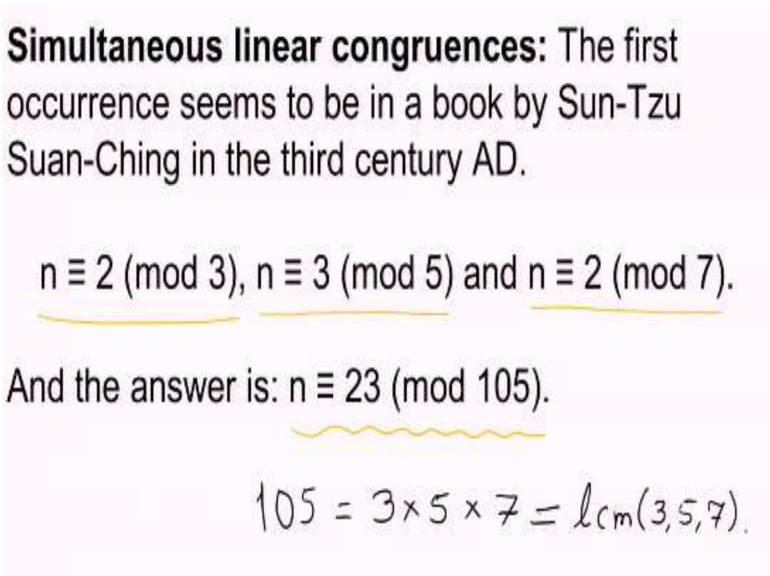
**A Basic Course in Number Theory**
**Professor Shripad Garge**
**Department of Mathematics**
**Indian Institute of Technology, Bombay**
**Lecture 17**
**Chinese Remainder Theorem the Initial Cases**

Welcome back. We are discussing about solving the system of simultaneous linear congruences. So I told you that this, the corresponding result the main result in this theory is called the Chinese Remainder Theorem. Remainder ofcourse stands for the ai's that we have. So, what we are really looking for is a number x such that whenever you divide by ni the remainder should be ai, this is the problem.

And the first occurrence until now is in the third century AD and that was from China and that is why it is called Chinese remainder theorem.

(Refer Slide Time: 01:02)



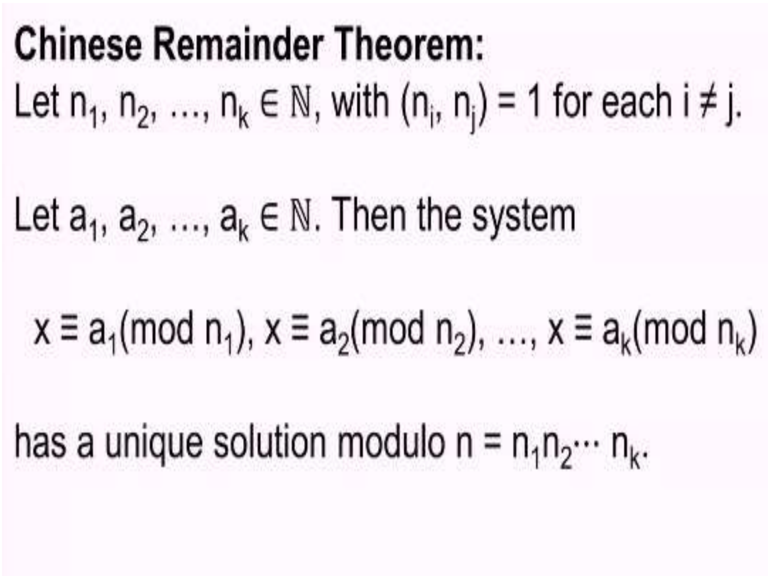

So as we can read it here it is in a book by Sun-Tzu Suan-Ching and the problem was an elaborate problem, but in the mathematical lingo this translates as asking for a solution for a natural number n which is congruent to 2 mod 3. So when you take out groups of 3 what is left is 2 it is 3 mod 5. So when you take out groups of 5 what is left is 3 and finally it is 2 mod 7.

So we solved this in the last lecture and we observed that the solution is 23 you can ofcourse add 105 to it so you have that 128 is also a solution. We just observe here that the number 105 is obtained as the product of these 3 moduli. The modulus 3 into the modulus 5 into the modulus 7 this is what we have. In general this is actually going to be replaced by what is called the LCM of these 3 numbers.

At the moment since these 3 numbers are pair wise co-prime therefore their LCM is nothing but their product. But when we see a general theory maybe 2 lectures on or 3 lectures later we will see that this product is going to be replaced by the LCM. So this is the statement of the theorem so statement that we have seen the problem and its solution let us now go towards the statement of the theorem.

It is an important theorem I am going to show it to you line by line and let us try to understand each line correctly.

(Refer Slide Time: 02:55)




So we start with n1, n2, nk these are natural numbers and the condition on them is that ni, nj is 1 whenever you have i not equal to j. So that means that pair wise these integers are co-prime this is the only condition and that is why and using only this condition we are going to get our result. So we have k tuple of natural numbers consisting of pair wise co-prime integers.

We start with any k tuple of integers a1, a2, ak so here there is no condition and now we ask for the solution of the system x congruent to a1 mod n1, x congruent to a2 mod n2 so on up to x congruent to ak mod nk. So, we want one single natural number which when we take out multiples of n1 common will give you the remainder a1. When you take out multiples of n2 out gives you the remainder a2 and so on up to kth stage where you are taking multiples of nk out the remainder is ak.

Once again note that there is no condition on a1, a2, ak. The only condition is on n1, n2, nk and the condition is that they be pair wise co-prime. Meaning if I take n1 and n2 then there is no common factor n1, n3 have no common factor so on up to n1, nk have no common prime factor then n2, n3 have no common prime factor n2, n4 have no common prime factor n2, nk have no common prime factor.

And the last pair that you will get is nk minus 1 and nk those two natural numbers also have no common prime factor. This is the only condition we have then this system has a unique solution we are not saying that there is a solution we even say that it has a unique solution modulo the product n which is n1, n2, nk this is the statement that we have we will prove this statement the proof is actually quite simple.

But there is one basic idea in the proof and so we will do some of the simpler cases of this theorem where k is 2 and k is 3 and then we will do the general result, but before doing any such thing you may wonder whether there are any applications of this result meaning number theory is it used to be the branch of mathematics which had no applications and Professor G. H. Hardy whose name has come up once before when I told you about the method of contradictions he had a book an Apology of a Mathematician.

So in the same book he also says that he is quite proud of the fact that number theory has no applications. So he was of the opinion that one should study only for the purpose of studying, it should not get clouded by these materialistic ambition. So he would say that you should not look at applications, you should study because the theory is beautiful, you should study because you like it.

So number theory used to be one such thing but ofcourse now with the advance of cryptography and so on there are plenty of applications of number theory, but let us go and look at one application of this particular theorem the Chinese remainder theorem and the application is as follows it is in astronomy. So the application is as follows.

(Refer Slide Time: 06:37)

**Applications in astronomy:** If k events occur regularly, with periods $n_1, n_2, \ldots, n_k$, with the i-th event happening at the time $x = a_i, a_i+n_i, \ldots$, then the k events occur simultaneously when

$$x \equiv a_i \pmod{n_i} \quad \text{for all } i.$$

If the periods $n_i$ are pairwise coprime then such an x can be found.

This may have been the motivation behind the CRT

Consider the situation where you have k events occurring regularly and the periods are n1, n2, nk. So there are these k events which occur regularly this event can be anything. So it can be a solar eclipse or lunar eclipse or I do not know if you remember, but when I was a child this there was this comet called Halley’s Comet and apparently this comet which circulates the solar system will come back and go pass through a distance which is closest to Earth every 76 years.

So there are these astronomical events and many of them are periodic events there is some nice definite periodicity which one can compute and so here we assume that there are these k events which occur regularly with these period n1, n2, nk. So if you had the first event occurring at some time then the next time it would occur would be at so suppose you are with the Ith event happening at the time x equal to ai.

So, suppose you have started counting with the Gregorian calendar and then in 2020 some event occurs and then the period of this thing occurring again we say 35 years. So in 2055 it will occur again so that is what we have as ai and then ai plus ni and then it would continue occurring regularly with respect to those period. So you have these k events occurring regularly with periods ni and we assume that ai, ai plus ni and so on these are the times when they are occurring.

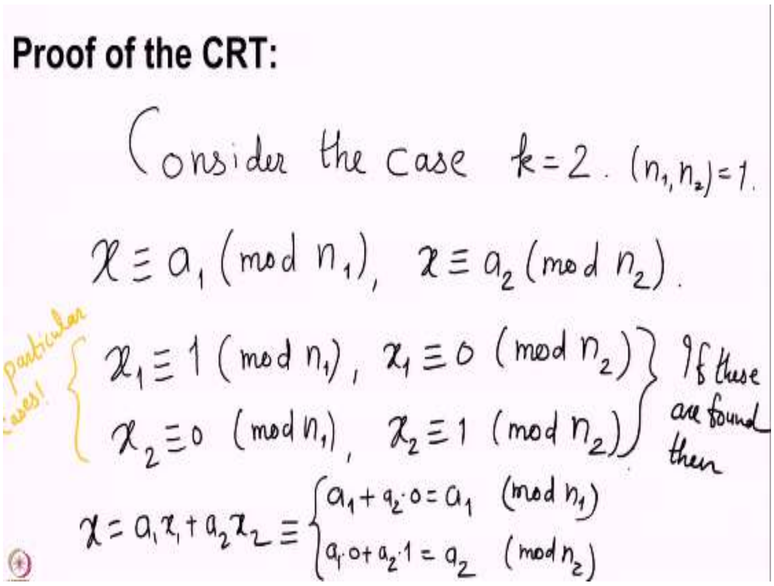
So when you go modulo ni the occurrence is x congruent to ai this is what we have and then you would ask for the simultaneous occurrence of this. This was an event which was of interest to astronomers when some particular set of events occur simultaneously. So this is solvable when you have these congruence moduli ni to be co-prime.

So if these periods ni happened to be pair wise co-prime then ofcourse such an x can be found and the ancient people of possibly all civilizations knew about this result and this is one event which could even be the motivation behind studying the Chinese remainder theorem. I believe that it could be one of the motivations behind the Chinese remainder theorem.

So what we are looking here is that when you have these k events occurring regularly with periods ni the first one occurring at ai then ai plus ni and so on then the occurrence is the simultaneous occurrence would be given by a solution to the simultaneous the system of simultaneous congruences x congruent to ai mod ni for all I and if these ni are pair wise co-prime then ofcourse you can simply write down and find the solution.

Many times in various proofs the solution is proved only up to existence, but we will see that with some techniques we can actually construct a solution. So now we are going to prove the Chinese remainder theorem let us walk through this proof together it is a simple proof, but there is one key idea so once you understand this key idea then the proof really becomes transparent.

(Refer Slide Time: 10:17)



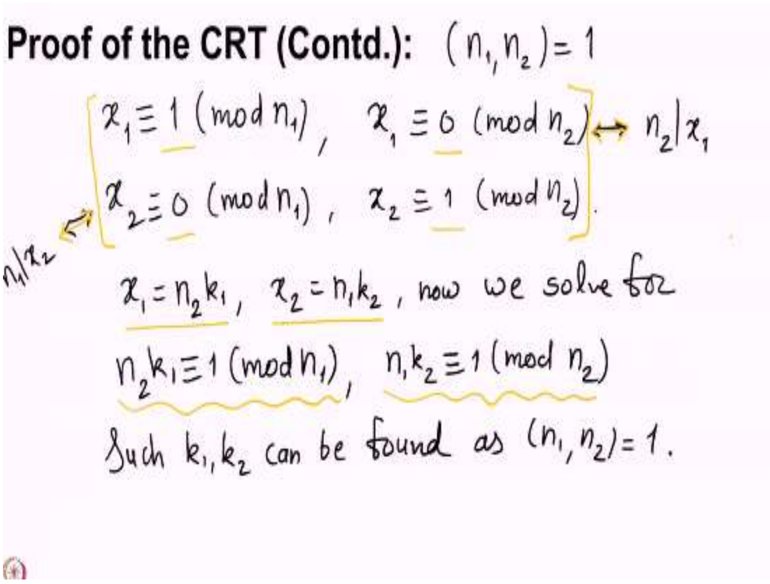

So, let us begin this proof what we are going to do to begin with is to consider the case k equal to 2. So what we are asking for is that we are interested in finding a solution to this system. Here of course we have n1 and n2 to be co-prime. So we are looking at pair wise co-prime and here we have a single pair. So we are asking that whenever n1 and n2 are co-prime do we have a solution to this.

Now here we are once again I will remark that we are looking at a1, a2 to be any tuples any pairs of natural numbers, but I will first try to get solution for this particular tuple. So I am asking for solution for x1 congruent to 1 mod n1 and x1 congruent to 0 mod n2 and another system where I am asking for the solutions to this. So I am looking at two particular cases so these two are particular cases of the above problem.

But if we have a solution to these so if these are found then I will simply take x to be a1 x1 plus a2 x2. So, assuming that there is a solution x1 and x2 satisfying these various conditions with the assumption we can solve a general equation. So if you are going modulo n1 then here x1 is 0 mod n2 and a2 is x2 is 1 mod n2. So, let us look at this modulo both n1 and n2. So when I am going modulo n1 modulo n1 (a) x1 is 1.

So this is going to be a1 times 1 plus a2 times 0 and therefore it gives me a1 and similarly for x2 we are going to get a1 modulo n2. Modulo n2 means we have to look at this particular part. So from here we see that modulo n2 x1 is 0 so I will get a1 n2 0 plus a2 n2 x2 which is 1 and therefore we get it to be a2. So once we have solution to these two particular cases then we are able to solve the equation. So we go to the next page and solve these two particular cases.

(Refer Slide Time: 14:28)




So we have n1, n2 equal to 1 and we are now going to solve for x1 congruent to 0 sorry x1 is congruent to 1 mod n1 and x1 is 0 mod n1 and when we look at x2 we demand that this be 0 mod n1 and x2 be congruent to 1 mod n2, but this second condition is equivalent to n2 dividing x2 and this n2 dividing x1 and this condition is n1 dividing x2.

So what we get is that x1 is of the type n2 k1 and x2 is n1 k2 and so now we have to solve n2 k1 which is x1 congruent to 1 mod n1 and x2 which is n1 k2 congruent to 1 mod n2 and such case k1 k2 can be found as n1 n2 is 1. So let us go through this proof once again. What we are asking for is to solve these two special cases x1 which has the property that it is 1 mod n1 and 0 mod n2 and x2 has the property that it is 0 mod n1 and 1 mod n2.

And we saw in the last slide that when you have solutions to such an x1 and x2 you can solve for a general x by simply putting it as a1 x1 plus a2 x2 gives a general solution. This is something that we have seen. So we want to solve only for these two special cases of our system of simultaneous congruences and then this immediately told us x1 congruent to 0 mod n2 says that n2 has to divide x1.

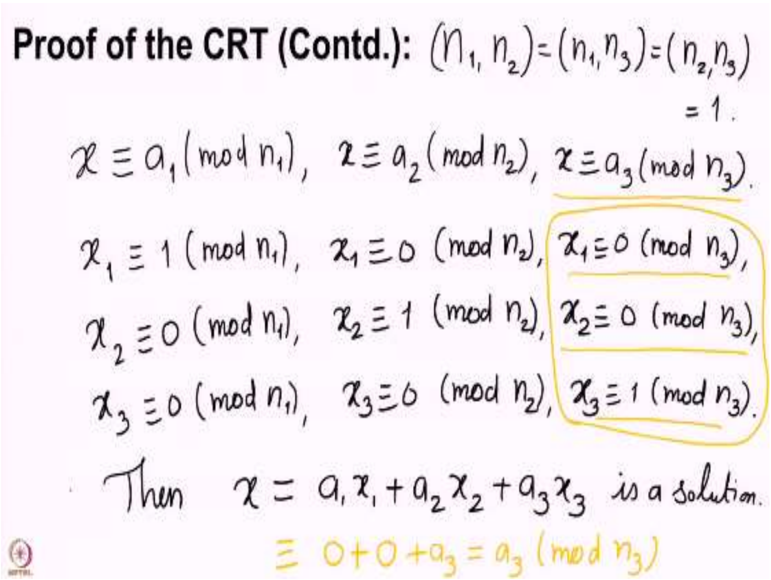
And therefore x1 is of the form n2 times some k1 and similarly x2 congruent to 0 mod n1 will tell you that x2 has to be of the form n1 times k2. So, the congruence x2 congruent to 0 mod n1 is solved because we are looking at x2 to be only multiples of n1. So by looking at we have solved this particular congruence the only congruence that remains to solve is this x2 congruent to 1 mod n2.

Similarly by taking x1 to be a multiple of n2 this congruence is solved and so we have to only solve the first congruence which is x1 congruent to 1 mod n1 so those things are now encoded here. So this is x1 congruent to 1 mod n1 x2 congruent to 1 mod n2, but n1 and n2 are co-prime and we know from the system of solution of a linear congruence that when you have GCD of the coefficient of x and the modulus dividing the constant term then you have a solution and the number of solutions is exactly the GCD.

Here you have n1, n2 are coprime so the GCD is 1 therefore you get a solution and since the GCD is 1 your solution is unique modulo that n1, but anyway the uniqueness will come later. We at least have a solution for x1 and solution for x2 by having computed k1 and k2 so when we deal with some particular problems we will need to compute these k1 and k2.

So k1 has the property that multiplied to n2 it gives you 1 mod n1 and k2 has the property that multiplied to n1 you get 1 mod n2. So once you solve this then you have a system then you have a solution to the simultaneous system of linear congruences. Let us do one more case we want to generalize these two k events, we want to generalize these two k tuple n1, n2, nk let us do it for 3 and then we go on to do the general case.

(Refer Slide Time: 20:10)




So here we have n1, n2 equal to n1, n3 equal to n2, n3 which is 1 and we are looking for solutions to x congruent to a1 mod n1 x congruent to a2 mod n2 and x congruent to a3 mod n3. Once again like the last time we are going to look at three special cases. Our first special case is x1 which is congruent to 1 mod n1, but it is 0 mod n2 and 0 mod 3. This is our first special case x2 is the one which has congruence 1 when you divide by when you go modulo by n2 and otherwise you get 0.

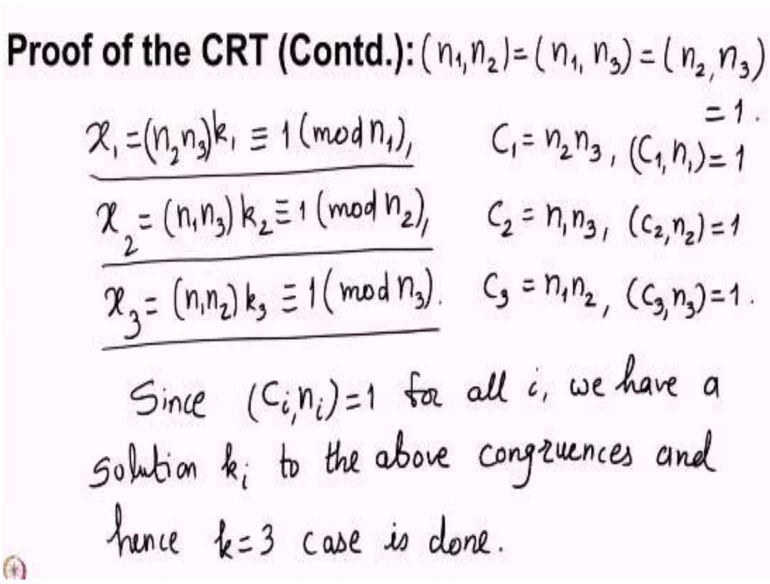
And finally we have x3 which will give you 0 when you divide by n1 it will give you 0 when you divide by n2, but it will give you 1 when you divide by n3 and then once you have a general solution then x which is a1 x1 plus a2 x2 plus a3 x3 is a solution because when I go modulo n1 so let us do this for one congruence at a time.

So this is going to be if I am going modulo n1 then modulo n1 x1 is 1, so I will get a1, x2 is 0 so I do not get anything for a2, x3 is 0 so I do not get anything for a3. So this is the congruence when I go modulo n1 which is what we wanted. We wanted to have x to be a1 mod n1. Now suppose we want to do it for n3 instead of n2 so the similar things would work for all the other moduli.

Suppose I want to go mod n3 so I have to look at this particular column of congruences. So x1 is 0 mod n3 therefore a1 x1 will give me 0 x2 is 0 mod n3 so a2 x2 this will give you a2 times 0 and finally x3 is 1 so I get a3 times 1 which is simply a3 mod n3 and this is what we wanted to obtain. So these three very special systems of simultaneous linear congruence will give you a general solution to a system of simultaneous linear congruences.

So now we have to solve for each of these three. So x1 congruent to 1 mod n1 and 0 mod n2, n3, x2 congruent to 1 mod n2 and 0 mod n1, n3 and x3 congruent to 1 mod n3 and 0 mod the first two n1, n2 this is to be solved.

(Refer Slide Time: 24:27)




So let me just write it here again that we have these three to be co-prime and we are looking at. So because x1 is 0 mod n2 and x1 is 0 mod n3 we have that x1 is n2, n3 times a k1 and we want to solve for 1 mod n1. So we have these n2, n3 then we look at x2 which is n1, n3, k2 because we would have that x2 is 0 mod n1 and 0 mod n3, but 1 mod n2. So x2 is divisible by n1 and n3.

So we have x2 to be n1, n3 k2 congruent to 1 mod n2 and finally we will solve for x3 to be n1, n2, k3 which we ask to be congruent to 1 mod n3. So all these numbers that we have in the bracket so call C1 to be product n2, n3 C2 to be the product n1, n3 and C3 to be the product n1, n2 then we observe that C1 and n1 are co-prime because n1 has no common prime with n2 and n1 has no common prime factor with n3.

So C1 which is nothing, but the product of n2 and n3 is going to be co-prime with n1. Similarly C2 n2 are co-prime and C3, n3 are co-prime. So once you have these co-prime things then we know that there is a unique solution to this, there is a unique solution to this, there is a unique solution to this modulo each of the ni. So since Ci ni is 1 for all i we have a solution ki to the above congruences and hence k equal to 3 case is done.

So we have done the case k equal to 2 where we had a pair of co-prime integers n1 and n2 and then we proved the Chinese remainder theorem for this particular case then we have now the case k equal to 3 where we had three elements, three natural numbers n1, n2, n3 and they had the property that they were relatively pair wise relatively prime or pair wise co-prime and then we proved that there is a solution to x congruent to a1 mod n1, x congruent to a2 mod n2 and x congruent to a3 mod 3.

Now the time is to go for a general prove, but we will do it in the next lecture. So, I hope you will remember the cases k equal to 2, k equal to 3 and see you in the next lecture. Thank you.