A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 18
Chinese Remainder Theorem, the General Case and Examples

Welcome back. We are looking at proof of the Chinese Remainder Theorem. We have done two baby cases k equal to 2 and k equal to 3. These two cases were easy, but they tell us how we can do the general cases. So, k equal to 2 case just to go through that orally very quickly was that we first solve for two systems of solutions x1 congruent to 1 mod n1 and 0 mod n2 and x2 congruent to 0 mod n1 and 1 mod n2.

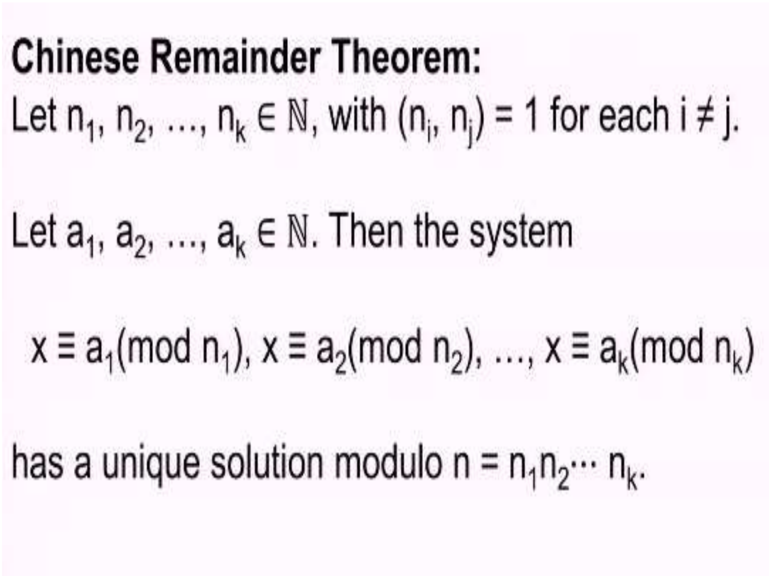
So the x1 which was 0 mod n2 directly gave you that x1 has to be a multiple of n2 and so we write it as n2 k1 and the first part of that system of simultaneous linear congruences would then ask you for solving for this k1. So we will then have a system n2 k1 congruent to 1 mod n1 and we are solving for k1 which is guaranteed because n1 and n2 are co-prime. Similarly, you solve for x2 because x2 is multiple of n1.

So x2 will be n1 k2 and then we are asking for n1 k2 congruent to 1 mod n2. So you can solve for k2 also and once you have solutions to these very special cases of simultaneous congruences you can solve the general case by taking linear combinations of these two. We have a similar situation when we had the case for k equal to 3, x1 was the system which was 1 mod n1 and 0 mod all others n2 and n3. So x1 was a multiple of n2 n3.

So we wrote x1 as n2 n3 k1 and we called that n2 n3 has C1 and then C1 n1 are co-prime because n1 had no common factor with n2 neither did it have a common factor with n3. So, n1 would have no common prime factor with the product n2 n3. So C1 and n1 are co-prime and therefore C1 k1 congruent to 1 mod n1 has a solution. Similarly, x2 was the special system where you had 1 mod n2 and 0 mod n1, 0 mod n3.

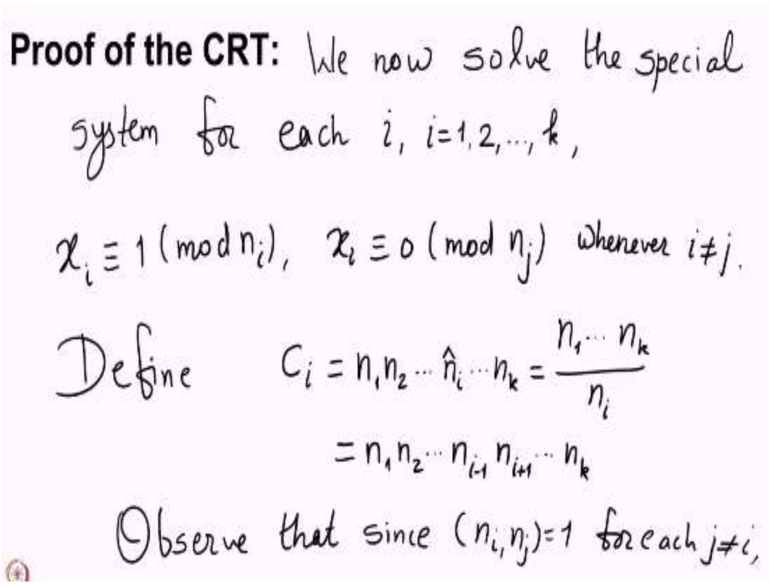
So, x2 should be a multiple of n1 n3 and then you solve for k2 because n2 n3 the product which we call n1 n3 the product which we call C2 is co-prime with n2 and then similarly we do x3 and so on. So we are going to do the general case now. Let me just remind you with the statement of the theorem. We have n1 n2 nk.

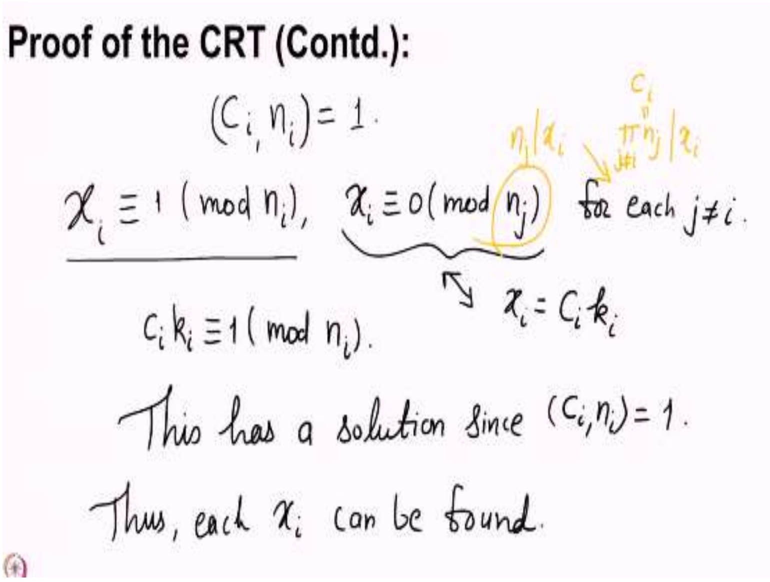
(Refer Slide Time: 03:09)



This is the case that we are now going to prove. We have a k tuple of natural numbers consisting of pair wise co-prime integers. We have another k tuple of natural numbers a1, a2, ak and we are asking for the solution to the system x congruent to a1 mod n1, a2 mod n2, ak mod nk. The uniqueness part will be seen later. So now we are going to prove this general case.

(Refer Slide Time: 03:37)





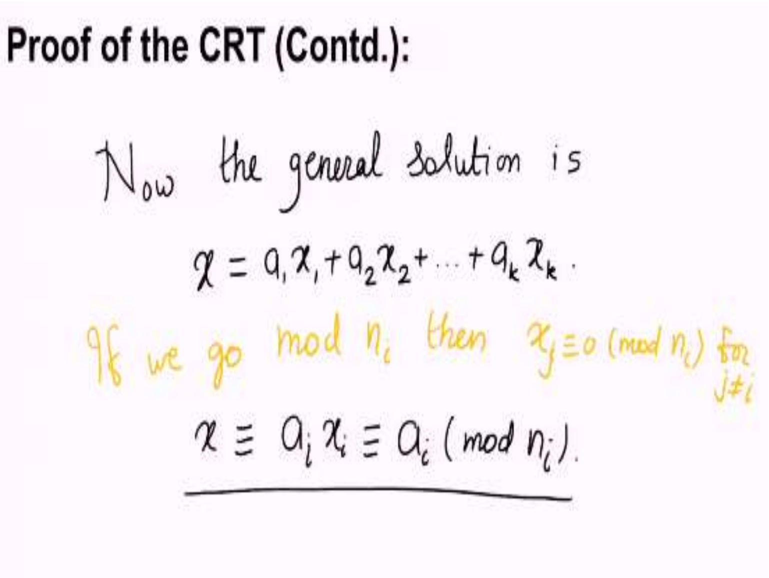
So we now prove or we now solve the special system for each i, i going from 1, 2, up to k and the special system is xi congruent to 1 mod ni and xi congruent to 0 mod nj whenever i not equal to j. So this was the system which we had in the last case, the case k equal to 3 where we had x1 which was 1 mod n1, 0 mod n2, 0 mod n3, x2 which was 1 mod n2, 0 mod n1, 0 mod n3 and x3 which was 1 mod n3, but 0 mod n1, 0 mod n2.

So similarly here we have this xi which is 1 mod ni and 0 mod nj whenever i is not equal to j. So if we define Ci to be n1, n2 dot, dot, dot ni hat dot, dot, dot nk. So here the hat means we are omitting this particular number, so what we are doing is that we are taking the product n1 n2 nk and dividing by ni okay or to make it more precise we are looking at the product n1 n2 ni minus 1, ni plus 1 up to nk.

We are looking at this particular product and now we observe that since ni with nj is 1 for each j not equal to i. So Ci and ni are coprime and let us again recall what we were looking at for xi, xi we wanted to be 1 mod ni and xi was 0 mod nj for each j not equal to i. So this condition tells us that this xi is a multiple of Ci because each nj wherever j is not equal to i would divide xi again for each j not equal to i and therefore the product nj where j not equal to i divides xi, but this is simply Ci by our definition of Ci.

So if we have that xi can be written as Ci times some integer ki and now we need to solve for this. So, we have Ci ki congruent to 1 mod ni, but this has a solution since Ci and ni are co-prime. So thus each xi can be found.

(Refer Slide Time: 08:03)

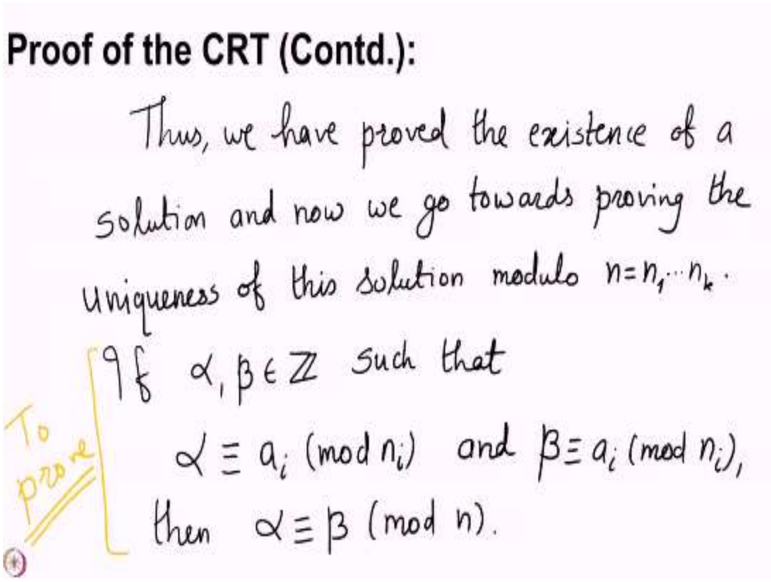


And now the general solution is x equal to a1 x1 plus a2 x2 plus dot, dot, dot ak xk. So, if you were to look at it modulo any particular ni so mod ni if we go then x is congruent to remember mod ni each of the xi where i is not equal to j is going to give you 0. So the only thing which survives in this is ai xi which is congruent to ai because xi is now 1 mod ni. So this is our solution to the general system of the simultaneous linear congruences.

So once again we solved very special systems which were giving 1 mod a particular ni and 0 mod all other njs. Then the solution will be multiple of the product of these njs and using the property that since each of the nj is coprime to ni the product of nj is also coprime to ni, we have a solution to that particular special system of simultaneous congruences and then we have a general solution.

So now that we have proved the existence of a solution we go towards proving the uniqueness. What is the meaning of uniqueness before that let me write what we have done and what we are yet to do.

(Refer Slide Time: 10:27)

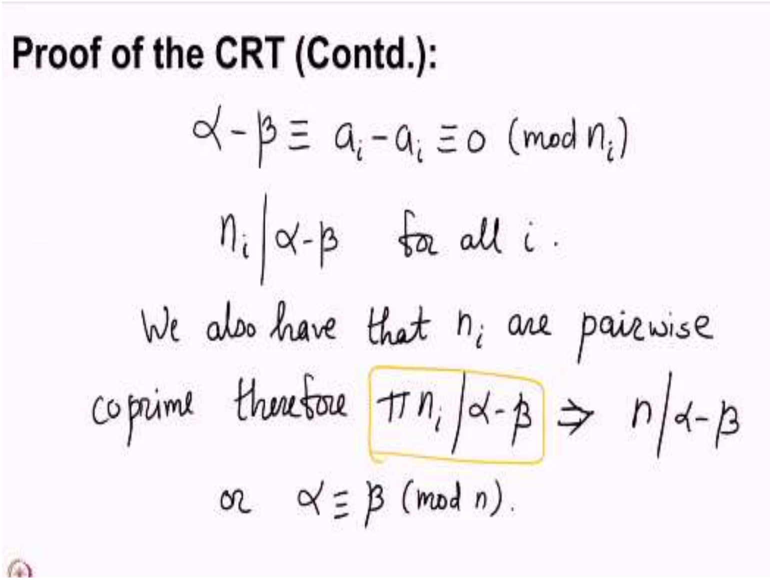


So, thus we have proved the existence of a solution and now we go towards proving the uniqueness of this solution modulo n which is the product of this k natural numbers. So what is the meaning to say that we are looking at uniqueness? It means that if you have two solutions. Suppose I have a natural number alpha which satisfies that simultaneous system of linear congruences.

So I would have alpha congruent to a1 mod n1, alpha congruent to a2 mod n2 so on up to alpha congruent to ak mod nk and suppose we have one more natural number beta satisfying the same then alpha and beta should be congruent to each other modulo n this is what we want to prove. So, let us write it if alpha, beta they exist in let say natural integers meaning why only natural numbers.

Such that alpha congruent to ai mod ni and beta also congruent to ai mod ni then alpha is congruent to beta mod n. This is the statement that we are to prove, this is the statement that we want to prove. So, let us see how one can prove such a statement.

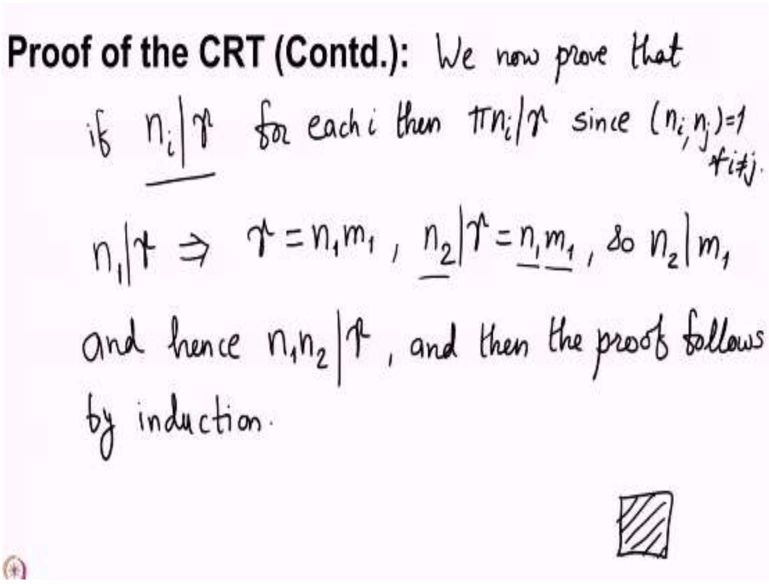
(Refer Slide Time: 12:57)



So since we want to show that alpha and beta are congruent modulo n we must look at alpha minus beta and we have that alpha is congruent to ai modulo ni and beta is also congruent to ai modulo ni. So mod each ni we are going to get that alpha minus beta is 0 and this is to say that each of the ni is going to divide the product alpha minus beta, but if ni divides alpha minus beta and we also have that ni are pair wise coprime.

Therefore, the product ni is going to divide alpha minus beta which says that n divides alpha minus beta or that we have alpha congruent to beta modulo n. So, let me make some comments about this particular statement that when you have some set of co-prime elements divide an element then the whole product goes and divides it. So, how do we think about this? So let me state that here and prove it for you.

(Refer Slide Time: 14:38)



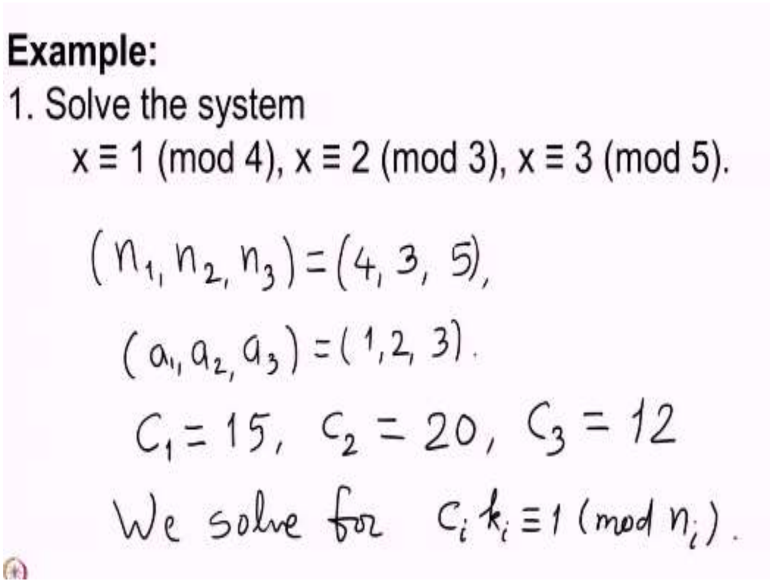
So we now prove that if ni divide gamma for each i then product ni divides gamma since ni nj is 1 or all i not equal to j. Okay so this tells us that first of all you have n1 dividing gamma and therefore gamma can be written as n1 into let say m1. Once you have written gamma as n1 m1 we consider the case that n2 divides gamma.

Once you have n2 dividing gamma, gamma is n1 m1. Now each prime factor of n2 will have to divide m1 because n1 and n2 are pair wise co-prime. So all the prime factors of n2 will divide m1 with the same power so n2 will divide m1 and hence the product n1 n2 divides gamma and then by induction then the proof follows by induction.

So the only thing to note here is that we have the fundamental theorem of arithmetic which guarantees that the primes occurring in a factorization are unique with the powers also being uniquely determined by the integer n that is the only thing which will give us all these solutions. So what we have now done is we have completed the proof of the Chinese Remainder Theorem.

We proved the existence of solution by proving the existence of solution for a very special case of simultaneous congruences and then we also have proved the uniqueness modulo n. So after having proved this impressive theorem the next thing to do is to try our hand at some problems. So we look at this particular problem to begin with.

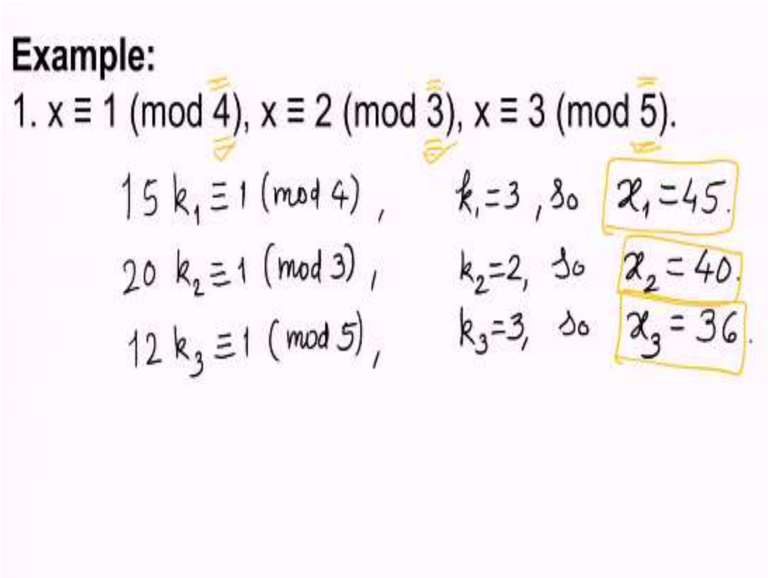
(Refer Slide Time: 17:15)



This systems says that we want to solve for x congruent 1 mod 4, x congruent to 2 mod 3 and x congruent to 3 mod 5. So, here our a1 is 1. Let us compute, let us write all our tuples so n1, n2, n3 are 4, 3, and 5 in that order and clearly we have that they are all pair wise co-prime then we have a1, a2, a3. So, these are 1, 2, and 3 and then if you remember the proof that we had done we had actually looked at C1, C2, C3. So C1 was n2 n3.

Therefore, this is 15, C2 was n1 n3. So that is here 20 and C3 was n1 n2 so that product is 4 into 3 which is 12 and then once again we observe that 4 and 15 are co-prime, 3 and 20 are co-prime and 5 and 12 are co-prime. So we construct three systems from this where we are asking for inverse of each of these Ci modulo ni. So we solve for Ci ki congruent to 1 mod ni. This is the system that we are going to now solve first. So 15, 20 and 12 modulo 4, 3 and 5.

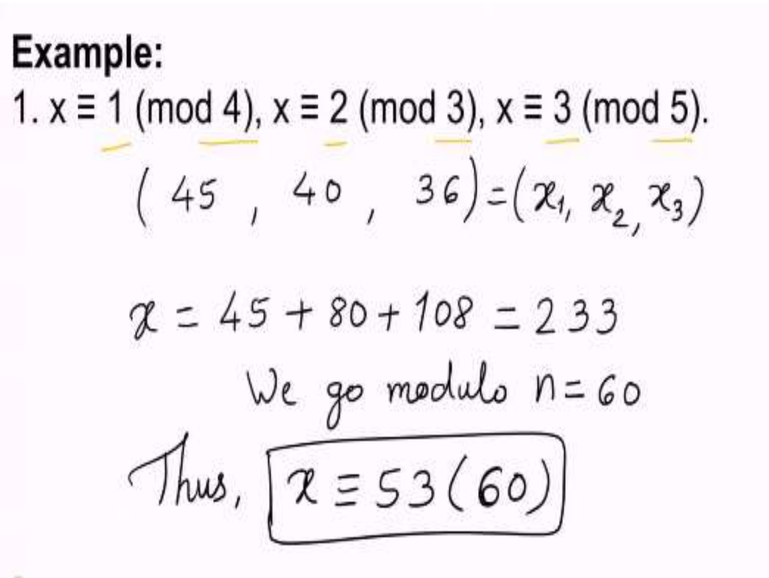
(Refer Slide Time: 19:05)



So the first one is the product of these two so 15 k1 congruent to 1 mod 4 and then we see this quite easily that here k1 has to be 3. So, x1 equal to 45. After that we look at 4 into 5 which is 20 k2 congruent to 1 mod 3 which will give us so remember 20 itself is congruent to 2 mod 3. So if I multiply 20 by 2 I get 40 which is congruent to 1 mod 3. So k2 is 2 and x2 is 40 and similarly we solve for x3 by asking for 12 k3 congruent to 1 mod 5 and then we observed that k3 is 3.

So we have x3 equal to 36. We can quickly observe that each of these have the required properties that 45 is divisible by 5 and 3 and is congruent to 1 mod 4. Similarly 40 is divisible by 5 and 4, but is congruent to 1 mod 3 and 36 is divisible by 4 and 3 and is congruent to 1 mod 5.

(Refer Slide Time: 21:04)

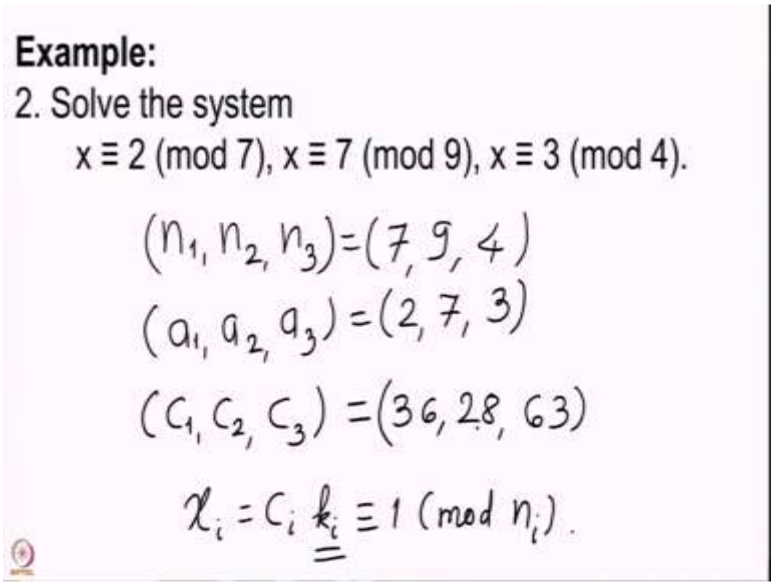


So let me write it here once again we have 45, 40, and 36. These are the values of x1, x2, x3 and to compute the final answer we have to simply multiply the xi by ai and compute the final answer. So x is 1 into 45 that is simply 45 plus 2 into 40 that is 80 plus 3 into 36 which gives you 108. So, we have 5 plus 8 gives you 13 so you have 1 coming out and then 8 plus 4 is 12 plus 1 gives you 13 so you have 3 and 1 more coming out.

And then finally you have 233, but we should also go modulo the product of the 3 moduli which we have here, so 4 into 3 into 5 which is 12 into 5 which is 60 and thus our answer is x is congruent to 53 mod 60. So I will just write 60 here and we can easily check that when we go modulo this is what we always tell all the school students that once you have computed the answer you should check it again.

So when you go modulo 4 for 53 you see that 52 goes out and what is remaining is 1. When you go mod 3 you see that 51 is subtracted and what is left is 2 and when you go modulo 5 then from 53 you subtract 50 and what you are left with is 3. So the answer is indeed 53 mod 60. Let us do one more problem before we finish this lecture.

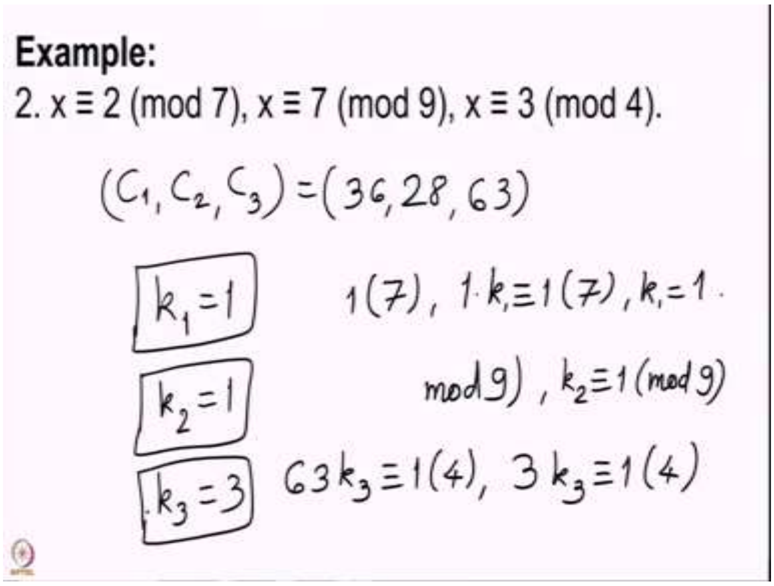
(Refer Slide Time: 23:02)



So this problem is similar. We want to solve this system of the simultaneous linear congruences and I will now be slightly fast because you know the method already. So you will write n1, n2, and n3 in the order 7, 9, and 4 and we have a1, a2, and a3 which are nothing but 2, 7, and 3 and then finally we need to compute C1, C2, C3. So, remember once again C1 is the product of n2 n3 so this is now 36.

C2 is the product of n1 and n3 which is 7 into 4 so that is 28 and C3 is n1 n2 which is the number 63. So, now we want to solve for xi to be Ci ki congruent to 1 mod ni. This is the solution. So, we need to solve for the k. So, we go to the next slide, but remember we have 36, 28 and 63 as the Ci.

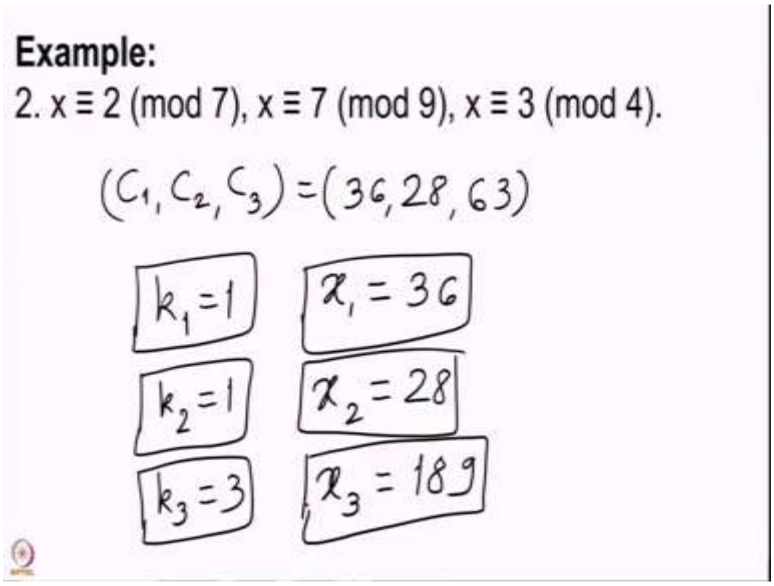
(Refer Slide Time: 24:27)



So C1, C2, and C3 are 36, 28, and 63 and I want to solve for k1. So k1 should give me the property that 36 k1 should be 1 mod 7, but 36 is already 1. So we have that this is 1 into k1 congruent to 1 modulo 7 and therefore k1 is 1. So, I get the final answer is that k1 is 1. I will solve similarly for k2 which should have the property that 28 k2 should be congruent to 1 modulo n2 which is 9, but 28 already is 1 mod 9.

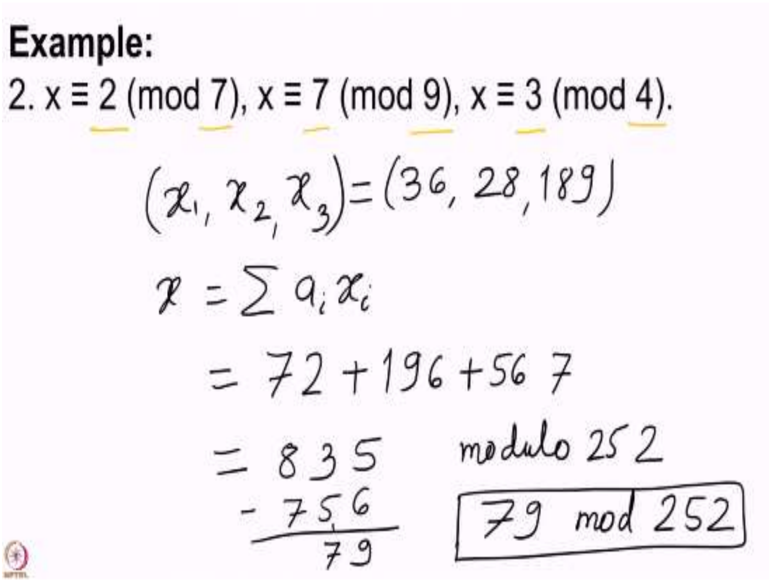
So this gives me k2 congruent to 1 mod 9 and therefore k2 is 1. So we get k2 also to be equal to 1. We should now solve for k3 with the property that 63 k3 is congruent to 1 mod 4, but 63 is 3 so we should solve for 3 k3 congruent to 1 mod 4, but 3 k3, the k3 should be equal to 3 because 3 into 3 is 9 which is 1 mod 4 so k3 has to be equal to 3. So these are the values which we obtain for k1, k2, k3 and from these we should now obtain the xi, x1, x2, x3. Remember x1 is C1 k1, x2 is C2 k2 and x3 is C3 k3.

(Refer Slide Time: 26:38)



So x1 is 36 into 1 therefore this is 36, x2 is 28 into 1 so that is simply 28 and x3 is going to be 63 into 3 so I hope you have your multiplication tables with you it gives you the number 189. So 36, 28, and 189 these are the x1, x2, x3.

(Refer Slide Time: 27:09)



36, 28 and 189 this is x1, x2 and x3 and now what we should do to compute the final answer is to take x to be summation ai xi. So I will multiply to 36 by 2 I get 72 then to 28 I multiply by 7 so 28 into 7, 28 is already 7 into 4, so that gives us 49 into 4 and 49 into 4 is 200 minus 4 because 50 into 4 is 200 so we get it to be 196 plus 189 into 3. So this is the product that we have to do in our head.

9 into 3 gives us 27 so we have 7 and then there are 2 left and 18 into 3 are 54 and we add those two to get 567. So the final answer here is 7 plus 6 is 13 plus 2 is 15, so we write 5 and 1 is left, 6 plus 1 is 7 plus 9 is 16 plus 7 is 23 so we have 3 and then there are 2. So 5 plus 2 is 7 and 1 8. 835 this is the answer, but we have to go modulo the LCM which is 9 into 7, 63 into 4, 63 into 4 is 252.

So, we need to subtract multiples of 252 from this number. We multiply 252 by 3 to get 756 after subtracting this from this we get 5 makes 15 minus 6 is 9, you have 1 here 383 minus 76. This becomes 7. So the answer is 79 mod 252. Let us just verify quickly that 79 is indeed the answer. So, when you go modulo 7 to 79, 11 into 7 are 77 and what we are left with is 2. When you go modulo 9 you will remove 72 what is left is 7.

And when you go modulo 4 of course 76 are removed and what is left is 3. So, we have successfully applied the Chinese Remainder Theorem to apply these two systems of linear congruences. What we are going to do in the next lecture is to look at some more complicated systems and try to use Chinese Remainder Theorem by doing some modifications to the system. So I hope to see you in the next lecture. Thank you.