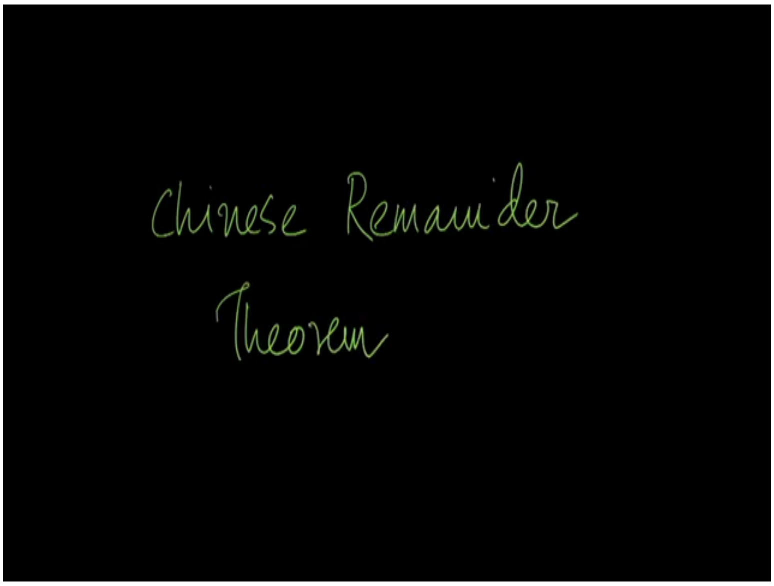
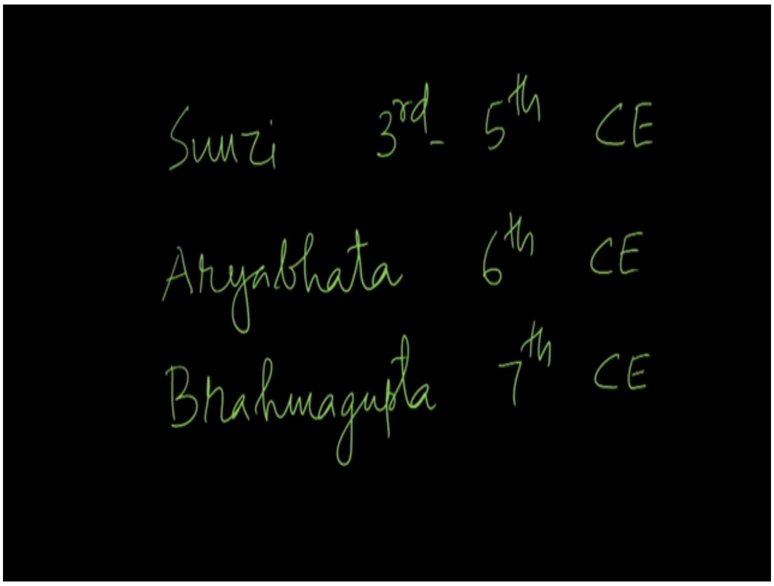
Discrete Mathematics
Professor Sajith Gopalan
Department of Computer Science and Engineering,
Indian Institute of Technology Guwahati
Lecture 35:
Chinese Reminder Theorem

Welcome to the NPTEL mock on discrete mathematics this is the sixth lecture on the number theory,

(Refer Slide Time: 00:40)

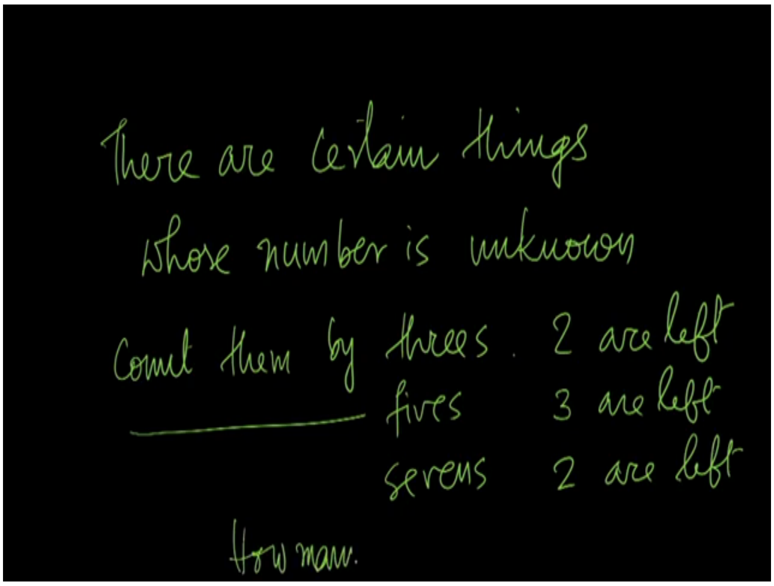




Today we study the Chinese reminder theorem, Chinese reminder theorem is one of the oldest mathematical theorem, it has been known since ancient times the first record of this problem was found in Chinese (())(0:57) on mathematics called Sunzi dated to 3rd to 5th century of the

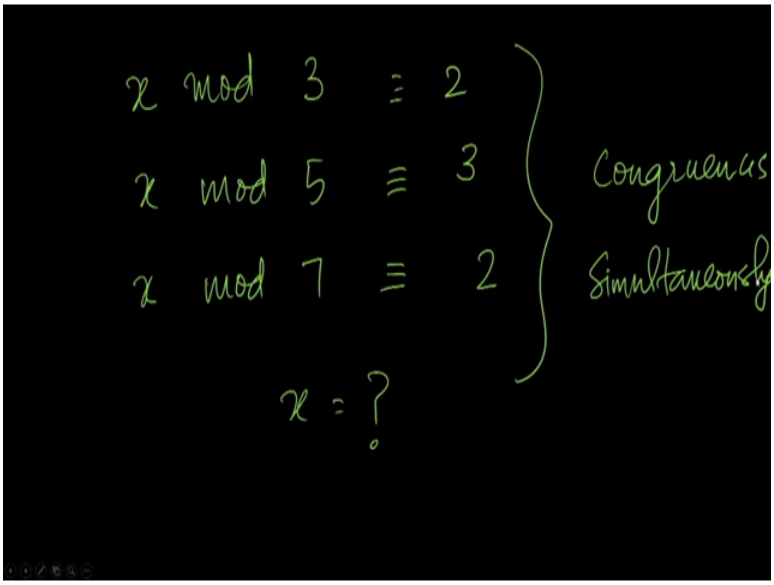
Common Era but a statement of the problem could be found at but the first known algorithmic solution was due to Indian mathematician Aryabhata who lived in the 6th century of the Common Era. The India mathematician Brahmagupta who lived almost the century later this is also known to have a been aware of the problem as well as the solution.

(Refer Slide Time: 1:49)



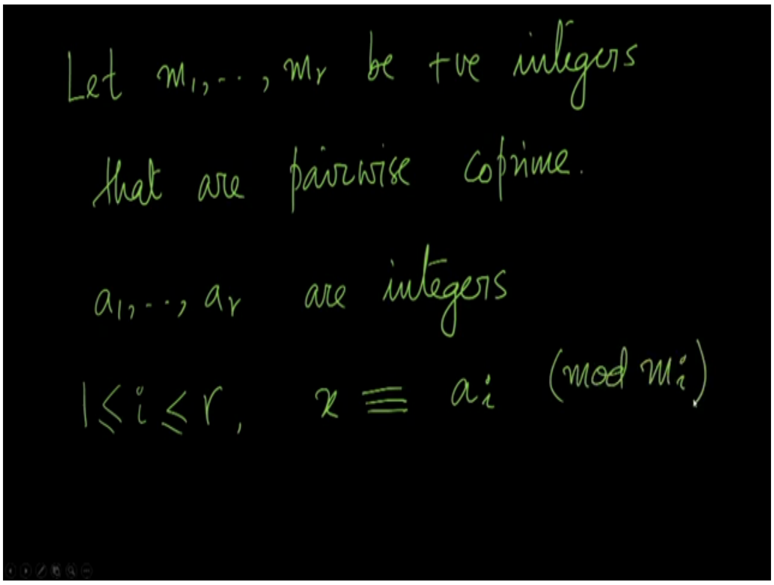
The Chinese (())(1:48) in which the problem first appears states thus, there are certain things whose number is unknown that is there is an unknown variable, count them by the threes 2 are left count then by fives 3 are left count then by sevens 2 are left how many are there, in other words.

(Refer Slide Time: 02:50)



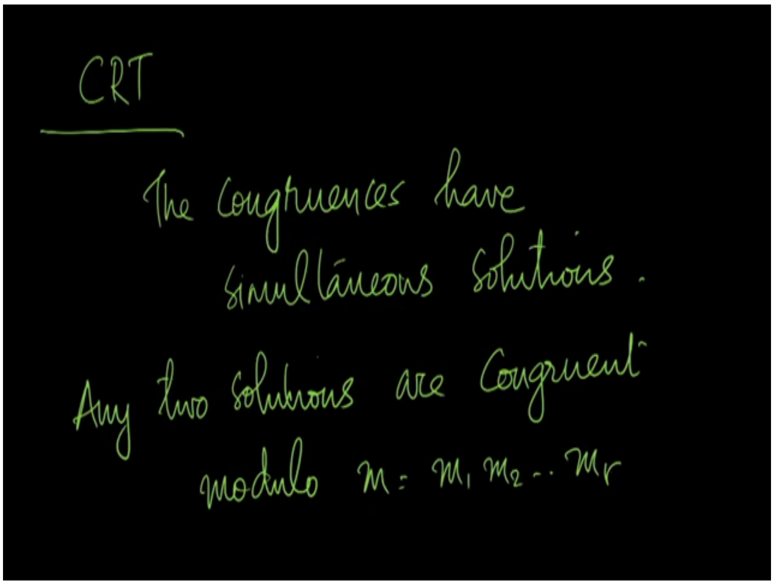
Let a see we have an unknown integer x what we is that x mod 3 is 2 x mod 5 is 3 x mod 7 is 2. What is x, this is the question that the Chinese mathematician posed basically we have to solve these three congruences simultaneously, that is we need a simultaneous solutions of a set of congruences.

(Refer Slide Time: 03:41)



So now let us look at the general statement of the problem. So let a see m1 through mr are let these be positive integers that are pair wise coprime let a say even through ar are integers we have a set of congruences are congruence is to be precise the ith congruence says that x is congruent to ai mod mi.

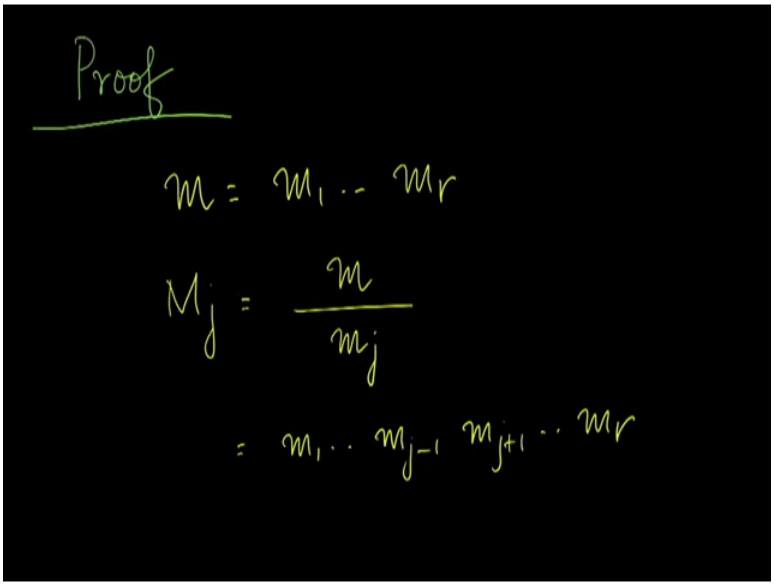
(Refer Slide Time: 04:47)



Then the Chinese reminder theorem says that in this context the congruences have simultaneous solution in particular any two such solutions are congruent to modulo m where m is the product of m1 through mr.

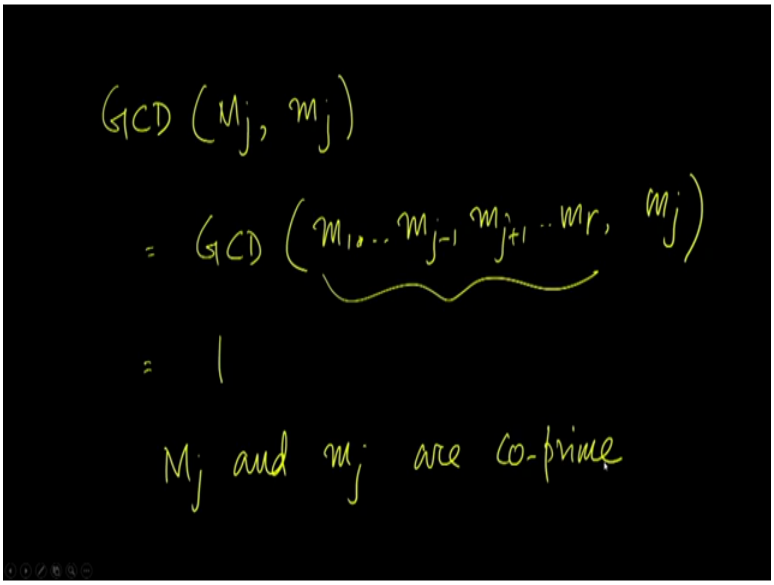
So that is what Chinese reminder theorem says, in this context where we have a set of positive integers r positive integers to be precise which are pair wise coprime which means the GCD of any pair is 1, then also given r, a 1 through ar that are r integers and we have these congruences r congruences x is congruent to ai mod mi in this context what the theorem says is that, this congruence is do have simultaneous solutions and any two solutions are congruent modulo m where m is the product of m1 through mr.

(Refer Slide Time: 06:03)



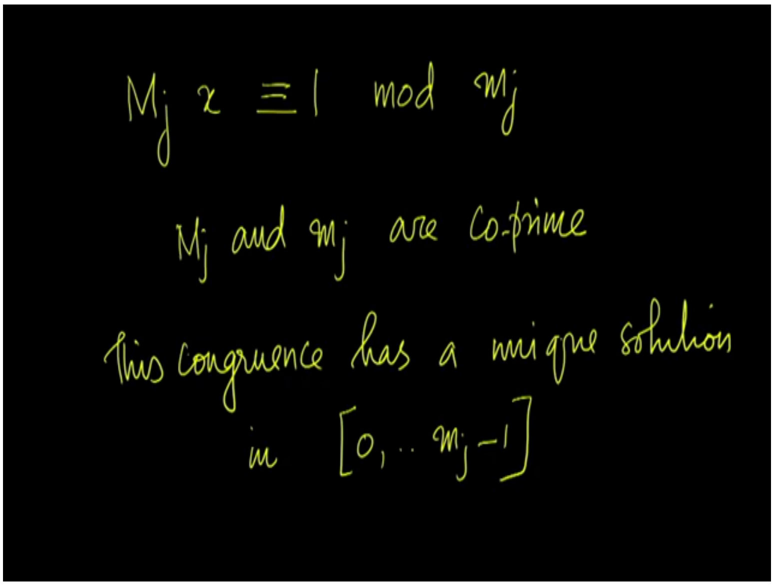
So let a see proof of this so small m is the product of m1 through mr let us define capital Mj as small m divided by small mj which means capital Mj is m1 through mj minus 1 and then mj plus 1 through mr that is we take a product of all the m s except mj.

(Refer Slide Time: 06:44)



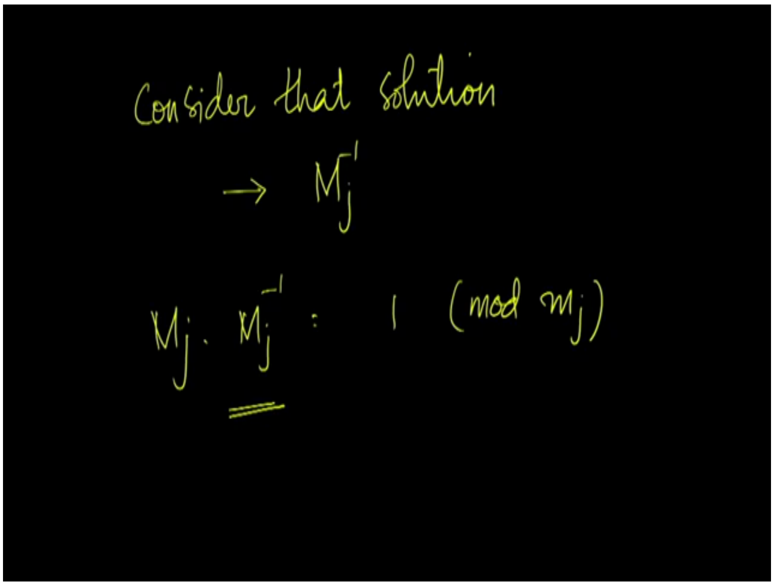
Then what would be the GCD of Mj and small mj that is we are seeking the GCD of this product m1 through mj minus 1 mj plus 1 through mr and mj. Now what we know is that the mj's are all pair wise coprime so mj is coprime with m1 m2 etc. each of these m s which means mj is coprime with the argument on the left hand side which means we have a 1 as the GCD of these, in other words mj and capital Mj and small mj are coprime. Product relatively prime. coprime is another word for it.

(Refer Slide Time: 07:46)



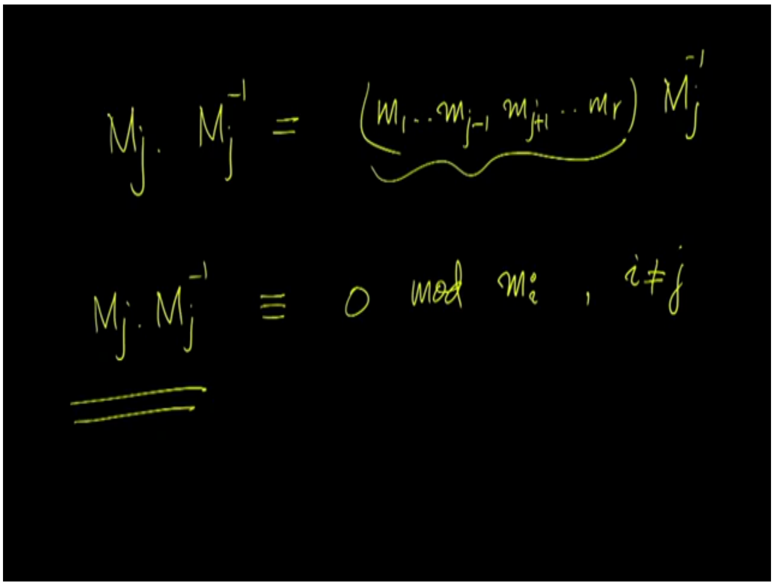
Let us consider this congruence now capital Mj x is 1 mod small mj so here we know that Mj and small mj are coprime that is what we have just shown, therefore by the discussion that we had in the previous classes we know that this congruence has a unique solution in 0 to mj minus 1 so there is a bj within this range which is a solution for this.

(Refer Slide Time: 08:40)



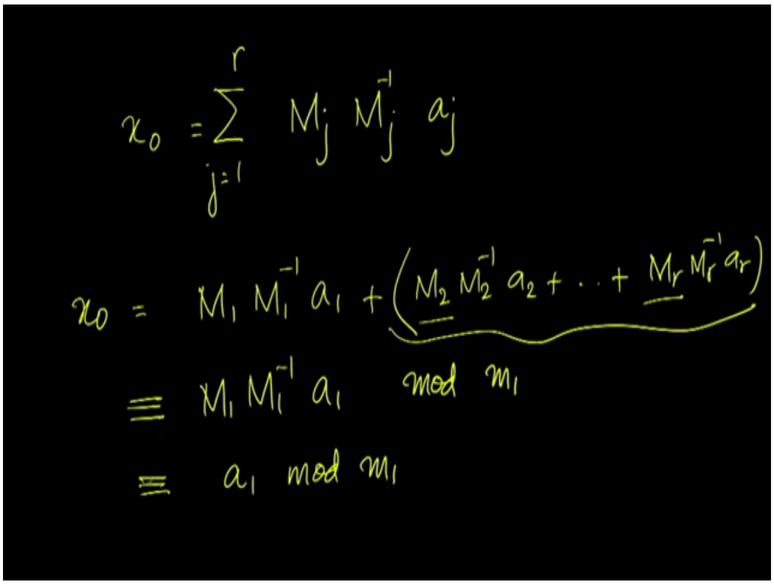
So consider that solution, that unique solution in the range 0 to mj minus 1. Let us denote it by Mj inverse what we find is that Mj multiplied by Mj inverse is 1 mod small mj so that is why we called it the inverse Mj multiplied by Mj inverse is 1 mod small mj.

(Refer Slide Time: 09:15)



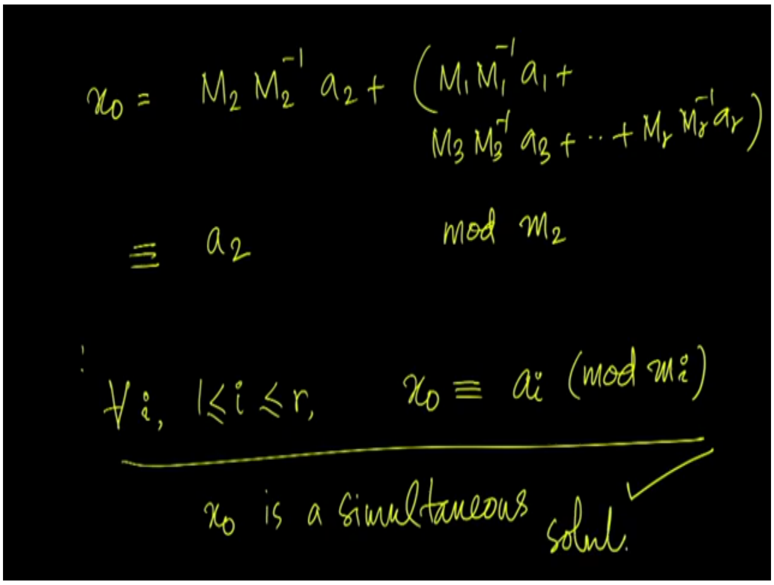
But, then Mj multiplied by Mj inverse can be written as m1 through mj minus 1 small m mj plus 1 through mr multiplied by Mj inverse. Therefore, Mj Mj inverse is 0 mod mi when I is not equal to j because mi will feature here when i not equal to j therefore mi will divide this factor therefore it would divide the entire product therefore Mj Mj inverse is divisible by mi when i is not equal to j.

(Refer Slide Time: 10:22)



So this naturally suggest that, we should x naught which is of this form take the sum of j varying from 1 to r of Mj Mj inverse aj so this is what x naught is. Now x naught can be written as M1 M1 inverse a1 plus M2 M2 inverse a2 through Mr inverse ar this we find is congruent to M1 M1 inverse a1 mod small m1. That is because M2 is a multiple of small m1, m3 so multiple small m1 and so on, similarly Mr. is also multiple of small m1, therefore this entire quantity within the brackets will go to 0, but then M1 multiplied by M1 inverse we know is 1 mod M1 therefore this is congruent to a1 mod m1. In other words, x naught is congruent to a1 mod m1.

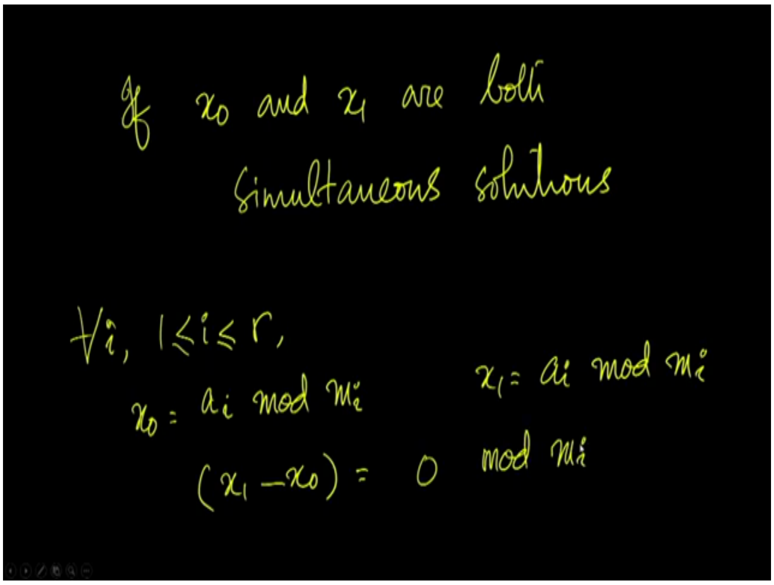
(Refer Slide Time: 11:53)



X naught can also be written as M2 M2 inverse a2 plus M1 M1 inverse a1 plus M3 M3 inverse a3 plus all the way to Mr Mr inverse ar that is the remaining terms if I take the congruence of this modulo m2. We find that the quantity within the bracket again goes to 0, because small m2 divides capital M1 capital M3 etc. Therefore, the quantity within the bracket is 0, and M2 M2 inverse is 1 mod m2 therefore this is a2 mod m2. So continuing lie this we find that for every i with 1 less than or equal to i less than or equal to r, x naught is congruent to ai mod mi that proves one part of the theorem, so x naught is indeed a simultaneous solution.

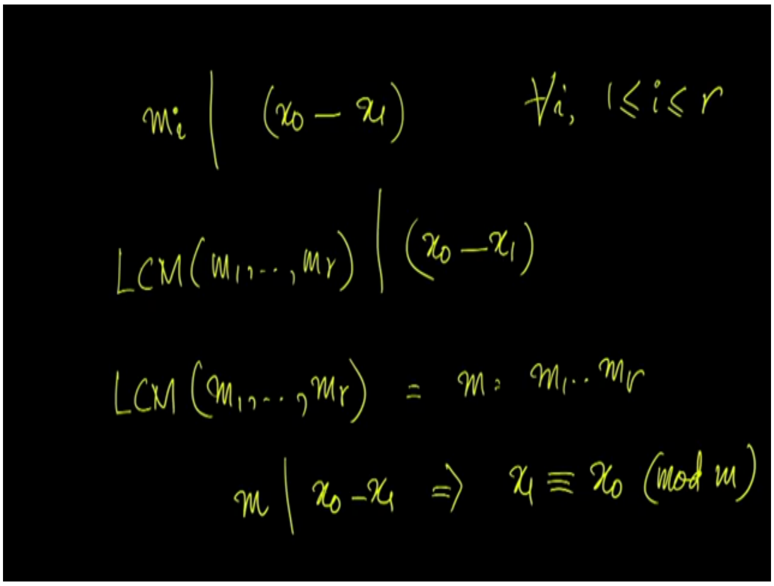
So looking back at the theorem we know that the theorem says the congruences do have simultaneous solutions so we have found one simultaneous solution, and then the rest of the theorem says that any two solutions are congruent modulo m where small m is m1 through mr so let us proof that now.

(Refer Slide Time: 13:45)



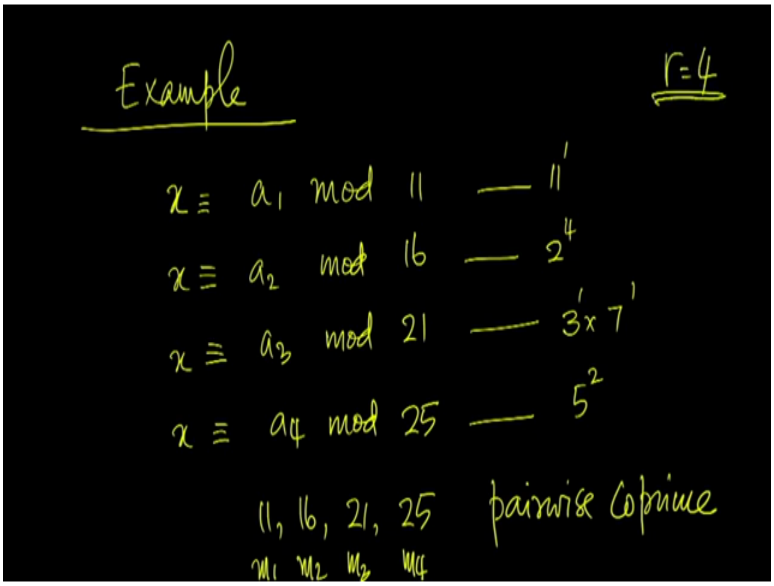
If x naught and x1 are both solutions both simultaneous solutions of the system then for every i 1 less than or equal to i less than or equal to r, we know that x naught is ai mod mi and x1 is ai mod mi which means x1 minus x naught is 0 mod mi.

(Refer Slide Time: 14:36)



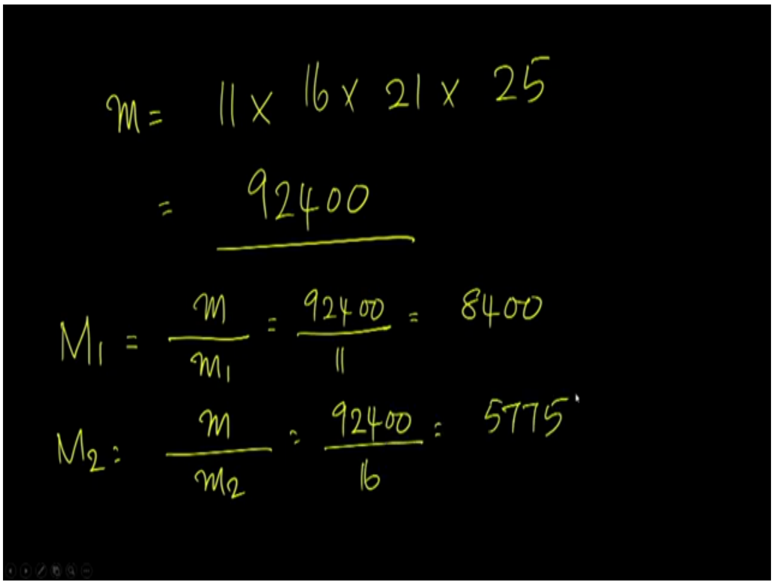
In other words mi divides x naught minus x1, for every i since every mi divides x naught minus x1, then the least common multiple of m1 through mr must also divide x naught minus x1, but then what is the LCM of m1 through mr this is nothing but m which is the product of m1 through mr that is because mi and mj are coprime with each other for any i not equal to j. So the LCM of these is nothing but m so what we have is that m divides x naught minus x1, in other words x1 is congruent to x naught mod m that is precisely what the theorem says. If for any two solutions these two solutions are congruent to each other modulo m. So that completes the poof of the theorem.

(Refer Slide Time: 15:50)



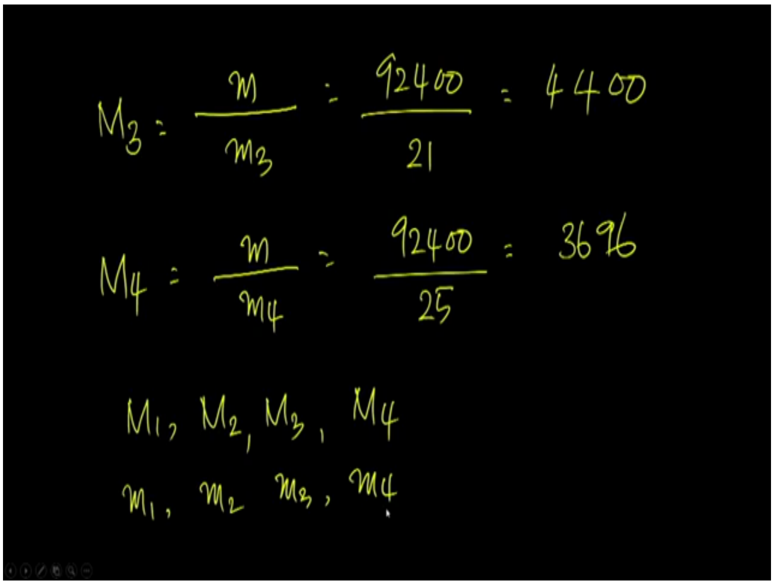
So now, let us work out an example let us say we have a congruence of this form x is congruent to a1 mod 11 x is also congruent to a2 mod 16 x is congruent to a3 mod 21, x is congruent to a4 mod 25. So 11 is a prime 16 is 2 power 4, 21 is 3 into 7 so 3 power 1 into 7 power 1, 25 is 5 power 2. So, there are all relatively prime. That is 11, 16, 21, 25 are all pair wise coprime so these are respectively m1, m2, m3 and m4 of the theorem. Here r is 4 so we have considering a problem of size 4.

(Refer Slide Time: 17:12)



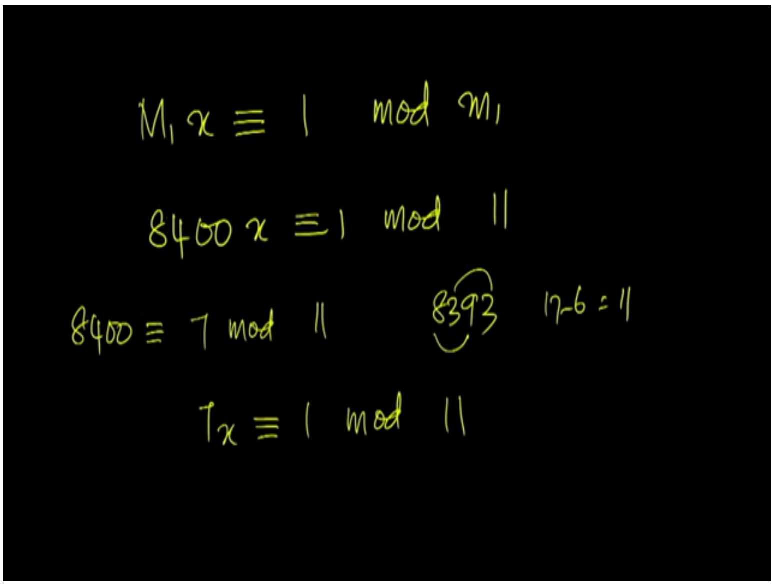
Now, small m is defined as the product of this 11 into 16 into 21 into 25 which is 92400. Then capital M1 would be small m divided by small m1 which is 92400, divided by 11 which is 8400, M2 is small m divided by small m2 which is 5775.

(Refer Slide Time: 17:55)



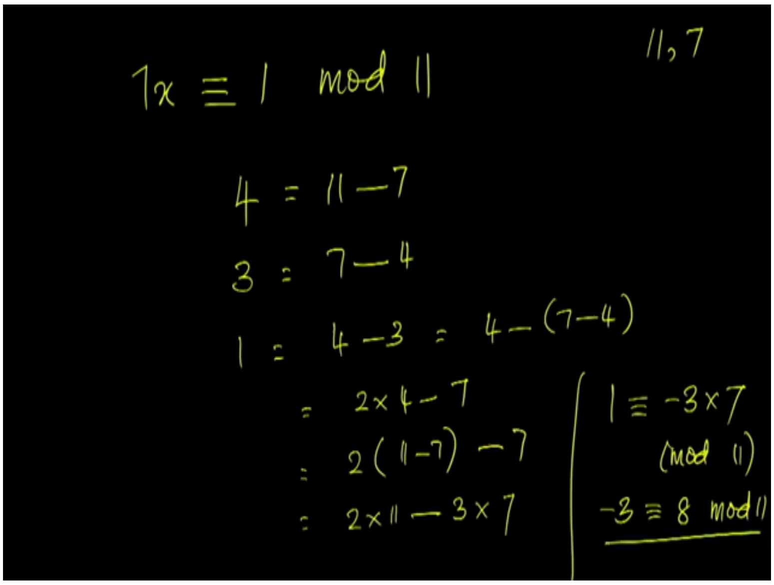
M3 is small m divided by 21 92400 divided by 21 this is small m3 which is 4400 and capital M4 is small m divided by small m4 which is 92400 divided by 25, which is 3696 so we have to now find the inverses of M1, M2, M3 and M4, modulo small m1, small m2, small m3 and small m4 respectively. So let us try to find those inverses.

(Refer Slide Time: 18:47)



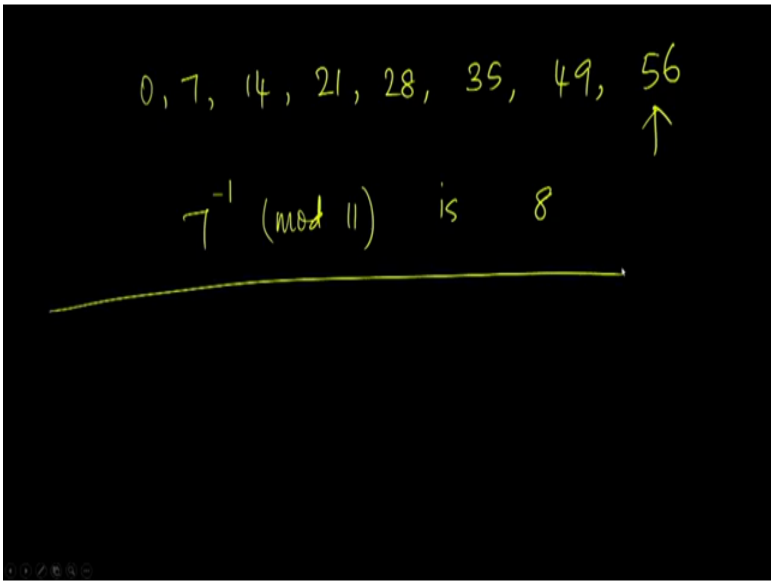
First we have to solve this M1 of x is 1 mod small m1 that we have to find the inverse of capital M1 with respect to small m1 which is 8400 x is congruent to 1 mod 11 let us 8400 is 7 mod 11 8393, 8 plus 9 17 3 plus 3 6 so 17 minus 6 is 11 so this is divisible by 11 so 8400 is 7 mod 11. So this congruence can be written as 7x equals 1 mod 11 so we only need to find the inverse of 7 with respect to 11 that would also be the inverse of 8400 with respect to 11.

(Refer Slide Time: 19:44)



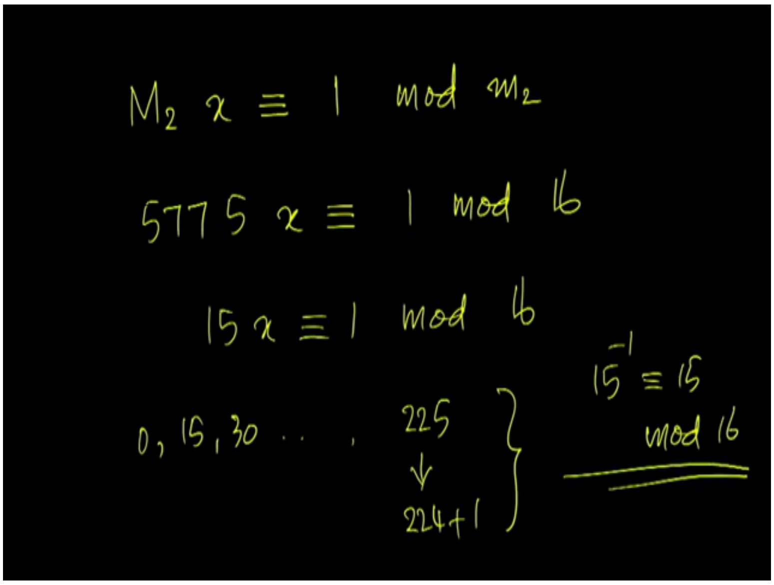
So this is what we have to solve, 7x is a 1 mod 11 of course you could use Euclid's algorithm for doing this if we use Euclid's algorithm on 11 and 7 we find that 4 is 11 minus 7 then 3 is 7 minus 4, 1 is 4 minus 3 which is then 4 minus 7 minus 4 which is 2 into 4 minus 7 but 4 is 11 minus 7 so into 11 minus 7 minus 7 so that will be 2 into 11 minus 3 into 7, so if you take modulo 11 on both sides of the equation we find that 1 is congruent to minus 3 into 7 so we want the solution for 7x equals 1 mod 11 so we find that minus 3 is a solution. But minus 3 is 8 mod 11 so 8 is a solution as well.

(Refer Slide Time: 21:06)



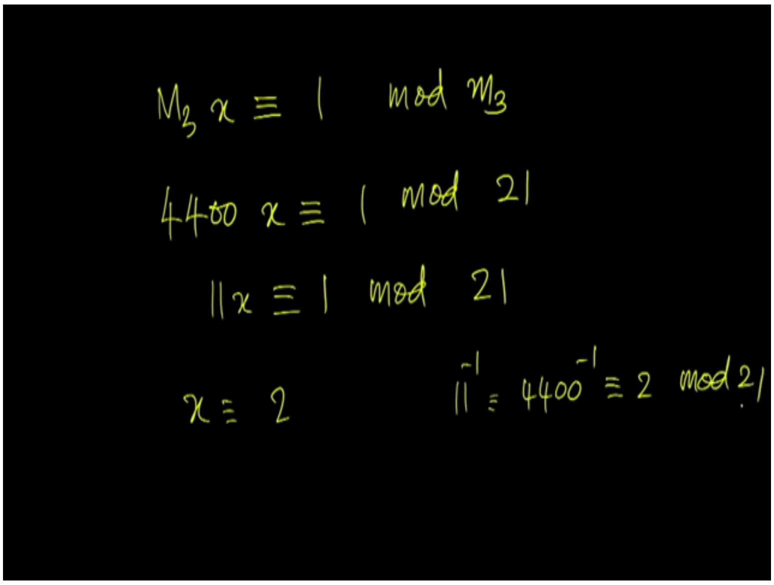
Of course an easier way of solving would be to count the multiples of 7 0, 7, 14, 21, 28, 35, 49, and 56. 56 is 1 mod 11. So 7 inverse mod 11 is 8.

(Refer Slide Time: 21:37)



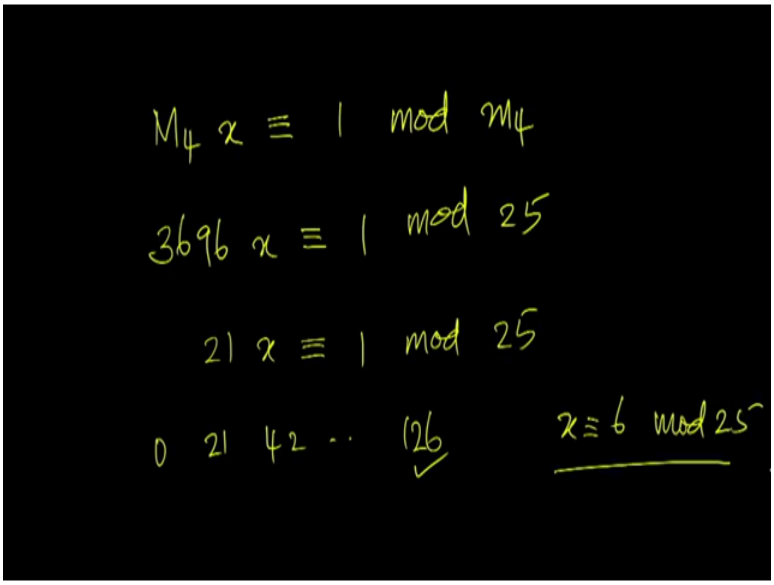
Then we have to solve this congruence M2 x equals 1 mod m2 or in other words 5775 x is congruent to 1 mod 16, 5760 is a multiple of 16 so we have a 5760 plus 15 x here so its 15 x is congruent to 1 mod 16 so when you run through the multiplication table for 15 you find that 0, 15, 30 etc. However, none of them 1 mod 16 until you comes to 225 the 255 is a 224 plus 1 224 is 14 into 16, so we find that 15 is the inverse of 15 mod 16. So the second solution is 15.

(Refer Slide Time: 22:38)



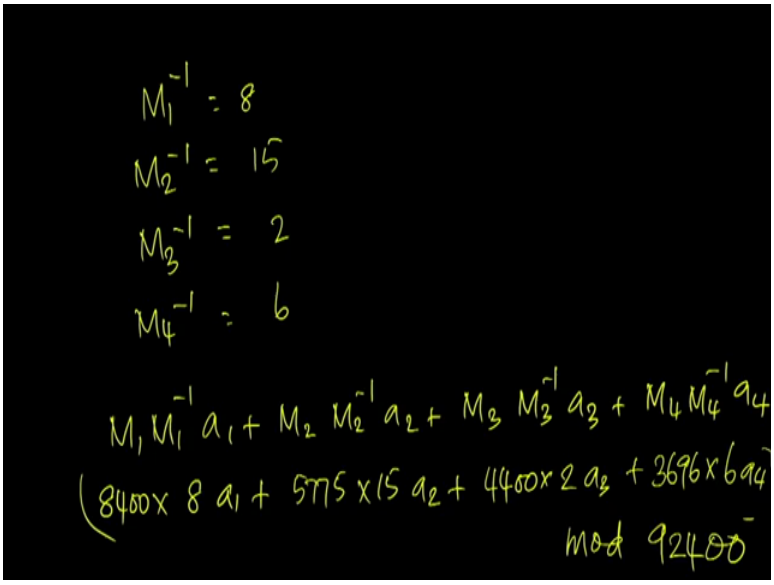
And the 3rd one is a M3 x is congruent to 1 mod small m3, what is capital M3 that is 4400 that is 1 mod 21 4400, 4200 and then 200 left 189 11, 11 x is 1 mod 21 so as you can readily see 21 is 1 mod 21 so x equal to 2 is a solution which means 11 inverse which is also 4400 inverse is 2 mod 21 so there is a 3rd solution.

(Refer Slide Time: 23:34)



And then coming to the 4th one M4 x is 1 mod small m4, which is 3696 x is 1 mod 25, 3696 is minus 4 3700 minus 4 which is 21. 21 x is 1 mod 25 this is what we have to solve, so running through the multiples of 21 etc. When we come to 126 we find that it is 1 mod 25. So x equal to 6 is the solution the 4th solution.

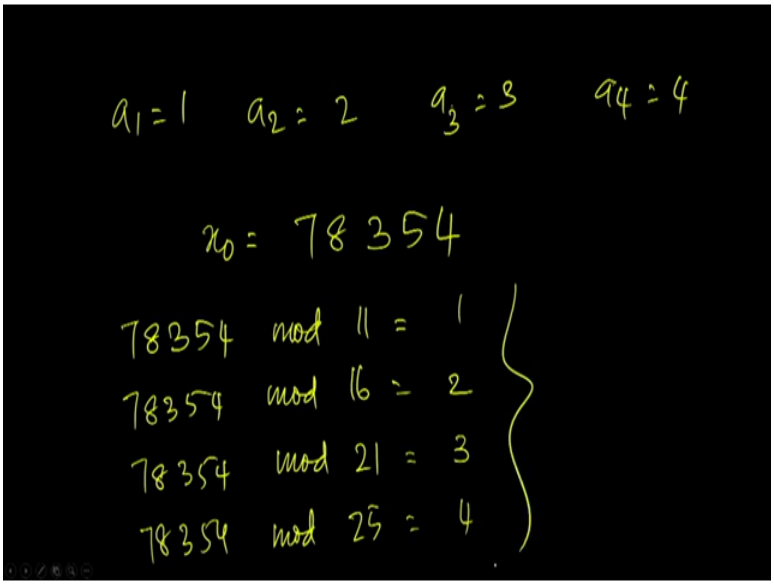
(Refer Slide Time: 24:30)



So we have now the 4 solutions M1 inverse is 8 M2 inverse is 15, M3 inverse is 2, M4 inverse is 6 so a solution then would be M1 M1 inverse a1 plus M2 M2 inverse a2 plus M3 M3 inverse a3, plus M4 M4 inverse a4 which means 8400 into 8 a1 plus 5775 into 15 into a2, plus 4400 into 2 into a3, plus 3696 into 6 into a4.

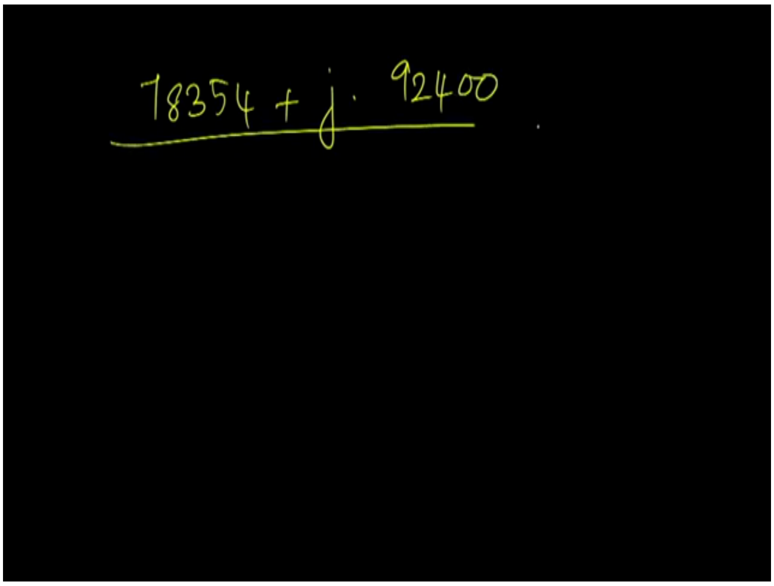
The whole of this modulo 92400 is the solution that we want. I have deliberately avoided choosing a1, a2, a3, a4 to show that the computation remains the same irrespective of these values so whatever a1, a2, a3, a4 are the solution will take on this from now we only have to plugin a1, a2, a3, a4.

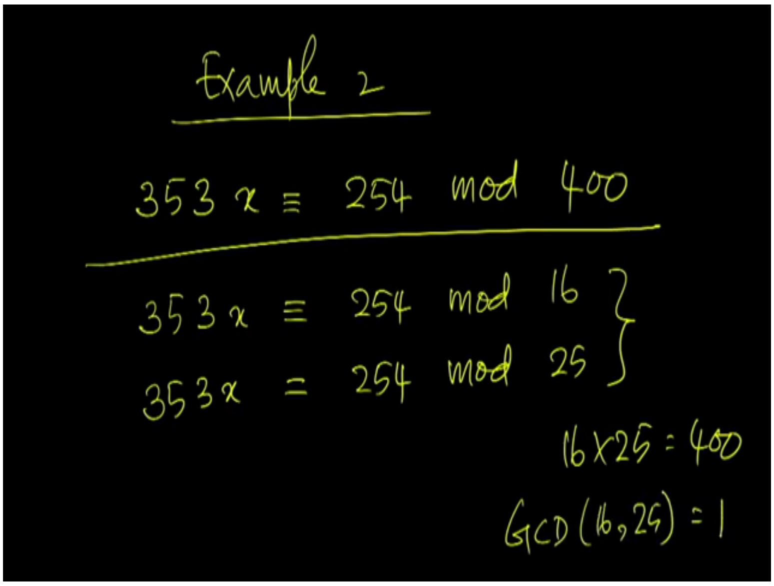
(Refer Slide Time: 26:11)



So let us assume that a1 equals to 1, a2 equal to 2, a3 equal to 3, a4 equal to 4 if this is the case plugin in these values we find that the solution x naught is 78354, verifying we find that 78354 mod 11 is 1, 78354 mod 16 is 2, 78354 mod 21 is 3, mod 25 is 4. So this is (())(27:08) solution that we seek.

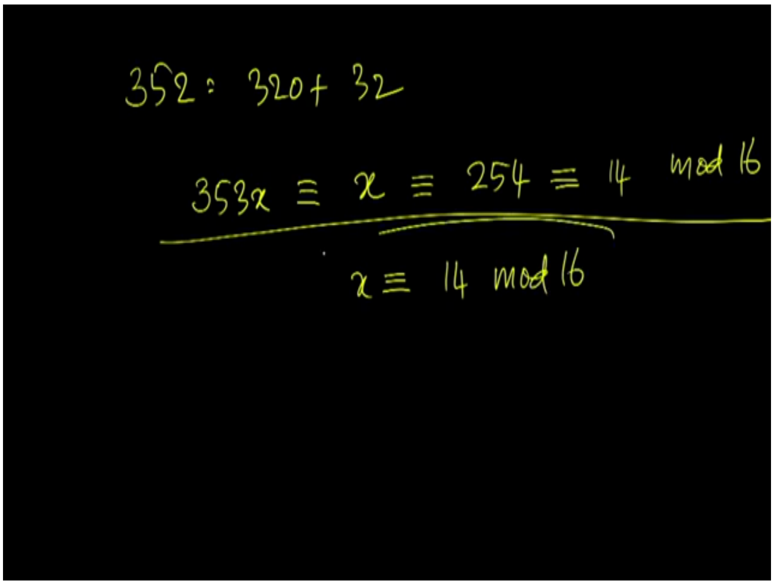
(Refer Slide Time: 27:12)





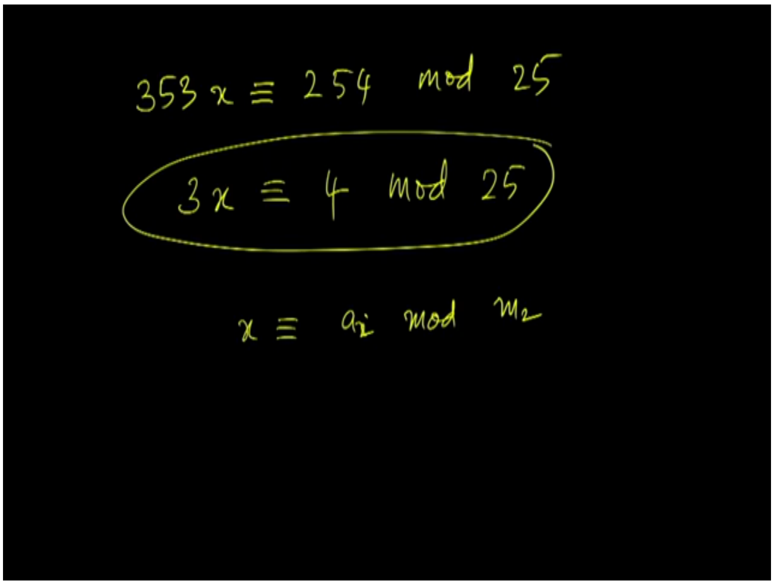
And then 78354 plus j into 92400 is the general solutions. So let us consider another example now so this is a familiar problem let a see we want to solve 353x is congruent to 254 modulo 400 we have seen two ways of solving this before so this is a 3rd way we could convert this into simultaneous congruences in this manner, 353 x is congruent to 254 mod 16 and 254 mod 25 separately this is because 16 into 25 is 400 and 16 and 25 are relatively prime to each other.

(Refer Slide Time: 28:27)



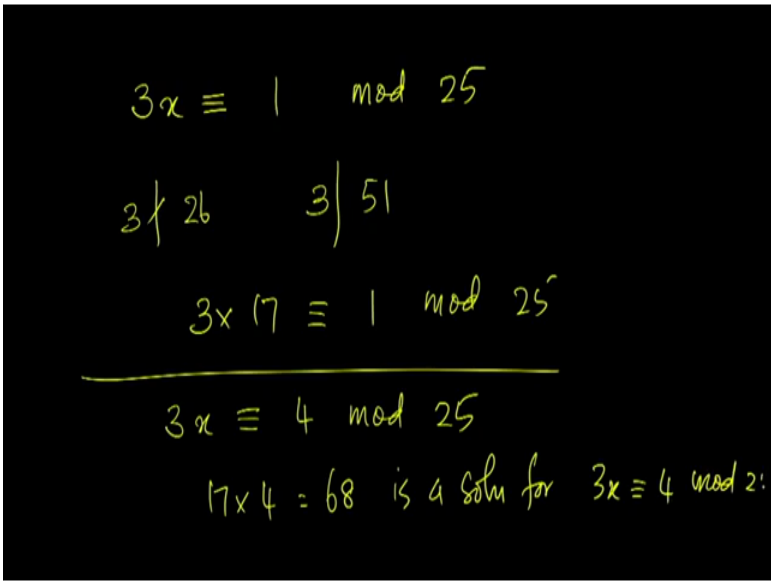
But then 352 is 320 plus 32 so that is a multiple of 16 so 353 x is congruent to x mod 16, which is equal to 254 mod 16 but then 254 is 240 plus 14 so 240 is a multiple of 16 so we have 14 mod 16. So the first congruence namely 353 x is congruent to 254 mod 16 reduces to x congruent to 14 mod 16 so this is one congruent that we have.

(Refer Slide Time: 29:17)



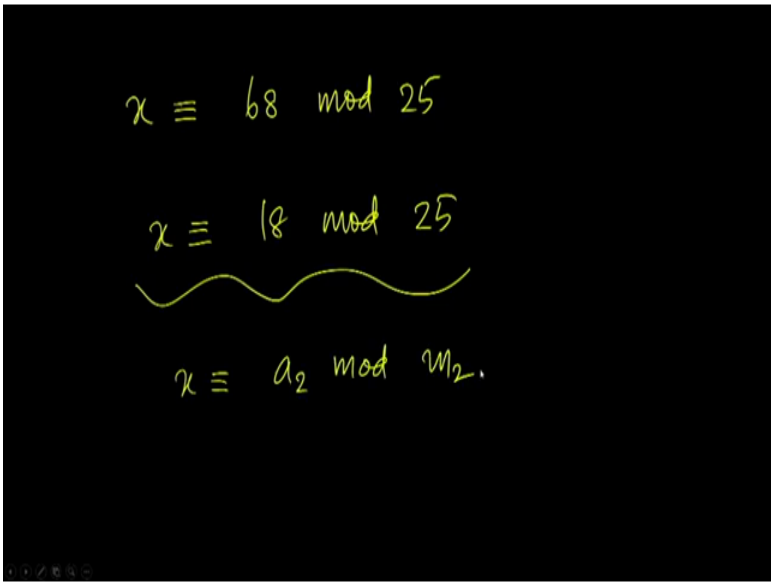
The other congruence namely 353 x is congruent to 254 mod 25 can be simplified like this 353 x is 3 x mod 25, 350 plus 3 and 254 is 250 plus 4 so there is 4, mod 25, so this congruence simplifies to 3x congruent to 4 mod 25, but this is not in the desired form because we would like this to be in this form. But, here we have 3 x on the left hand side.

(Refer Slide Time: 30:01)



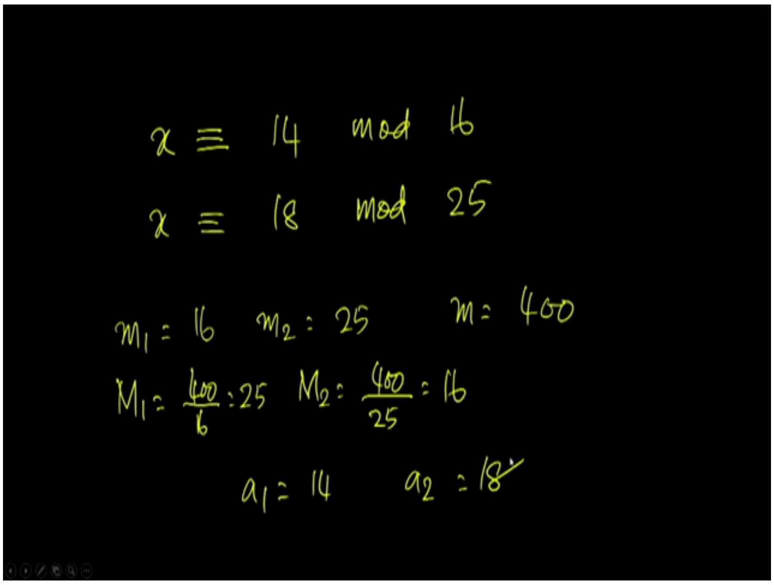
So let us solve 3x equals 1 mod 25 first so, considering the multiples of 25 plus 1 example consider 26 3 does not divide 26 but, 3 divides 51 which is 2 into 25 plus 1. Which means 3 into 17 is 1 mod 25 so 17 is a solution for this. so we have now a solution for 3x equals 1 mod 25 but, we are looking at the congruence 3x equals 4 mod 25 so if 17 is a solution for 3x equals 1 mod 25 then 17 into 4 which is 68 is a solution for 3x equals 4 mod 25.

(Refer Slide Time: 31:07)



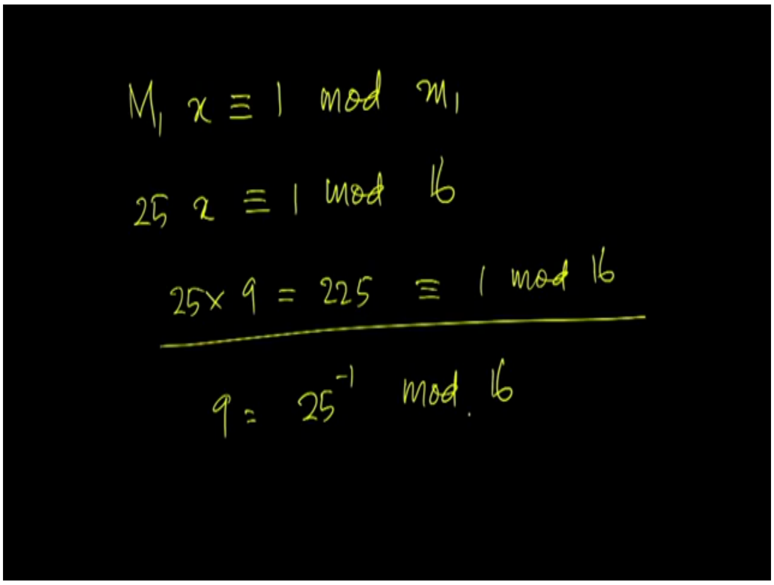
In other words, x is 68 mod 25 is a solution or x is 18 mod 25 is a solution now this is an the desired form, this is in the x equals a2 mod m2 form so this is our second congruence.

(Refer Slide Time: 31:34)



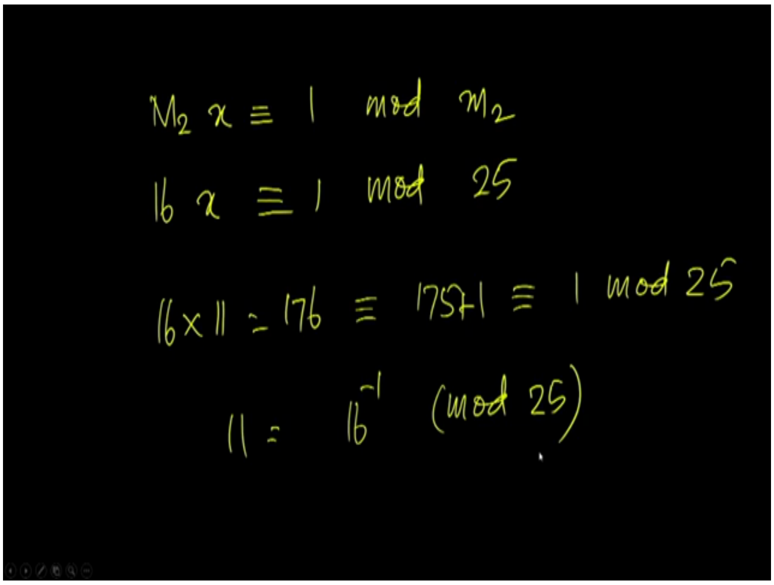
So now putting the two congruent to together we have x congruent to 14 mod 16 x congruent to 18 mod 25, so now we can apply the Chinese reminder theorem here m1 is 16, m2 is 25 so small m is 400 capital M1 is 400 by 16 which is 25 capital M2 is 400 by 25 which is 16, a1 is 14, a2 is 18.

(Refer Slide Time: 32:19)



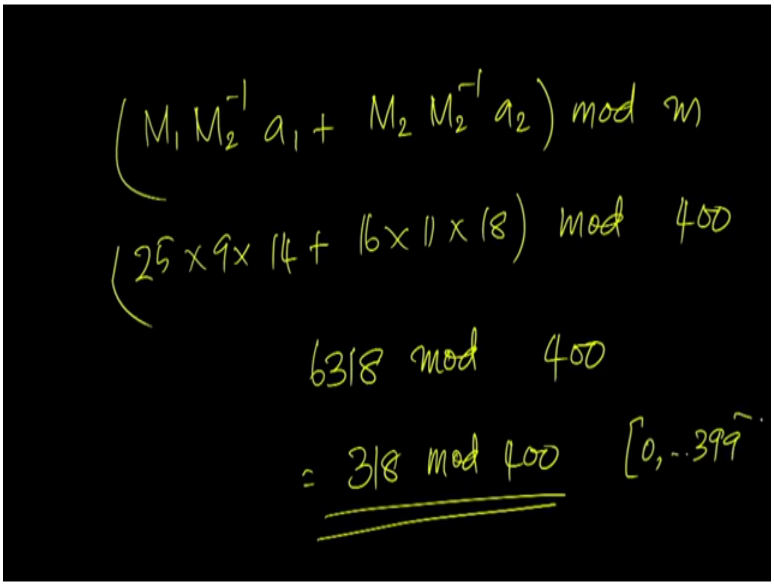
So n ow we have to solve M1 x is 1 mod small m1 which means we have to find the inverse of capital M1 with respect to small m1 or 25 x is 1 mod 16 so taking the multiples of 25 we find that 225 is 1 mod 16 nut, 225 is 25 into 9, so 9 is a solution so 9 is 25 inverse mod 16.

(Refer Slide Time: 32:55)



The other congruence we have to solve is M2 x is 1 mod small m2, which is 16 x is 1 mod 25 counting through the multiples of 16 we find that 16 into 11 this 176 which is 175 plus 1 so, 1 mod 25. Which means 11 is 16 inverse mod 25 so we now have the inverse is.

(Refer Slide Time: 33:37)



The first solution would be M1 M2 inverse a1, plus M2 M2 inverse a2, mod m which means 25 into 9 into 14, plus 16 into 11 into 18 mod 400 this looks out to 6318 mod 400 which is 318 mod 400. So this is the only solution in the range 0 to 399. So that is about the Chinese reminder theorem that is it from this lecture hope to see you in the next, Thank You.