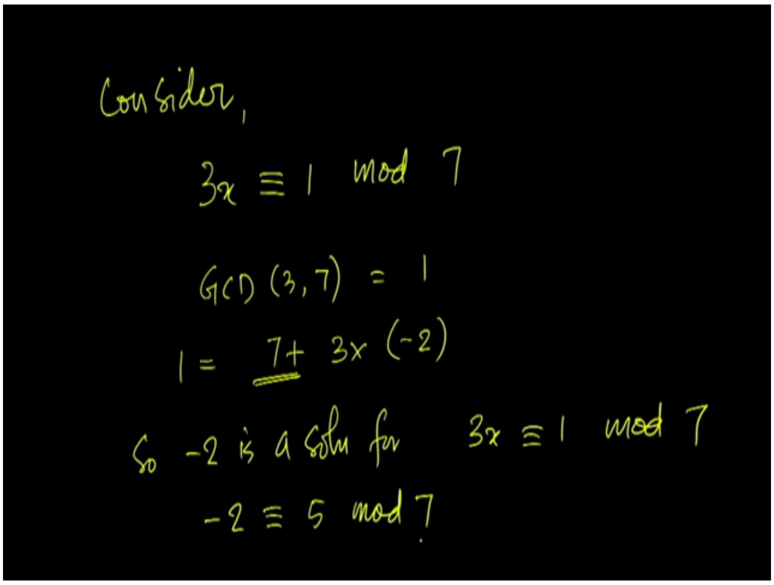
Which means 17 into 254 which is 4318 so is congruent to 318 mod 400. We find that 318 is a solution for the original congruence 353 x is 254 modulo 400. So here we have manage to find the solution without resorting to large exponents.

(Refer Slide Time: 38:05)



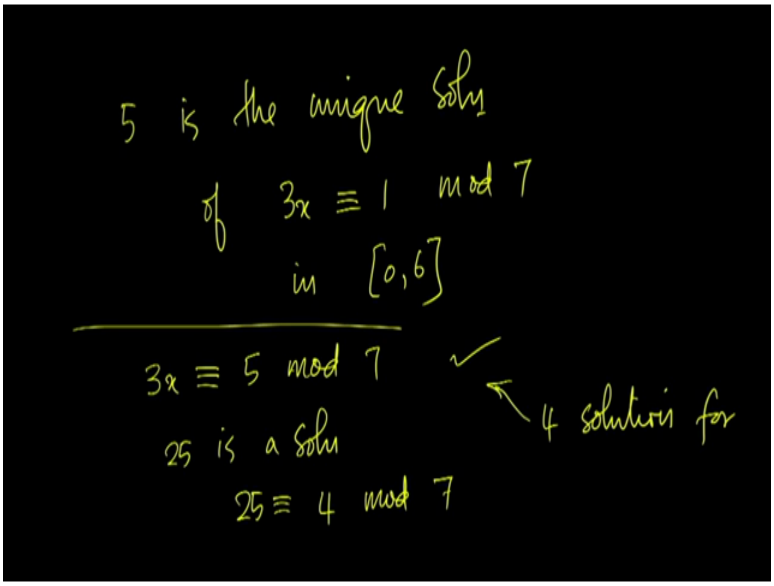
Let us consider one more example, let a see we want solve this congruence 15 x is congruent to 25 mod 35 so this is the of the form ax equals b mod m where, a and m are not relatively prime GCD of 15 and 35 is 5. Therefore, it is enough to solve the congruence obtain by dividing this by 5, so a by g is 3, so we have 3x congruent to 5 b by g is 5 mod 7. So let us solve 3x congruent to 5 mod 7.

(Refer Slide Time: 39:00)



To solve this first consider, 3x is congruent to 1 mod 7 so let us solve this first GCD of 3 and 7 is 1 therefore 1 can be expressed as a linear combination of 3 and 7 so 1 is 7 plus 3 into minus 2 therefore minus 2 is a solution for 3x congruent to 1 mod 7, this 7 can be ignored since we are taking mod 7 on both sides, so we have 3 into minus 2 equals 1 mod 7 so minus 2 is a solution for this but, minus 2 is the same as 5 mod 7.

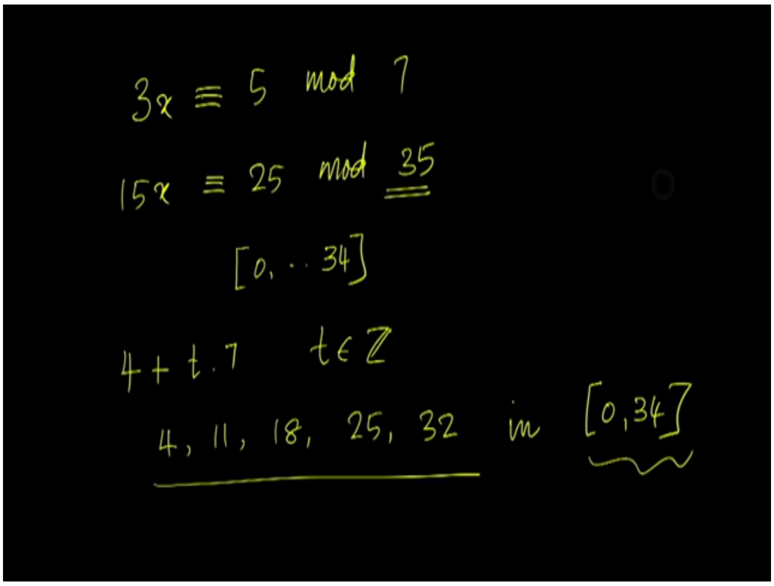
(Refer Slide Time: 40:00)



Therefore, 5 is the unique solution of 3x is 1 mod 7 in 0 to 6 in the interval 0 to 6, 5 is a unique solution for this congruence. But, what we need is a solution not for this congruence but, for 3x is congruent to 5 mod 7 this is what we want to solve since, 5 is a solution for 3x is congruent to 1 mod 7, 5 into 5 25, is a solution for 3x is 5 mod 7 but 25 is 4 mod 7, 21 plus

4 therefore 4 is a solution for this congruence 3x equal to 5 mod 7, of course substituting 4 here you can readily verify 3 into 4 is 1a 2 which is 5 mod 7 so it is indeed a solution.

(Refer Slide Time: 41:16)



So we have a found a solution for 3x is 5 mod 7 but we want the solution for 15 x is 25 mod 35 since we want the solution mod 35 we would like solutions in the range 0 to 34 both inclusive we know that 4 is a solution, 4 is the unique solution for 3x is 5 mod 7 but, then 4 plus t into 7 where t belongs to z the set of integers, is also a solution. So any integer of the form 4 plus 7t is a solution so 4 is a solution 4 plus 7, 11 is a solution 11 plus 7 18 is a solution, 25 is also solution, 32 is a solution, but these are the solutions in 0 to 34 so these are all solutions for 15 x is 25 mod 35 so this we find all solutions within the interval 0 to 34 that is it from the lecture, hope to see you in the next, Thank you.