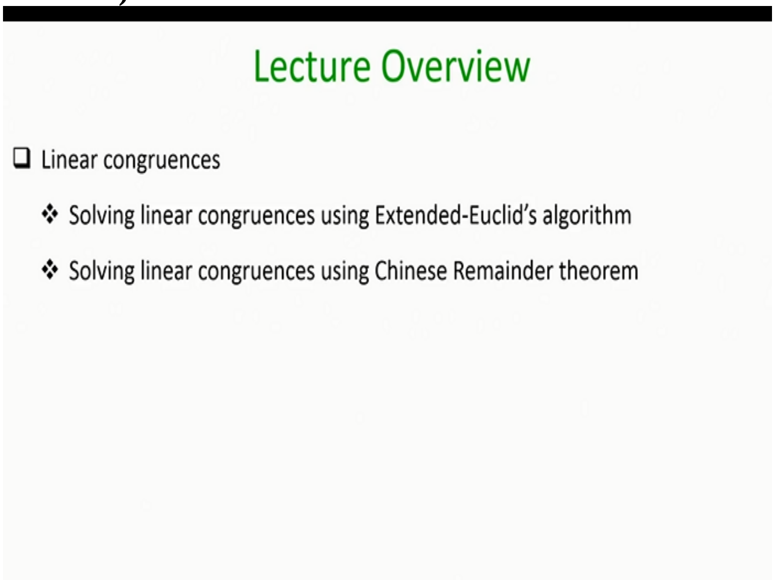
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology, Bangalore

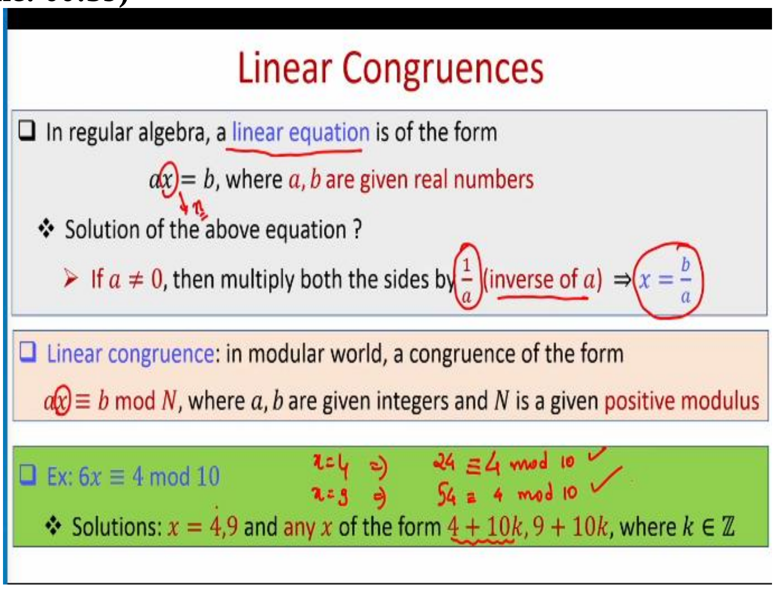
Lecture – 58
Linear Congruence Equations and Chinese Remainder Theorem

(Refer Slide Time: 00:21)



Hello, everyone, welcome to this lecture, the plan for this lecture is as follows: in this lecture, we will introduce linear congruences. And we will see 2 methods for solving linear congruences one using extended Euclid's algorithm and another one due to the famous Chinese Remainder Theorem or CRT.

(Refer Slide Time: 00:39)



So, let us start with linear congruences so, in regular algebra, you often come across linear equations of the forms a times x = b, that means you are given some real numbers a and b, and you have to find out the value of this unknown variable x such that this condition is satisfied. And how do we find out the solution for the above equation; by solution of the above equation, I mean to find out the value of this unknown x.

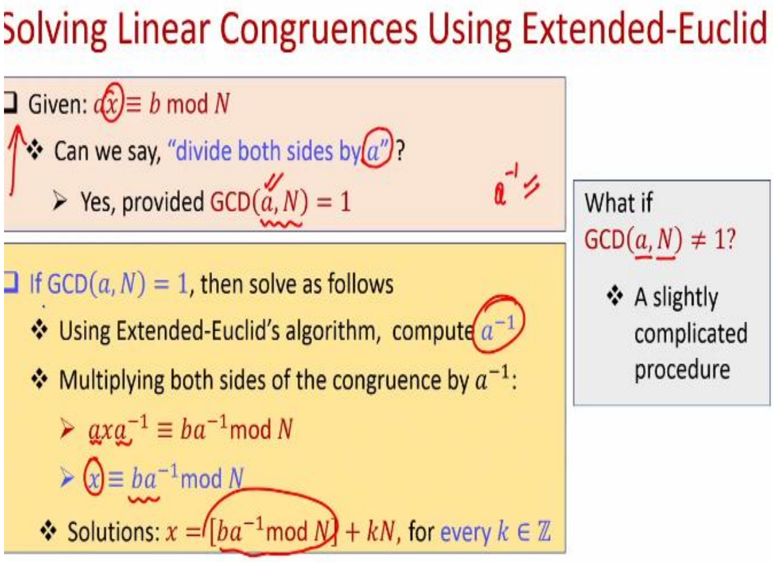
And if you know that the value of a is not 0 then I can say that, if you multiply both sides by 1/a, and 1/a is considered as the inverse of a in your regular algebra, then I say that x = b/a. That is a solution for your linear equation here. Now, when I say linear congruence, we are more or less in the same situation except that we are in the modular world, that means everything is given some modulus.

So, we will be given some a and b and a modulus N and our goal will be to find out x such that $ax \equiv b \bmod N$ and that means x when divided by N and b when divided by N gives the same remainder, you have to find out the value of x, or equivalently ax - b is completely divisible by N. So, for instance if I say that I am given 6x congruent to 4 modulo 10 and if I want to find out the value of x then the possible solutions are x = 4 because if x = 4 then you get 24 congruent to 4 modulo 10 which is true.

Because 24 - 4 is completely divisible by 10, If you substitute x = 9, then you get 54 congruent to 4 modulo 10, which is again true, because 54 - 4 is 50, which is completely divisible by 10. And it is not the case that these are the only solutions, you have infinite number of solution. That means any number of the form 4 + 10k, where k can be either positive or negative will also satisfy this linear congruence.

In the same way, every number of the form 9 + 10k, where k can be either positive or negative will also be a solution of this linear congruence. So, that is an interesting thing unlike regular algebra, where the solution was just b/a, of course you can also say 2 times b over 2 times a is also a solution, 3 times b over 3 times a is also a solution but more or less their primitive form is b over a. In the same way, the primitive solutions, primitive in the sense the base solutions are 4 and 9. And now you can create infinite number of solutions out of these 2 solutions by adding all multiples of 10.

(Refer Slide Time: 03:52)



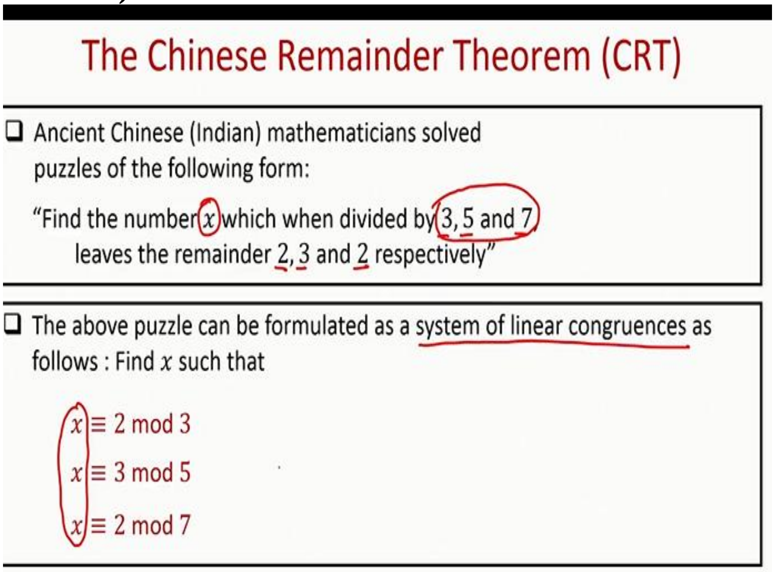
So, now let us see how we can solve linear congruences using extended Euclid's algorithm that is our method number one. So, you are given a, b and N, goal is to find out this unknown x. Now, as we did for our equation in the linear algebra where we said that divide both sides by a provided a is not 0. The question is can we do something similar in the modular world as well that is can we say divide both sides by a. And divide both sides by a by that I mean multiplying both sides by multiplicative inverse of a.

And that is possible only if GCD(a, N) is 1. So, remember, in the earlier; in the last lecture, we proved that the multiplicative inverse modulo N exists only if the number for which you want to find out the inverse is co-prime to your modulus. So, if your number a is co-prime to your modulus N, then I know that a^{-1} exists. And hence I can say that multiply both sides by the multiplicative inverse. So that is the method of solving linear congruence under this restricted condition.

So, if your GCD(a, N) is 1 then by running the extended Euclid's algorithm, compute the multiplicative inverse of a namely b, I stress that it is not 1/a in the modular world it is an integer. And now I multiply both the sides of this linear congruence by this a^{-1}. So, I will get this linear congruence and I know that a into a^{-1} is 1 modulo N and 1 into x modulo N is x. So, I get that x is congruence to b^{-1} modulo N that means; I can say that the value of x being this plus any multiple of N is a solution for this linear congruence ($x = [ba^{-1} \bmod N] + kN$).

Because all these values of x minus this value ba^{-1} is completely divisible by a. However, this method will work only if your number a is co-prime to your modulus N. What if the number a is not co-prime to your modulus N, then we have to follow a slightly different approach which is complicated and I am not going to discuss that matter.

(Refer Slide Time: 06:31)

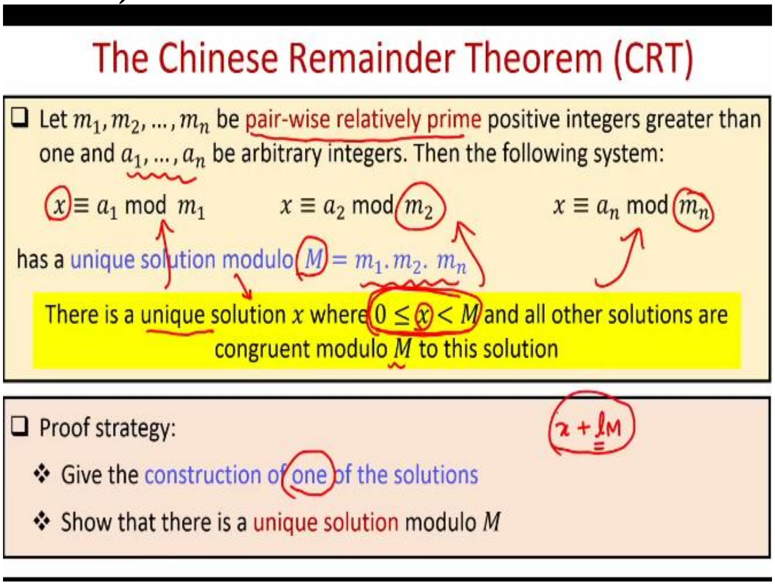


Instead I will discuss another way of solving linear congruences; in fact, a set of linear congruences and this method is often called as the Chinese Remainder Theorem attributed to the ancient Chinese but it is also believed that the ancient Indian mathematicians also used the same technique for solving a system of linear congruences. So, what exactly we mean by system of linear congruences.

So, very often you come across a puzzle of the following form you have an unknown number x which is not given to you, but it is given to you that unknown number x has a property that when it is divided by 3, it gives you the remainder 2, when divided by 5 it gives you the remainder 3 and say when it is divided by 7 it gives you the remainder 2. Under this condition, find out the value of x of course, again you can find out infinite number of x satisfying this condition, but what the CRT method says is it gives you at least one x which satisfy this condition.

And then from that you can find out the other values of x as well, so the above puzzle, above instance of the puzzle can be formulated as a system of linear congruence namely, my goal is to find out an unknown x satisfying the linear congruence that it is congruent to 2 modulo 3 it is congruent to 3 modulo 5 and it is congruent to 2 modulo 7. And the special property of this problem instance is that you are given the value of x modulo various modulus, those individual modulus are pairwise co-prime.

(Refer Slide Time: 08:10)



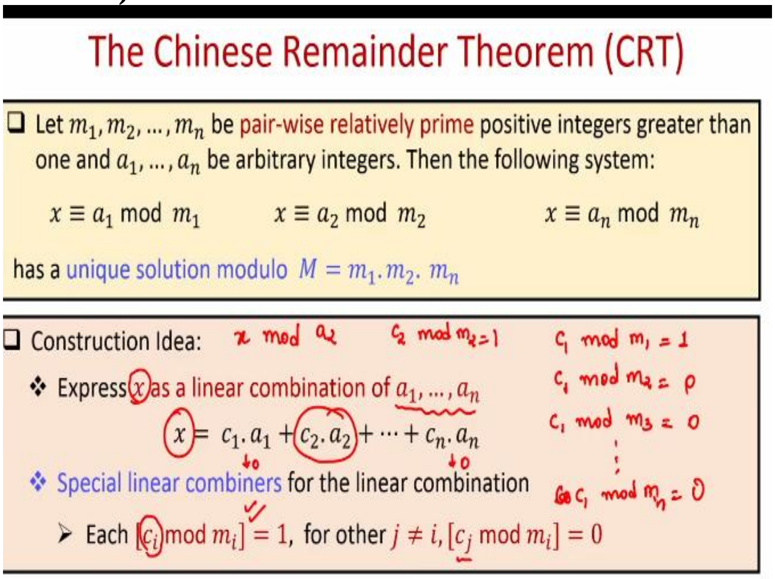
So, let me now formally state the theorem statement of Chinese remainder theorem and then we will prove it. So, you are given n different modulus which are pairwise relatively prime, that means, you take any pair of modulus m_i and m_j they are co-prime to each other. And you are given n number of remainders a_1 to a_n. So, you have to find out an unknown x which is congruent to a_1 modulo the first modulus, it is congruent to a_2 modulo the second modulus, it is congruent to a_n modulo the last modulus.

Now, what is the Chinese Remainder Theorem : it says that this system of n linear congruence has a unique solution modulo the bigger modulus and what is the bigger modulus it is defined to be the product of n modulus. So, in other words, what does it mean unique solution by unique solution I mean that there is only one value of x in the range 0 to M-1 which satisfies simultaneously all the n linear congruences but that does not mean there are there is only one solution in this range.

But there can be other solutions as well outside this range, in fact there are other infinite number of solutions and what you can say about other solutions: they are obtained by adding various multiples of M namely they are congruent to modulo M to this solution x which is in the range 0 to M-1. So, we now want to prove the Chinese Remainder theorem and there are multiple things which we have to prove, the proof strategy is as follows, we will give the construction of one of the solutions in the range 0 to M - 1.

But that does not mean that is a unique solution, remember there are 2 parts of the proof, we have to show that there is at least one solution in the range 0 to M - 1 which we will be doing in this lecture. And then we also need to show that, that is the only solution you cannot have any other solution in the range 0 to M – 1. That we will do in the next lecture. By the way, when I say unique solution again and again, I am stressing unique solution modulo M that means unique solution in this range, Outside this range if x is a solution, any number of the form x + *l* times m, where *l* is positive negative will also be a solution of this system of linear congruence. But these values, these solutions will be outside the ranges of 0 to M -1. So, do not get confused in this term unique solution.

(Refer Slide Time: 11:12)



So now, let us see how exactly we can find at least one solution that will be the goal of this lecture. So, the construction idea of that solution will be as follows: we will define; we will try to find out a special linear combination of the N remainders that are given to us. So remember, we are given N remainders a_1 to a_n, we will try to express that unknown x which we want to find out as a special linear combination of these n remainders namely, we will try to find out this special linear combiners c_1, c_2, c_n.

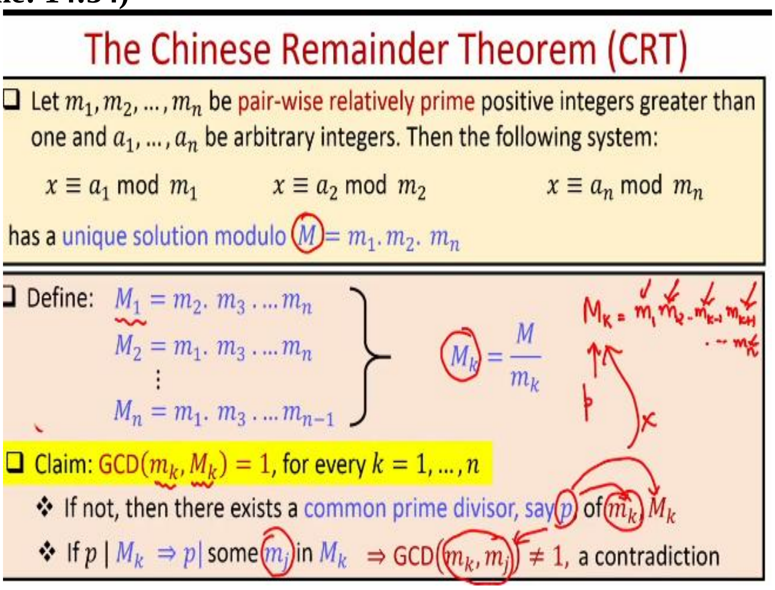
These linear combiners will be special in the sense that if you take the ith combiner c_i and reduce ith modulo m_i namely m_i modulus you will get 1, but if you take the jth combiner and try to reduce it modulo any other modulus, you will get 0. So for instance, what I am saying is that my combiner c_1 will be such that c_1 modulo m_1 will be 1, but the same linear combiner c_1 modulo any other modulus will be 0, namely the n - 1 other modulus, all this will be 0.

In the same way your c_2 modulo m_2 will be 1, but c_2 modulo m_1, c_2 modulo m_3, c_2 modulo m_4, c_2 modulo m_n will be 0. So, that will be the property of the special linear combiners; how exactly we find them that is our whole process, but imagine for the moment that it is possible to find out this linear combiners. That means, I know how to find out this linear combiners such that x is indeed equal to this.

Now, you can see that if I take this value, once I have found c_1 c_2 c_n then I will have this exact value, then if I take this RHS and compute RHS modulo m_1 then that will be same as a_1 modulo m_1 because for all other summands I will be getting c_2 modulo m_1 , c_3 modulo m_1 , c_n modulo m_1 and their effect will be 0 0 0 0 0 it will be only c_1 times a_1 modulo m_1 and c_1 modulo m_1 is 1, because that will be the property for my linear combiner. And hence, this value of x that I have obtained modulo m_1 will be indeed a_1.

In the same way assuming that I have found c_1 c_2 c_n satisfying these conditions what I can say about the x that I have obtained modulo a_2, if I do x modulo a_2, then it will be equivalent to this c_2 times a_2 modulo m_2 because the effect of this term will be 0, the effect of third term will be 0, the effect of the nth term will be 0 and so that is the idea here. So, everything falls down to how exactly we find this special linear combiners c_1 c_2 c_n satisfying this properties.

(Refer Slide Time: 14:34)



So, let us see how we find; so, remember, my bigger modulus M is the product of all n modulus. Now, I define n number of small sum modulus, so my first sum modulus M_1 is the product of all the n modulus except the first namely m_1, my M_2 is the product of all the n modulus except m_2 and so on. So, in general the sum modulus M_k is the product of all the n modulus except the kth modulus.

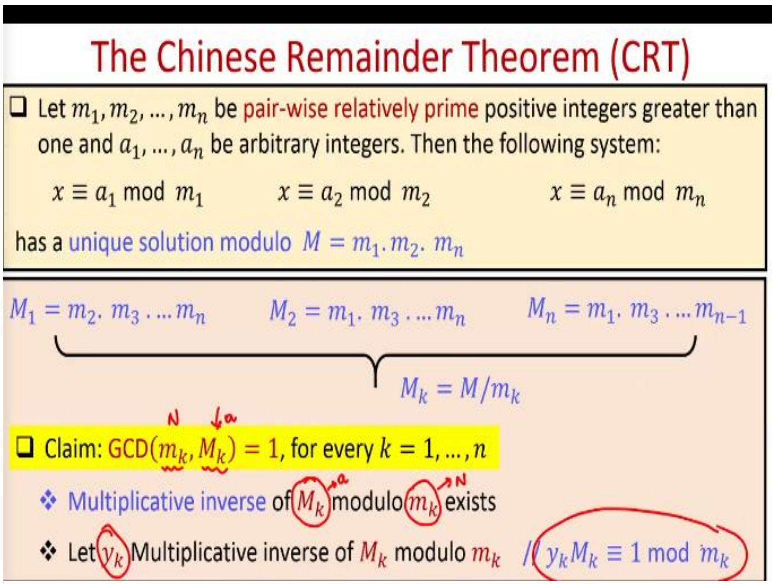
Now, my claim is that if I take the modulus m_k and the modulus M_k then they are co-prime to each other and this is true for every k from 1 to n. Now, the proof is very simple assume that the GCD of m_k and M_k is not one. So, if your GCD is not one that means, there is another common divisor and that will have some prime factor as well because every number has a prime factorization.

So, that means, if the GCD is not one, then that means there is at least some common prime divisor which divides both m_k and M_k. Now, if this prime number p divides this modulus M_k then since M_k is the product of n – 1 number of small modulus so, it is the product of m_1, m_2, $m_{k - 1}$ and m_k is missing $m_{k + 1}$ up to m_n it is the product of n - 1 modulus. And I know and I am assuming here that p is a divisor of M_k.

p is a divisor of this M_k it has to either divide m_1 or it has to either divide m_2 or it has to either divide $m_{k - 1}$ or it has to divide either $m_{k + 1}$ and so on, because if p does not divide any of these small modulus m_1 m_2 $m_{k - 1}$ $m_{k + 1}$ m_n. Then how in the first place it can divide M_k because p is a prime number. So, that means, it has to divide some small modulus call it m_j and we already know that p divides m_k. Now, this m_j is definitely different from m_k because m_k is not present in this M_k; it is not present.

So, that means now I have obtained a pair of small modulus m_k and m_j which are not co-prime because p is a common divisor of both m_k and m_j which is a contradiction to the fact that the n small modulus which are given to us they are pairwise co-prime, so that is a proof of this claim.

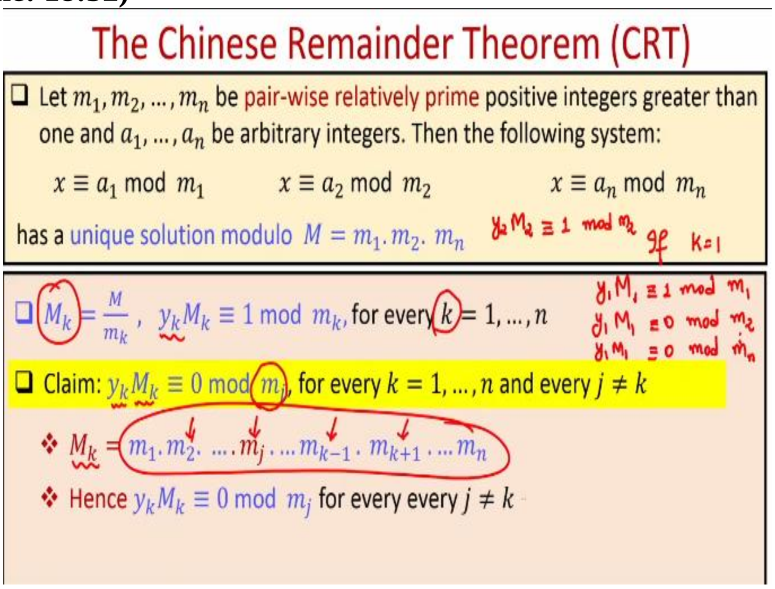
(Refer Slide Time: 17:43)



So, I am retaining this claim here, now, if this small modulus m_k is co-prime to this M_k and I can say that I can find out the multiplicative inverse of this M_k modulo m_k. I am treating m_k my modulus and M_k as the number so, I am treating it as my a and this is my N and I have shown that a is co-prime to N and hence I know that multiplicative inverse of a modulo N exists.

So, I know that multiplicative inverse of M_k modulo m_k exists and I can find it out using the extended Euclid's algorithm. So, let y_k be the multiplicative inverse of M_k modulo m_k. That means this property holds that means you multiply y_k with M_k and then you take modulo M_k you will get the remainder 1, you will get the answer 1.

(Refer Slide Time: 18:52)

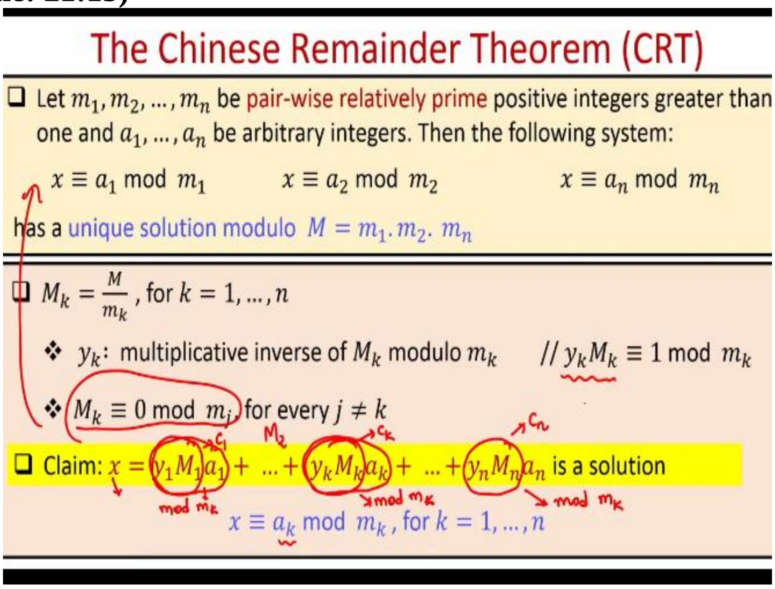


So, these are the various facts here so, this is my M_k and the corresponding multiplicative inverse is y_k. And this I can find out for every k in the range 1 to n. Now, my claim is that the product of this y_k and M_k modulo every other modulus except the kth modulus is 0. So, for instance if k = 1, what I am saying is, we know that y_1M_1 is congruent to 1 modulo the first modulus.

But the claim that I am now making is the following that y_1 times m_1 will be congruent to 0 modulo every other small modulo, that means you take the remaining n - 1 modulus says y_1 times m_1 will be congruent to 0 modulo those n – 1 modulus. Similarly, if you take y_2 times m_2, we know that that is congruent to 1 modulo the second small modulo m_2. But with respect to the first modulo m_1, the third module m_3, fourth modulo m_4 and so on y_2 times m_2 is 0 and the proof is very simple here.

So, I know that M_k is the product of n - 1 small modulus is here, that means it is a product of all the n modulus expect the kth modulus. And hence, if I divide this M_k by m_1 I will get remainder 0 because this number is completely divisible by m_1. If I divide this M_k by m_2, again it is completely divisible by m_2, if I divide this M_k by m_j again, it is completely divisible by m_j, if divided by m_{k-1}, it is completely divisible. If I divide it by the k + 1 th modulus again it is completely that is a very simple fact.

(Refer Slide Time: 21:15)



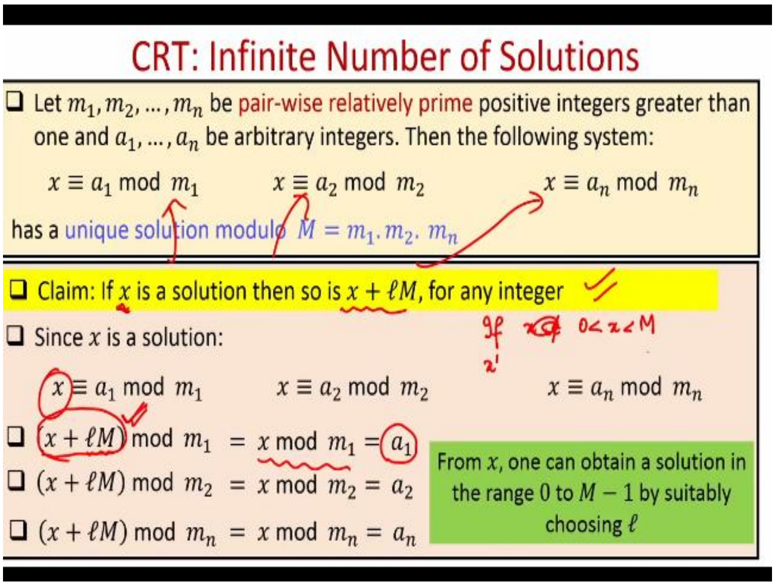
So that is the third property that I have retained here, now remember, the proof strategy was that I want to express my unknown x as a special linear combination of my remainders a_1 to a_n. And my claim is that now I have obtained those special linear combiners. So, my claim is that if I take this linear combination of the n remainders, namely y_1 times M_1 times a_1. So, this is my first linear combiner, this is my kth linear combiner and this is my nth linear combiner.

My claim is that this value of x ($x = y_1M_1a_1 + \ldots + y_kM_ka_k + \ldots + y_nM_na_n$) is indeed a solution for this system of linear congruences and you can easily verify that; what will happen if I take the value of this x and compute modulo m_k. I compute x modulo m_k so, if I compute x modulo m_k then that will be same as this first summand modulo m_k the second summand modulo m_k, the kth summand modulo m_k and the last summand modulo m_k.

Now what can I say about the first summand modulo m_k, so I know that this property holds; that means if I take the first summand here there M_1 is present and M_1 is congruent to 0 modulo m_k that means M_1 is completely divisible by my small modulus m_k. So, this first summand is completely divisible by m_k, so it will give me the remainder 0. Similarly, the second summand will have M_2 which is completely divisible by M_k.

So that is why the overall second summand is completely divisible by M_k and it will give me the remainder 0. But when I come to the kth summand here, in the kth summand, I know that I have y_k times M_k present and y_k times M_k modulo m_k is 1. So that is why this overall term modulo m_k will give me a_k and again the remaining other terms will vanish they will turn out to be 0 that means it tells me that if I divide x by m_k, I will obtain the same remainder that a_k gives me on dividing by m_k or equivalently x - a_k is completely divisible by m_k. So that means, by following this process, I can find out at least one solution satisfying the whole equation, the whole equation in the sense the whole system of linear congruences. But I want to find out a solution in the range 0 to M – 1.

(Refer Slide Time: 24:38)



How do I obtain that? So, for that, again, let me reiterate what I am been saying again and again, if you have one solution x, satisfying the n linear congruences here. Then any number of the form x + *l* times your bigger modulus is also a solution for the same system of linear congruences where *l* can be positive or negative. That means, let us first prove this claim and then we will see how exactly we can find out a solution in the range 0 to M - 1.

So, since x is a solution which satisfies the system of linear congruences, that means, x has these properties, that means x is congruent to a_1 modulo m_1, it is congruent to a_2 modulo m_2 and so on. Then what can I say about x + *l* M modulo m_1, x + *l* M modulo m_1 will be same as x modulo m_1 because *l* times M modulo m_1 will give you 0 because M is completely divisible by m_1.

Because remember your M is the product of all the n modulus, that means, even though this might look like a different number, this different number when divided by m_1 will give you the same remainder which you obtained by dividing just the value x by m_1 and we know that x on divided by m_1 will give you the remainder a_1. So, that means, this different number satisfies the first linear congruence. In the same way, the same different number satisfies the second linear congruence and so on.

So, now this claim is true, we have proved that, so assuming you have a solution x satisfying your linear congruence. Now, if that x is not within the range 0 to M - 1, then you keep on subtracting multiples of M from it, you make it small and small, because every time you subtract one full multiple of M, the new number is still a solution.

That means, if x does not belong to the range; if this condition is not satisfied and you want to find out an x’, which is also a solution and within the range 0 to M, then what I am saying is that you keep on subtracting means you first compute x - M and check whether this x – M is within the range 0 to M - 1 or not. If not, then compute x - 2M and compute x – 3M.

Because all of these new numbers also will be solution for your system of linear congruences and eventually by appropriately choosing the value of *l* you will obtain an x will be in the range 0 to M - 1 and which satisfies all the n linear congruences. So, that shows that using the Chinese Remainder Theorem, you can obtain at least one solution modulo the bigger modulus satisfying the system of n linear congruences, namely, you have to find out your special linear combiners as we have seen in the last slide.

We have to find out this y_k which is the multiplicative inverse of your kth sub modulus M_k modulo m_k and if you do this, then this x will be one of the solutions, if this x that you have obtained as per the Chinese Remainder Theorem satisfies the condition that is it is in the range 0 to M-1, then well and good else, you find out an appropriate multiple or you select an appropriate value of *l* which will ensure that you obtain a solution in the range of 0 to M - 1.

So, that brings me to the end of today's lecture just to summarize, in this lecture, we introduced linear congruences and we discussed 2 methods of solving the system of linear congruence one using the extended Euclidean algorithm and another one due to Chinese Remainder Theorem. Thank you.