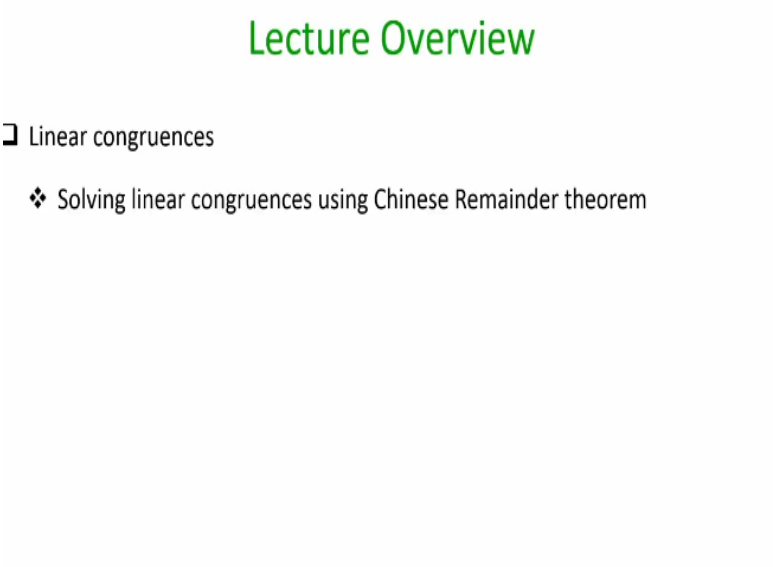
Discrete Mathematics
Prof. Ashish Choudhury
International Institute of Information Technology, Bangalore

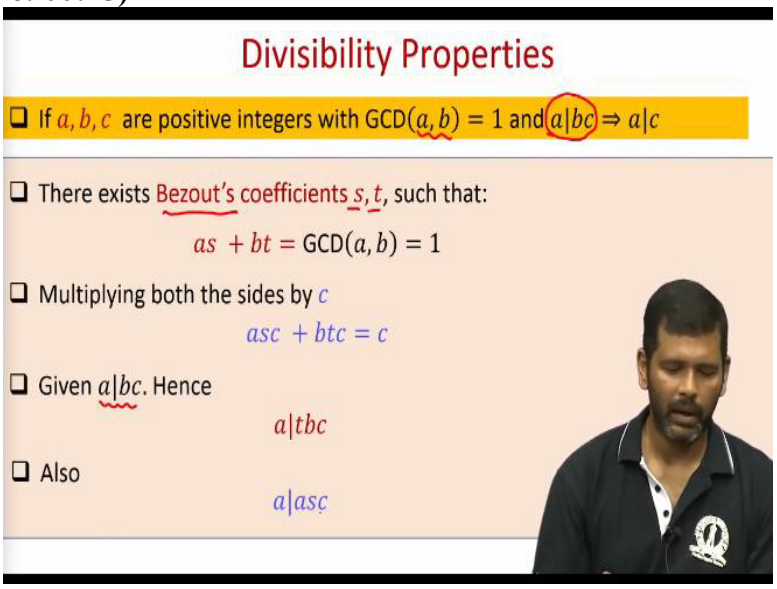
Lecture – 59
Uniqueness Proof of the CRT

(Refer Slide Time: 00:23)



Hello everyone, welcome to this lecture, so, in this lecture we will continue our discussion regarding solving linear congruences using CRT. And specifically we will focus on the uniqueness part of the solution. So, we want to prove that there exists a unique solution in the range 0 to M - 1 satisfying the system of linear congruence.

(Refer Slide Time: 00:45)



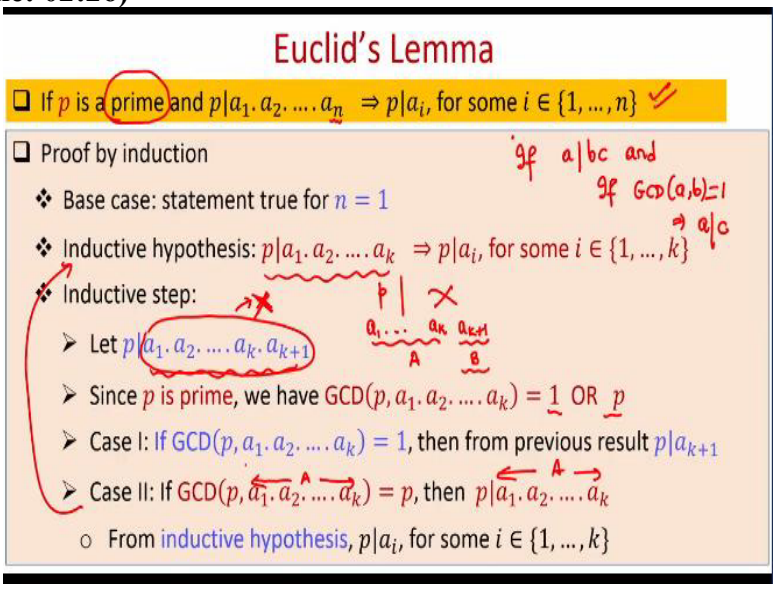
So, we start with some basic properties of divisibility, so the first property is the following imagine you are given 3 positive integers a, b, c and it is given to you that a divides the product of b and c but a is co-prime to b. Then I can conclude that a divides c that means, if a

divides the product of b and c but a is co prime to b then it must be the case that a divides c and the proof is as follows.

So, we know that as per the Bezout's theorem, we have integer linear combiners s and t, such that I can write the GCD(a,b) which is 1 as per my premise as s times a + b times t. Now, if I multiply both the sides of this equation by c, I get this equation: $asc + btc = c$, now I know that it is given to me a divides the product of b and c and hence it divides any multiple of b times c. So, it divides t times bc as well and any how a divides any multiple of a, so it will divide s times c times a.

And now if I know that a divides 2 numbers, it divides the summation of those 2 numbers as well, but the summation of the 2 numbers that I am taking here is nothing but the value c. That is the proof of this fact, very simple fact but useful.

(Refer Slide Time: 02:26)



Now we prove another property which we often call as the Euclid's Lemma, which is also very useful while proving the uniqueness part of the CRT theorem. So, the Euclid's Lemma, is as follows, it says that if p is a prime number and if it is given that p divides the product of n numbers. Then definitely, it has to be the case that p divides at least one of those n numbers, it cannot be the case that p is a prime number and p does not divide a_1 it does not divide a_2 it does not divide a_n.

But still it automatically divides the product of those n numbers; and there are again multiple ways to prove this. I will prove it using induction because it is convenient to prove it using

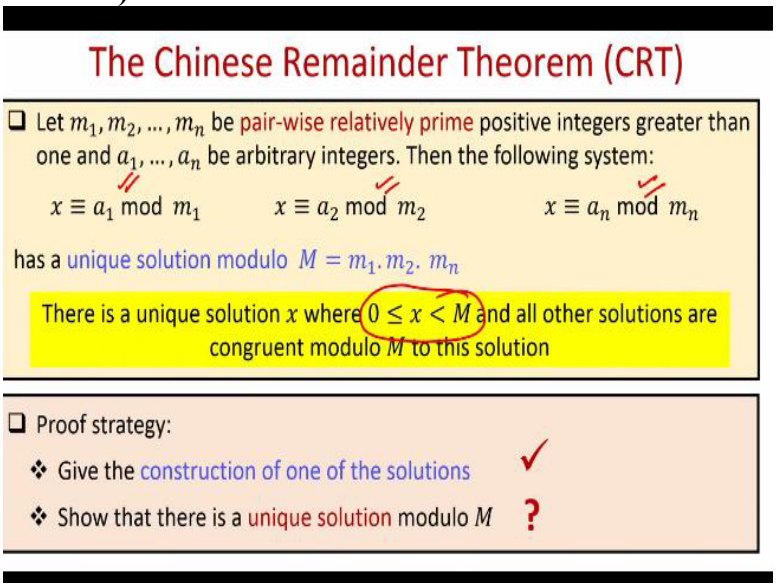
induction, since it is a universally quantified statement for all. So, the base case will be for n = 1 and which is trivial, because if it is given to you that p divides a_1 that means p divides a_1. Now assume that the inductive hypothesis is true that means assume that if p divides the product of k numbers where p is a prime, then there is at least one of those k numbers which is divisible by p, I do not know which one but it is there. Assume this statement is true for every k and every k numbers. Now let us do the inductive step and take a new number which is the product of k + 1 number and imagine you have a prime number p which divides the product of those k + 1 number. My goal is to show that there is at least 1 number out of this k + 1 number which is completely divisible by p.

So, the first thing to observe here is that since p is a prime number, what can I say about the greatest common divisor of p and this bigger number. So let me call this bigger number as X, so what can I say about the GCD(p, X)? The GCD will be either one or p because the only divisor of p are 1 and the number p itself there cannot be any other third value of GCD. So, there are 2 possible cases so let us analyse those 2 cases.

Now if the GCD of p and the product of the first k numbers is 1, then from the previous result means in the previous slide I showed that if a divides bc and if GCD(a,b) is 1, then in the previous slide I showed that it has to be the case that a divides c. So, my X is the product of first k numbers and the k + 1 th number; so, I can treat my X as a_1 to a_k as product,. so, this is my say A and I also have a_{k+1} also in the product that is B. So, I know that p divides X that means, p divides the product of A and B and I am in the case where p is co-prime to A because this product of the first k terms I am calling it as A then from the previous result, I know that p has to divide B and B is nothing but a_{k+1}. So, that proves my inductive step because in the inductive step I have to show that there exists at least one number which are involved in the product here in the number X which is completely divisible by p.

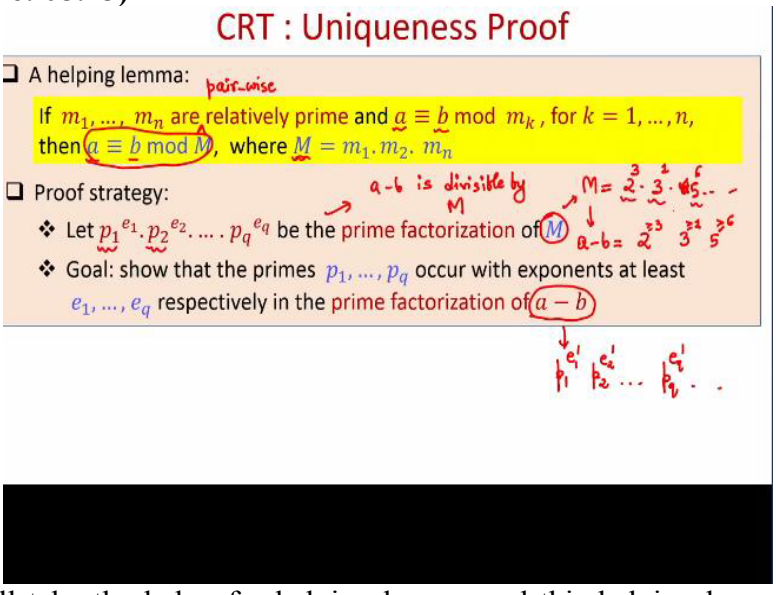
And I have shown the existence of one such number this is when the GCD(p,A) = 1. Now, consider the case when the GCD(p, A) = p and then in that case, if the GCD(p, A) = p then p of course divides A and if p divides A and A is a product of k numbers and since p is a prime number, I can use my inductive hypothesis and argue that there exists at least one number which are involved in the computation of A which is completely divisible by p that means either p divides a_1 or p divides a_2 or p divides a_k. So, that proves my Euclid's Lemma, important property which will be again useful.

(Refer Slide Time: 07:43)



So now, coming back to the uniqueness proof part for the Chinese remainder theorem in the last lecture, we showed that there exists at least one solution in the range 0 to M – 1. How do I prove that there is no other solution possible satisfying the same system of linear congruences and which is also in the range 0 to M - 1, we have to refute the existence of second solution.

(Refer Slide Time: 08:13)



So, again we will take the help of a helping lemma and this helping lemma will be useful later as well. So, what this helping lemma says is the following: imagine you are given n 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 suppose you know that you are given 2 numbers a and b which are congruent with respect to all the n individual modulus.

It means they are congruent with respect to modulo m_1, they are congruent with respect to modulo m_2, and they are congruent with respect to modulo m_3 and so on. Then, the claim here is that the same 2 numbers a and b are congruent with respect to the bigger modulus M, which is the product of all the n modulus and again there are multiple ways to prove this, let us follow the following strategy.

So, as per the fundamental theorem, I know that this bigger modulus M must be having a unique prime factorization, that means, I can express this bigger modulus M as product of powers of prime. So, let those powers e_1, e_2, e_q and so on. Now, my goal is to show the following, in my proof I will show that if I take the prime power factorization of a - b. So, a - b also will be a number and it will have a prime power factorization.

So, I have to select the prime power factorization of a – b be $p_1^{e1'}$, $p_2^{e2'}$, and like that $p_q^{eq'}$ and so on. So, what I want to show is that each of the prime factors, which are involved in the prime factorization of M, they are also involved in the prime power factorization of a - b and with at least the same individual powers with which they were involved in the prime factorization of M.

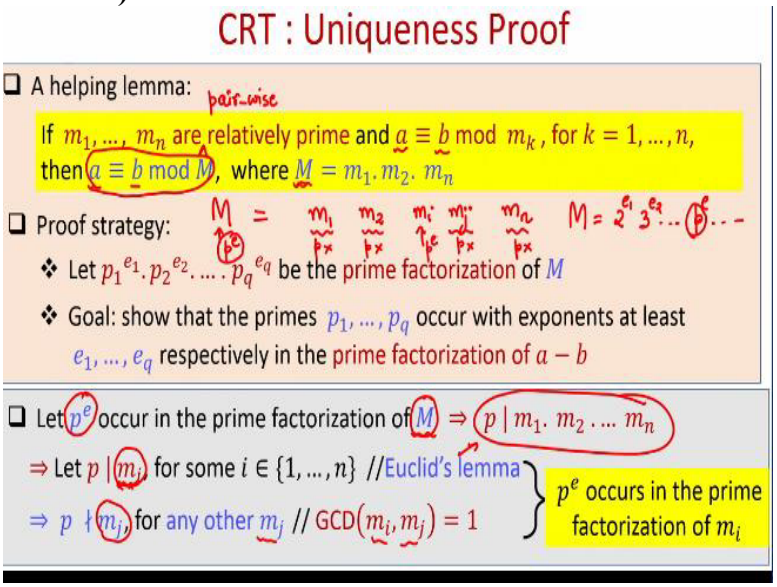
So, what I am trying to say here is the following: say for instance, if my M was say $2^3.3^1.5^6$ and so on. Suppose these are the various powers of primes which are involved in the prime power factorization of M, my goal will be to show that if I consider a - b, then the same prime factor 2 is involved at least 3 or more than 3 times that means it will be either greater than or equal to 3 power it is must that means 2 should have 3 or more power appearing in the prime factorization of a - b.

Similarly, the factor 3 should appear with the power at least 1, the next prime factor 5 should appear with at least power 6 and so on. If I show this, then that shows that a - b is completely divisible by M; if I show this then this will imply that a - b is divisible by M. And that is what precisely I want to show I want to show a is congruent to b modulo M. And remember, an equivalent definition of congruence is that if a is congruent to b modulo m then that also implies a - b is completely divisible by M.

So, if I can show that each of the prime factors, which are involved in the prime factorization of M are also involved in the prime factorization of a - b and with at least the same powers

with which they were appearing in the prime factorization of M, that means, a - b is completely divisible by M and that is what the proof strategy will be.

(Refer Slide Time: 12:45)



So, let us consider an arbitrary prime factor of the bigger modulo M and suppose it is appearing with power e in the prime power factorization that means so, M = 2^{e1}, 3^{e2} and so on and some p^e so on. So, I am taking an arbitrary prime which is appearing with some power in the prime power factorization of M, I have to show that the same power, at least, is also present in the prime power factorization of a - b as well.

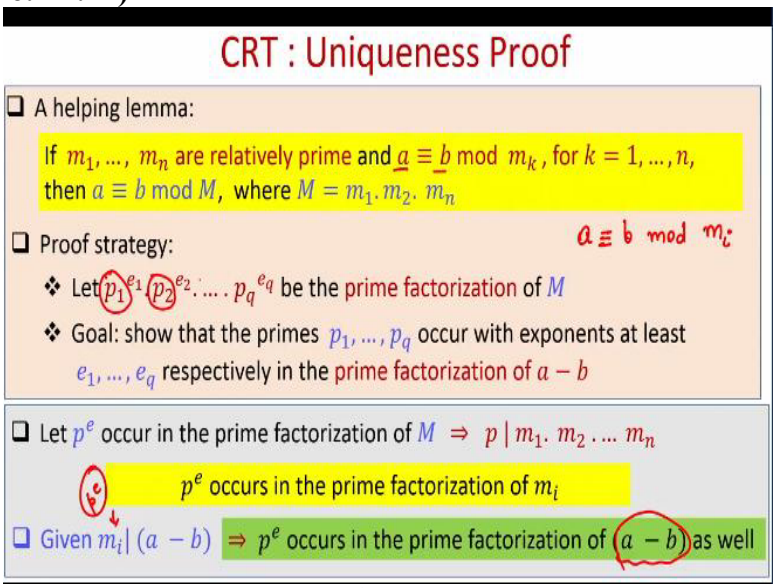
Now, since p is occurring with power e in the prime power factorization of M, that means I can definitely say that p divides the product of m_1 to m_n because M involves a prime power of the form p^e in its prime power factorization; that means, p has to divide the product of m_1 to m_n which is nothing but M. That means, this condition holds. And now, I can apply the Euclid's Lemma which I just proved some time back that if p is a prime number and if it divides the product of n values, then it has to divide at least one of those n values.

So that means p divides at least one of the small modulus, let us call it as m_i and I know that p does not divide any other modulus m_j, I can conclude that because I know that the various modulus m_1 to m_n they are pairwise prime that means, there cannot be any other modulus m_j such that p divides that other modulus m_j as well because if p divides the other modulus m_j as well, then I already have the fact that p divides m_i and if p divides m_j as well, then I will get the conclusion there is a common divisor other than 1 namely the prime number p which divides both m_i and m_j and which goes against assumption that my modulus m_i and m_j are

pair-wise prime. And if p does not divide any other modulus m_j and I know that p^e is occurring in M in the prime power factorization, then the only way the contribution p^e can come in the prime power factorization of M is because the p^e was contributed in the prime power factorization of m_i itself so, remember each of the modulus m_1, m_2, m_i, m_j, m_n will individually have their own prime power factorization and I have the product of all this modulus which is M, I know that p^e is contributed in the prime power factorization of M. So, this p^e might be accumulated through several modulus m_1, m_2, m_i, m_j, m_n.

But what I have shown here is that if at all p is coming from m_i that means if p's contribution was there in the prime power factorization of m_i. Because if p divides m_i then p would not be appearing in the prime power factorization of m_1, p would not be appearing in the prime power factorization of m_2, p would not be appearing in the prime power factorization of m_j, p would not be appearing in the prime power factorization of m_n and so on. So, that means the only way this p^e would have been accumulated in the prime power factorization of M is because it was present in the prime power factorization of m_i itself.

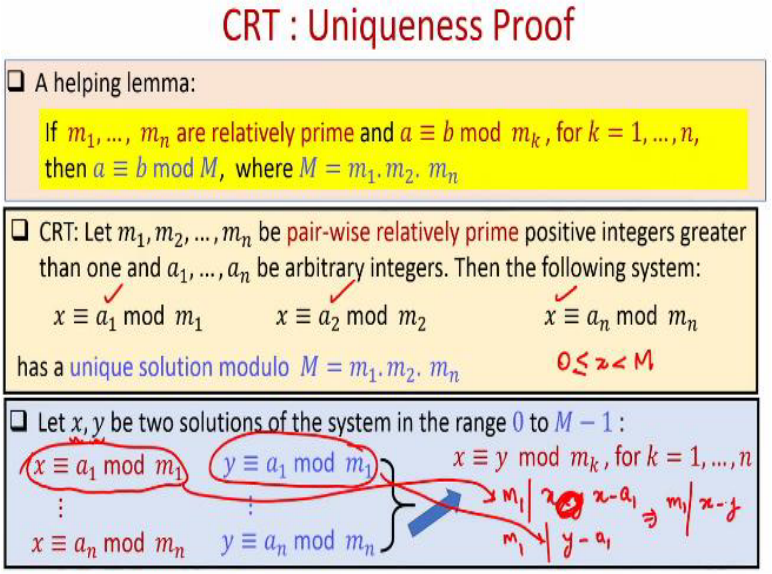
(Refer Slide Time: 17:14)



So that is a conclusion I have drawn that p^e occurs in the prime power factorization of m_i. Now, remember, the properties of a and b is the following they are congruent with respect to every modulus that means a - b is completely divisible by all the n individual modulus. So, a - b is also divisible by m_i as well because as per my premise a and b they are congruent modulo m_i as well, the same m_i where p^e occurs in the prime power factorization.

That means p^e occurs in the prime power factorization of m_i and if m_i divides a - b that means p^e also occurs in the prime power factorization of a - b as well and that is what precisely I wanted to show. So, namely if I substitute p with p_1 I have shown that p_1^{e1} will also occur in the prime power factorization of a - b. If I substitute p with p_2 in this whole proof then I concluded that at least p_2^{e2} also occurs in the prime power factorization of a – b; p_2 can occur with higher power as well, but at least p_2^{e2} is definitely there that much power is always there in the prime power factorization of a - b and so on.

(Refer Slide Time: 18:52)



So, we have proved the helping lemma now, coming back to the proof of the uniqueness of the solution, we wanted to prove that there is a unique solution x in the range 0 to M - 1 satisfying the system of n linear congruence says, so we will prove it as follows. On contrary imagine you have 2 solutions, 2 solutions in the range 0 to M - 1 satisfying this system of linear congruences and those solutions be let x and y.

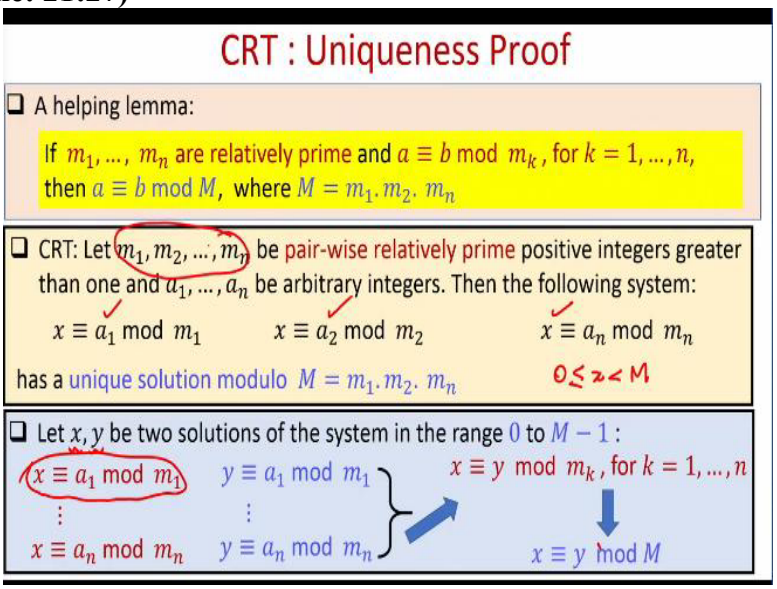
That means x satisfies this system of n linear congruence is that when x is congruent to a_1 modulo m_1, x is congruent to a_2 modulo m_2 and x is congruent to a_n modulo m_n. And similarly, since y is also a solution, for the same system of linear congruences, this set of n linear congruences will also get satisfied. Now, from the first equation here and the first equation here, I get that x is congruent to y modulo m_k, or x is congruent to y modulo m_1.

Because x - a_1 is completely divisible by m_1 and y - a_1 is completely divisible by m_1, then what can I say about x - y, if m_1 divides x - a_1 completely that comes because of the first linear congruence here, and this linear congruence tells me that m_1 divides y – a_1. Then I can

say that and m_1 divides the difference of these 2 numbers as well and the difference of these 2 numbers will be x - y.

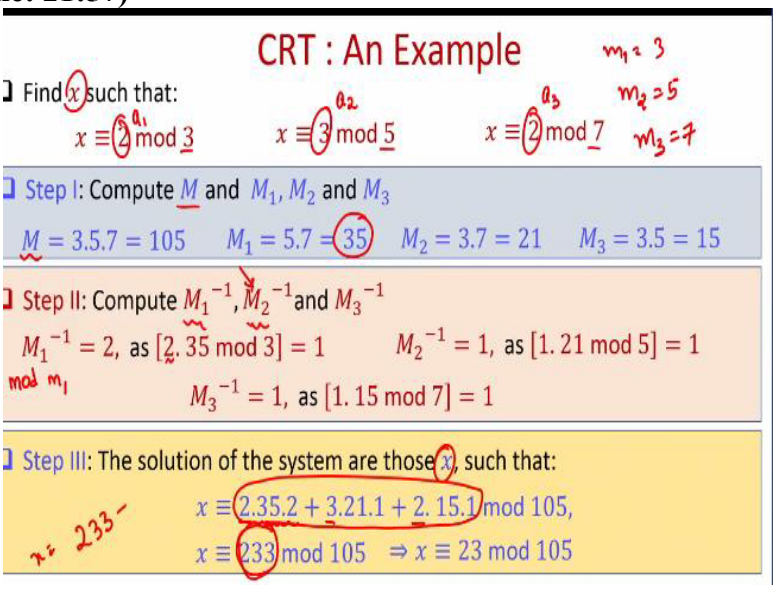
In the same way, I can say that x - y is completely divisible by m_2, I can say that x - y is completely divisible by m_k and x - y is completely divisible by m_n. So, I get n congruences like, that means x and y are congruent modulo m_1, m_2, m_n and remember that my m_1, m_2, m_n they are pairwise relatively prime.

(Refer Slide Time: 21:27)



So, I can take the help of helping lemma and I can conclude that both x and y are congruent modulo M. And since both x and y were in the range 0 to M - 1, that means they were strictly less than M, and both of them are congruent, then that is possible only when x = y that shows that there exists a unique solution modulo M satisfying your system of linear congruence.

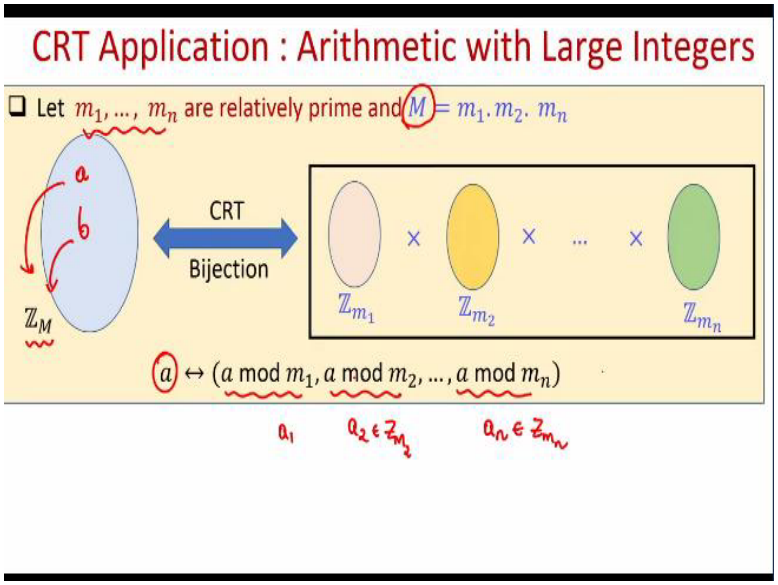
(Refer Slide Time: 21:57)



So now, let us see an example for Chinese remainder theorem. So, say we want to find out this unknown x satisfying the system of linear congruences : $x \equiv 2 \bmod 3, x \equiv 3 \bmod 5, x \equiv 2 \bmod 7$. So, we will find out the bigger modulus and sum modulus so, the bigger modulus will be the product of 3, 5, 7 and you can see your m_1 is 3, m_2 is 5, m_3 is 7 and a_1 is 2, a_2 is 3 and a_3 is 2. So, my bigger modulus will be 105, M_1 will be the product of all the modulus except 3, so 35. M_2 will be the product of all the small modulus except 5, and M_3 will be the product of all the 3 modulus except 7 so, I found M_1, M_2, M_3. Now, my next goal will be to find out M_1 inverse modulo m_1, M_2 inverse modulo m_2 and M_3 inverse modulo m_3, which I can do by using extended Euclid's algorithm. So, M_1 inverse modulo m_1 will be 2 because, you can see that your M_1 is 35 if you multiply 35 with 2 and then you take small modulo m_1 then you will get answer 1 in the same way M_2 inverse modulo m_2 is 1 and M_3 inverse modulo m_3 is also 1. So, then as per the Chinese remainder theorem, we will compute the value x which is the linear combination of your a_1, a_2 and a_3 and the linear combiners are the various m_1, m_2, m_3 and their respective multiplicative inverse multiplied with each other, so this will be the value of x = 233 $x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \bmod 105, x \equiv 233 \bmod 105$.

Now this x will be 233 modulo 105 so, our goal is to find out the unique solutions of course, 233 is a solution if I take x = 233 you can verify that it satisfies the system of linear equation, but we want to find out a unique solution in the range 0 to 104 so, how I can do that I can keep on subtracting 105 or equivalently I can directly take 233 modulo 105 because that will tell me exact number of times 105 have to be subtracted so that I get a remainder within the range 0 to 104, namely 23 which will be a solution for the system of given linear congruences.

(Refer Slide Time: 25:07)



So now, let us see some application of Chinese Remainder Theorem, it has tremendous applications, of course in cryptography, but in general it has other applications and our main application is when we want to do arithmetic with large values. So, what basically CRT tells us that if you are dealing with very big modulus and you want to do arithmetic involving those big modulus, then instead of doing operations modulo those big modulus you can do operations with small modulus and they will be equivalent, what do I mean by that?

So imagine, you are given n modulus m_1 to m_n which are relatively prime and you are given a bigger modulo M, which is a product of these n modulus. So, consider the set Z_M, the set Z_M is nothing but it has all the integers 0 to M – 1 and you have n number of small sets here, you have Z_{m1} which is nothing but you have all the integers from 0 to m_1 - 1, Z_{m2} has all the integers from 0 to m_2 - 1 and Z_{mn} has all the integers from 0 to m_n – 1, we will later encounter these sets again.

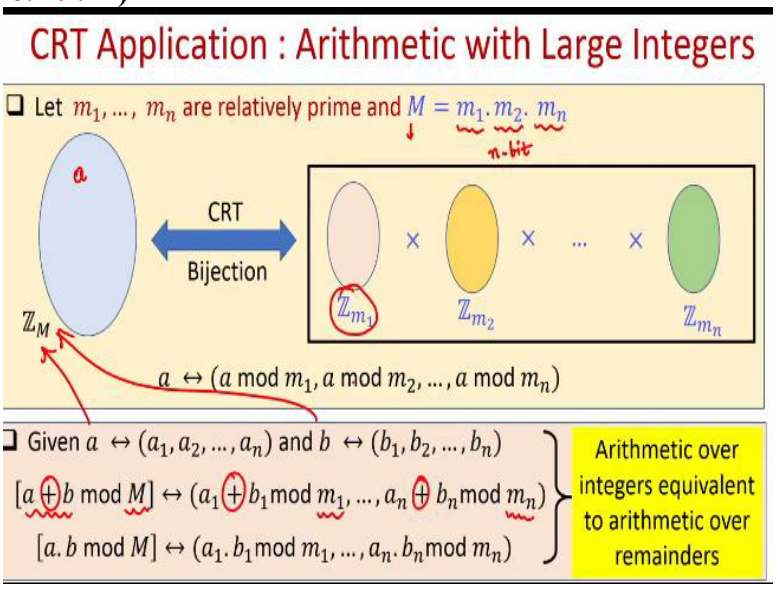
Now what Chinese Remainder Theorem basically tells you: it establishes a bijection between this bigger set Z_M and the Cartesian product of these n sets, what exactly is the bijection? The bijection is the following: if you are given a value a here and you want to find out the corresponding mapping as per this bijection then the image of a is obtained by computing a modulo m_1, a modulo m_2, a modulo m_n that will be the representation of a.

And my claim is that this representation that we have obtained is an injective mapping because, if you have 2 different values a and b where a is different from b then definitely there will be at least one m_i where a modulo m_i and b modulo m_i will be different because if a

modulo m_1 and b modulo m_1 is same, a modulo m_2 and b modulo m_2 is same, a modulo m_i and b modulo m_i is same and a modulo m_n and b modulo m_n are same, then since my modulus m_1 to m_n are pairwise relatively prime using the helping lemma that we have just proved we come to the conclusion that a and b are also congruent namely, they are same because both a and b are in the range 0 to M - 1. So, you cannot have 2 different values a and b and at the same time their representations are also same; by the way by representation I mean though each value in the range 0 to M - 1 or an element of Z_M will be now represented by an n tuple.

So, why n tuple because there will be n values which will be treated as the representation of a, so, that is an injective mapping and the mapping is surjective as well, because if I give you arbitrary values of a_1, a_2, a_n where a_1 is in the range 0 to m_1 - 1, a_2 is in the range 0 to m_2 - 1 and a_n is in the range 0 to m_n – 1, then I can find out the corresponding a in the range 0 to M - 1 whose CRT representation will be a_1, a_2, a_n that shows that my mapping is subjective as well.

(Refer Slide Time: 29:14)



So, basically what I can now say is the following, if you are given 2 numbers a and b and their corresponding representations; that means, now any operation which you want to do in the bigger set modulo the bigger modulus that can be equivalently performed in their smaller worlds modulo small modulus, modulo m_1, modulo m_2, modulo m_n. So, what do you have to do is you have to focus on the first component of the representation of a and b, they will be in this set.

You perform the same operation which you want to perform in the bigger set and do modulo the small modulus, you perform the same operation in the second world modulo m_2, you perform the same operation in the nth world modulo m_n and so on and same holds for product as well. That means equivalently what it shows is that using CRT any arithmetic operations which you want to perform over integers modulo some bigger modulus that is equivalent to performing arithmetic over the remainders as well. And this is a very interesting fact which we use extensively at least in cryptography. So, for instance, if your, say m_1 is; each of this modulus is m_1, m_2, m_n are n bit prime numbers then my M is an enormously large value.

Now if I want to do a + b modulo that enormously large modulus then it will be an overkill instead, what I am saying is that to perform a + b modulo several small modulus and that will be the equivalent representation of whatever remainder you would have obtained by adding a and b in the modulo the bigger modulus. So, that gives you a tremendous saving in the computation that is involved.

So that makes CRT a very interesting theorem, it has got tremendous application especially in cryptography. So, with that I conclude today's lecture, these are the references and just to summarize, in this lecture, we continued our discussion on the Chinese Remainder Theorem. And we proved that, indeed there exists a unique solution modulo the bigger modulus, satisfying the given system of linear congruences. Thank you.