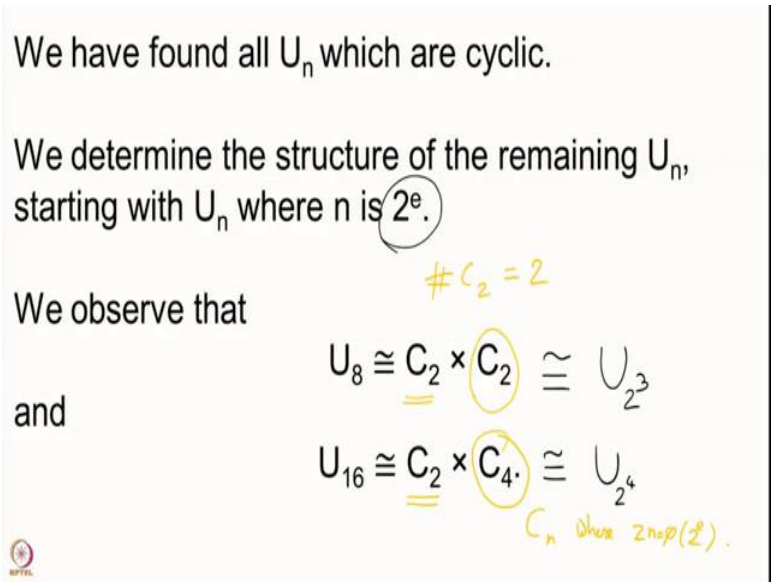
A Basic Course in Number Theory
Professor Shripad Garge
Indian Institute of Technology, Bombay
Department of Mathematics
Lecture-29.
Structure of Un - I

Welcome back, we are looking at the structure of the unit groups in the rings of integers modulo n or what are also known as the residue classes modulo n. And we found a lot of those Un which are cyclic and after that we are studying the structure of the remaining Un. So, we began by looking at U to power e because we observed that whenever the prime was an odd prime Up power e is always a cyclic group for any e bigger than or equal to 1.

However, that was not the case for 2 power e. So, when we are looking are the other Un which are not necessarily cyclic, then we want to start their structure by understanding the structure of U to power e first. We also looked at you 4 and you 8, and in fact, if I remember correctly, we also looked at you 16 in our last lecture.

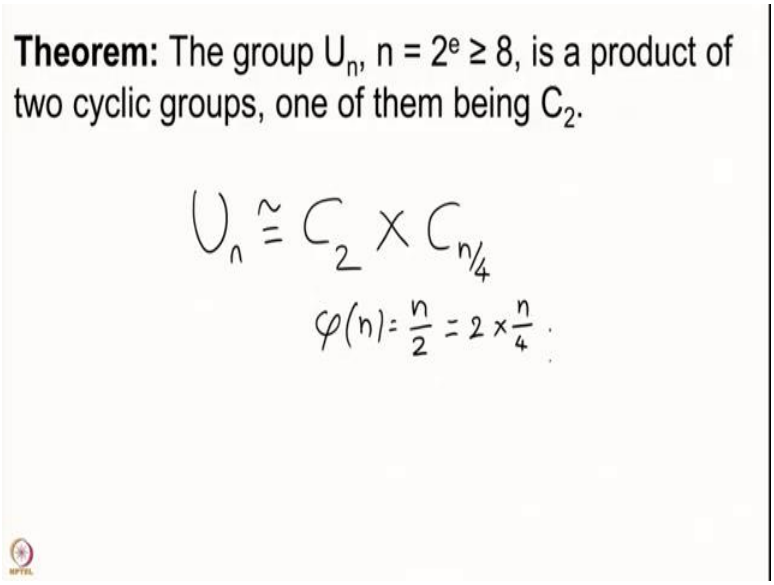
(Refer Slide Time: 1:25)



So, let us recall that quickly we have found all Un which are cyclic. And then we are determining the structure of the remaining Un starting with these U2 power e and we looked at U2 cube which is our 8 and U2 power 4, which is u 16. And we observed that there is one copy of the group C2 always sitting in these and the remaining one has order equal to the order of this group upon 2. So, this has order to hash C2 has ordered is 2, and then the remaining one is C n, where you have that 2 times n is the correct number that we are looking at.

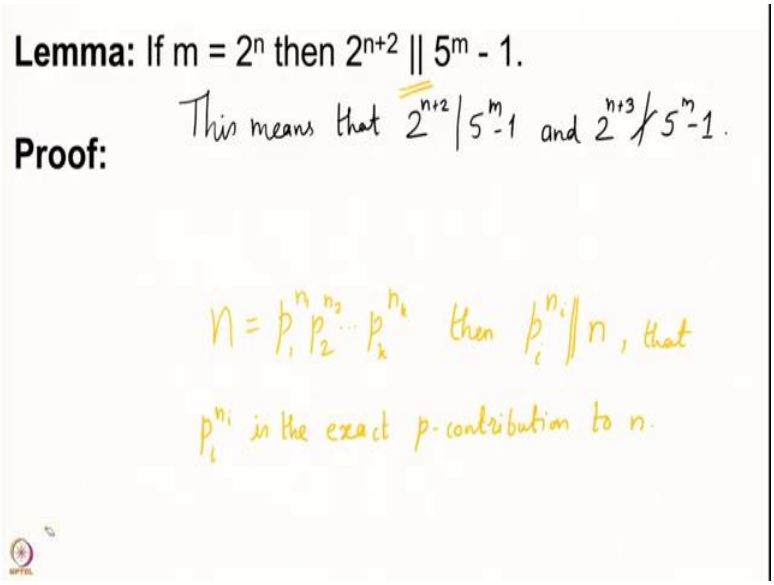
So, this is what we would like to show we would like to show that, when you are looking at n equal to a power of 2, then the group of units is almost a cyclic group. Which is to say that it is not really cyclic, but it is product of 2 cyclic groups, one of them being of order 2. So, up to a sign in fact, we will show that it is a cyclic group. but before we do that, we will need to do one small result regarding integers and let me state that result.

(Refer Slide Time: 2:57)



So, this is the result that we are going to prove the group Un n equal to 2 power e bigger than or equal to eight is a product of 2 cyclic groups, one of them being C2. So, what we are going to do here is that Un is isomorphic to C2 cross C n by 4 remember that since n is a power of 2 phi n is n by 2, which is same thing as 2 into n by 4, your n is bigger than or equal to 8. So, n by 4 is an integer, that is not a problem.

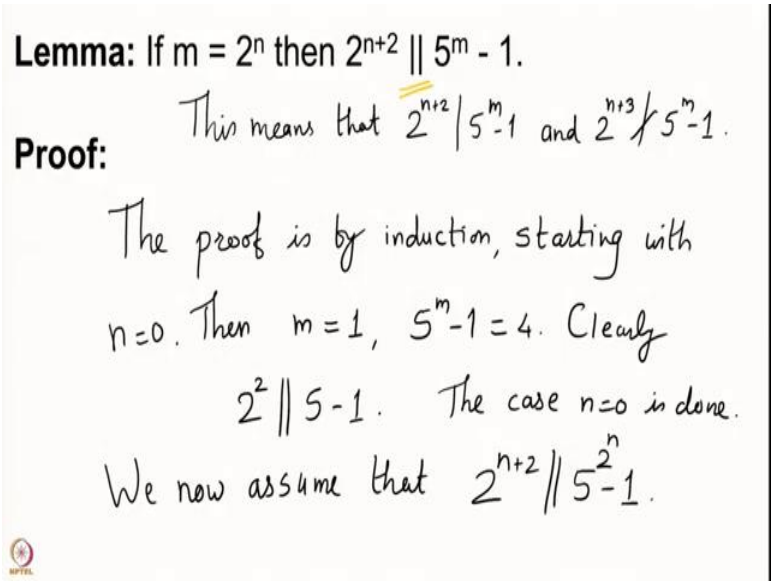
(Refer Slide Time: 3:36)



As I said we will have to do one small lemma here. So, the lemma says that if m is a power of 2, call it to power n, then 2 power n plus 2 double divides 5 power m minus 1. What is this double divide? The double divide is the exact contribution of the prime 2 to this number. So, this means that first of all 2 power n plus 2 divides this quantity 5 power n minus 1 and the next power of 2 does not divide it. This is the meaning of the sign that we have here called double divide.

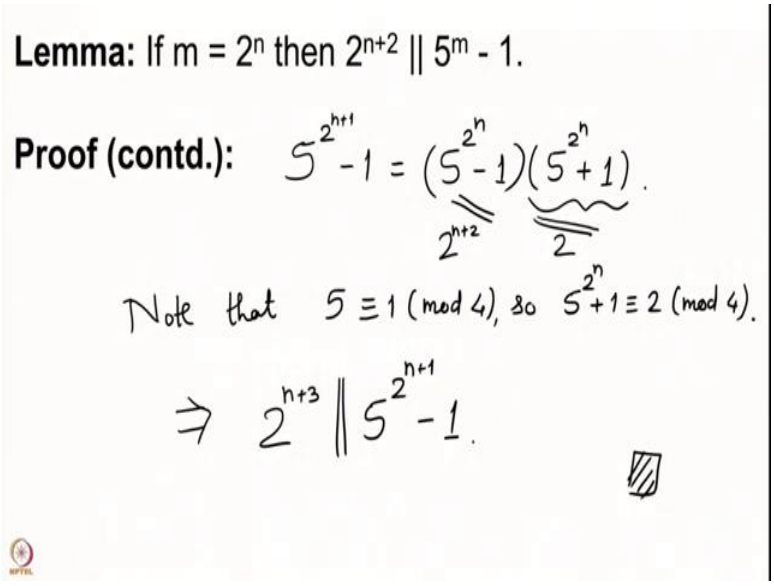
So, whenever you write any number n as p 1 power n 1 p 2 power n 2, so on up to pk power n k, then we have that pi power ni double divided n or you may call it exactly divide n, which means to say that pi power ni, is the exact p contribution to n. This is what we mean when we use this double dividing symbol. We are now going to prove this result. So, what we are going to prove first of all that this is a power of 2 that divides the 5 power m minus 1, but no higher power divides it and the proof is by induction.

(Refer Slide Time: 5:52)



It is a very simple proof, starting with n equal to 0. So, we then have m is 1, 2 power 0 and 5 power m minus 1 is 4. So, clearly 2 square is the exact contribution of 2 to the number 5 minus 1. So, the case n equal to 0 is done. We now assume, so there is this induction hypothesis that we assume, that 2 power n plus 2 exactly divides 5 power 2 to the n minus 1. And we will go to the higher n, so we will look at 5 power 2 to the n plus 1 minus 1.

(Refer Slide Time: 7:19)

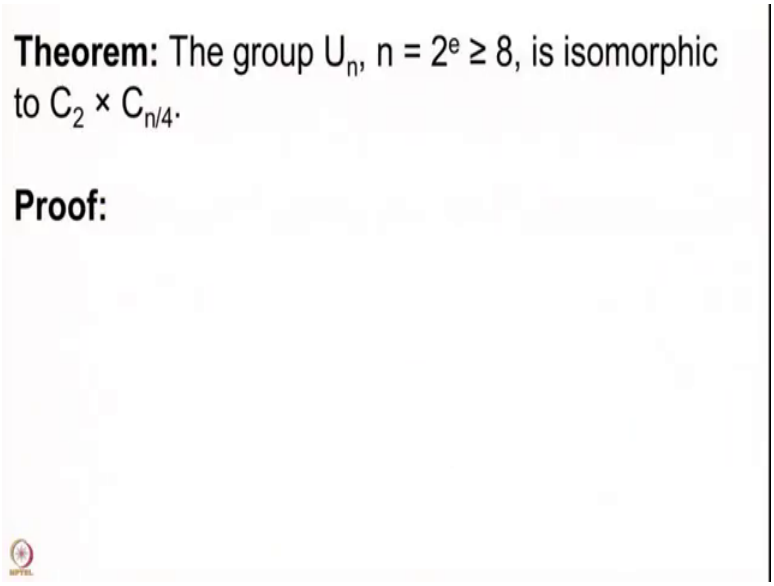


But this can be written as 5 power 2 to the n minus 1 into 5 power 2 to the n plus 1. And we have seen that 2 power n plus 2 exactly divide this, divides this, this quantity is of course, even number, so 2 divides this number. but note that 5 is congruent to 1 modulo 4, so 5 power

anything plus 1 is going to be congruent to 2 mod 4, any power of 5 is going to remain congruent to 1 modulo 4.

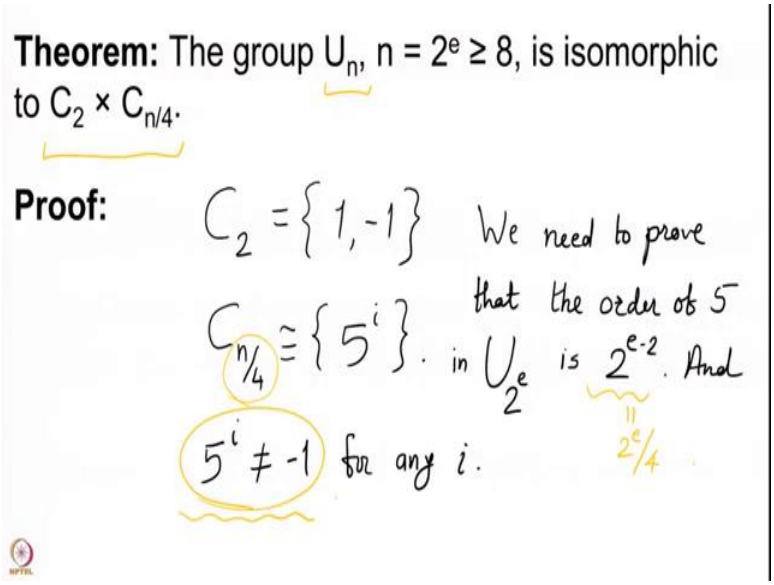
And therefore, when you add 1 to that you are going to get 2 modulo 4, so 4 will not divide this number and therefore we will say that 2 exactly divides 5 power 2 to the n plus 1. And so collecting the powers of 2, we get that 2 to the n plus 3 divides 5 to the 2 to the n plus 1 minus 1. So, by induction, we are done with this proof. The only thing that we have to remember is that when you are putting the powers of 2 as power of 5, then there is an exact power of 2 that divides this power of 5 minus 1. So, that will help us compute the order of 5 modulo 2 power n and this is the thing that we are going to use to prove our next result.

(Refer Slide Time: 9:18)



So, our next result is when we look at the group Un, this is isomorphic to C2 cross C 2 by 4, I 4have already told you that we are going to prove this result.

(Refer Slide Time: 9:40)



But we are going to prove something more general. So, what we are going to prove is the following thing. We will produce generator for each of these, we observe that C2 is simply the group of square roots of 1 in this Un and we are going to write C n by 4 as the group generated by 5 powers. So, we will need to prove that the order of 5 in U2 power e is 2 power e minus 2, this is one thing that we will have to prove. And 5 power i is not equal to minus 1 for any i.

When we talk about 2 groups being isomorphic or one group Un being isomorphic to product of 2 of its subgroups, this is what is called as the internal direct product. You have one group, a finite group preferably which we have here and then there are 2 subgroups sitting in them, there are some conditions when the product of these 2 sub groups is isomorphic to your group. Condition number 1 being that the two subgroups commute with each other.

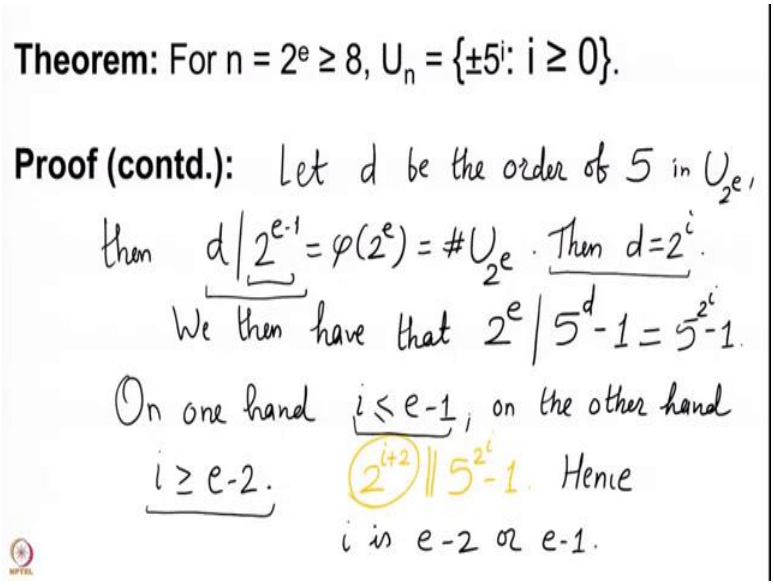
Meaning if you take an element from one group and another element from the another group, then these 2 elements commute with each other, which is satisfied in our case, because our groups are all abelian. So, this condition number 1 is satisfied. Second thing says that there is no intersection in these two subgroups. So, this is the statement that I have written here that 5 power i is not minus 1 for any i.

And then the third theorem will say, third part of the statement says that the product of the cardinalities of these 2 subgroups is equal to the cardinality of the group. So, that you get everything in the group as coming from this direct product. So, that will also follow once you have the correct cardinalities of the groups. If you show that this subgroup has cardinality n

by 4 by showing that the order of 5 is this, this is 2 power e upon 4, then we are done as long as we prove that 5 power i is not minus 1 for any i.

So, there are 2 things that we have to show, we have to show that the order of the element 5 is the correct number 2 power e minus 2 and we will then show that 5 power i cannot be equal to minus 1 in this group, then we are done. Then we will simply call upon some result in group theory, use that and deduce our result. So, we are going to do only the number theory part here and not do any of the group theory part. So, the first part in number theory is to show that the order of 5 is the exact number that we want.

(Refer Slide Time: 12:56)

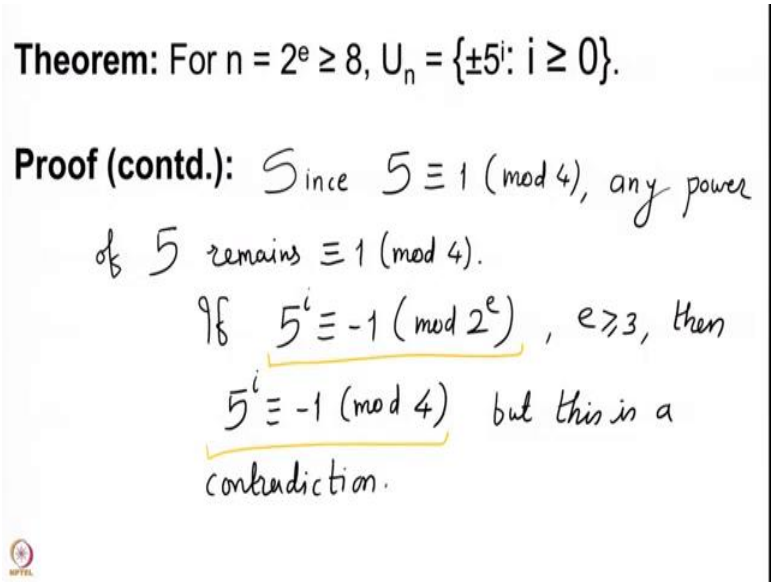


So, let d be the order of 5 in U2 power e then we know that d has to divide 2 power e minus, 1 which is 5 2 power e, which is also the cardinality of this group U2 power e. We then have that 2 power e divides 5 power d minus 1 this is because, the order of the element 5 in U2 power e is d. So, 5 power d is 1 in our group U2 power e, which means that in the residue class language the element 2 power e divides the difference of these 2 natural numbers 5 power d and 1.

Now, we have already deduced something about powers of 2 being divisors of powers of 5 by a power of 2 minus 1. So, when you have 2 power e dividing 5 power d minus 1, we of course, observe that this d has to be a power of 2. This is because d divides a power of 2, so the only way we have d dividing a power of 2 is that d itself be a power of 2. So, I will write this as 5 power 2 to the i minus 1. So, on one hand i is less than or equal to a minus 1, this is because d divides this.

On the other hand, i has to be bigger than or equal to e minus 2, this is because we know that the exact power of 2 that divides 5 power 2 power i is 2 power i plus 2, this is the exact power of 2 which divides this. If you want this to be 2 power e then i plus 2 is e and therefore, i is e minus 2. So, the possibilities for i from these two things is that e minus 2 or e minus 1 these are the only two possibilities. Either your element 5 is a primitive element which will generate everything if the order is e minus 1, 2 power e minus 1, or its order is 2 power e minus 2.

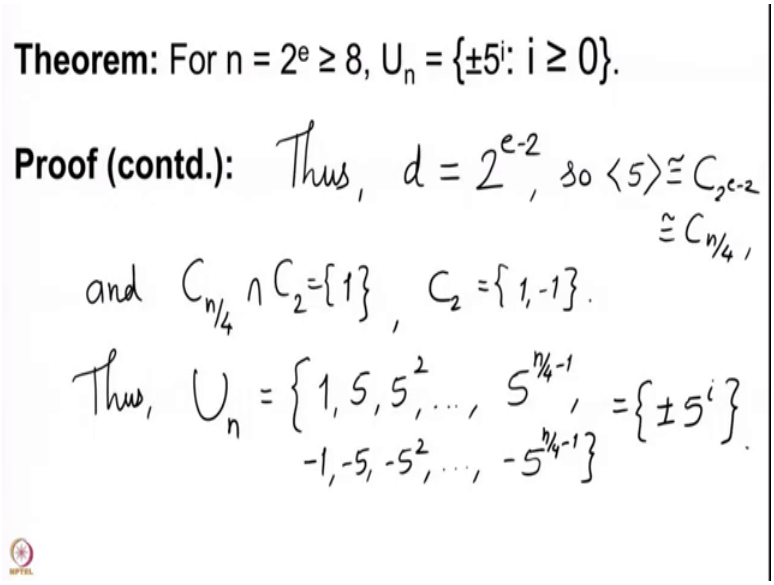
(Refer Slide Time: 16:19)



And here is what we note, the another thing. Since 5 is congruent to 1 mod 4, any power of 5 remains congruent to 1 modulo 4. If we have 5 power i have to be congruent to minus 1 mod any of this 2 power e, where we remember that we are taking e to be bigger than or equal to 3, then 5 power i will give you minus 1 mod 4 as well. because this will tell you that 2 power e divides the difference of these two and 2 power e being a multiple of 4, it will tell you that this should also happen, but this gives you a contradiction.

So, this statement does two things in one go, it tells you that no power of 5 can be minus 1. This is what we wanted to show when we wanted to show that the elements in the C n by 4, the elements in the group generated by 5 has nothing in common with the subgroup of order 2, 1 and minus 1, that is 1 thing which is proved by this. Second thing which is proved by this is that 5 cannot be a primitive element. because if I was a primitive element if the order of 5 was 2 power e minus 1, then its powers will give you all the elements in U2 power e, in particular, it will give you minus 1 as well, but that is not possible.

(Refer Slide Time: 18:28)



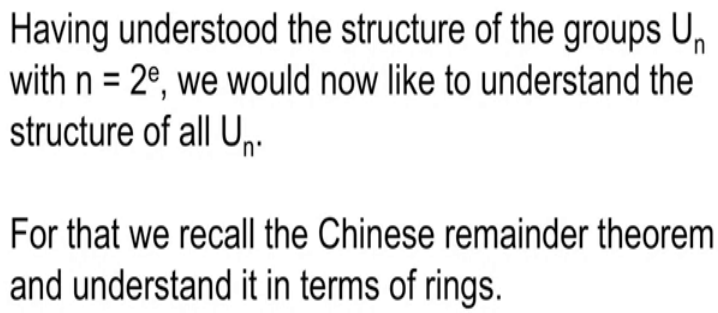
So, this tells you in one shot, thus d which is the order of 5 in that group is 2 power e minus 2. So, the group generated by 5 is indeed a group, cyclic group of order 2 power e minus 2 which is same thing as cyclic group of order n by 4 and this C n by 4 has only the trivial intersection with our group C2, where remember C2 is simply plus or minus 1. So, every element in the group Un is now of the form 1, 5, 5 Square dot dot dot 5 to the n by 4 minus 1, these are the powers of 5 and then you have minus 1, minus 5, minus 5 square, dot dot dot minus of 5 to the power n by 4 minus 1.

So, what we have got is that our whole group can be written in the correct way. So, we have now determined the structure of Un when n is a prime power. If the prime happened to be an odd prime, then Un is a cyclic group, if the prime happens to be equal to 2, then U 2 is trivial, U4 is cyclic of order 2 and 8 onwards Un is C2 cross a cyclic subgroup of the correct order. This tells us everything about U p power e, it gives us the structure completely. And now, the time has come that we move to general Un, we would like to understand the structure of all Un, whether n is a prime number, whether it is a prime power or whether it is a composite number.

And our experience so far tells us that whenever we have understood things from 4 prime powers, we can use some nice theorem and get the information about all Un. And here we are going to use one theorem which we have proved quite some time back. The theorem is called the Chinese Remainder Theorem.

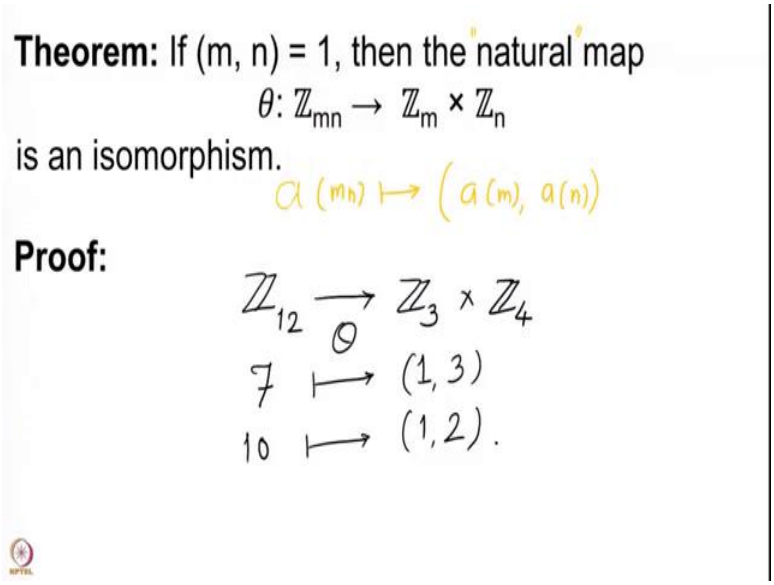
If you remember this statement of the theorem, it told you that if you have linear congruences, simultaneous linear congruences modulo some numbers ni which are co prime, pairwise co prime, then any such simultaneous system of linear congruences has a unique solution modulo the product of those moduli, modulo the product of those ni, this is what we had. But, so, when we did Chinese remainder theorem, we did not want to use the language of group theory or ring theory.

(Refer Slide Time: 21:44)



What we now are going to do is to understand this Chinese remainder theorem and understand it in terms of rings. We will understand it in the language of ring theory. It is a very space say, a simple statement that we are going to state but with the help of this statement, we will understand the Chinese remainder theorem and we will also have some understanding of Un with the help of this theorem.

(Refer Slide Time: 22:12)

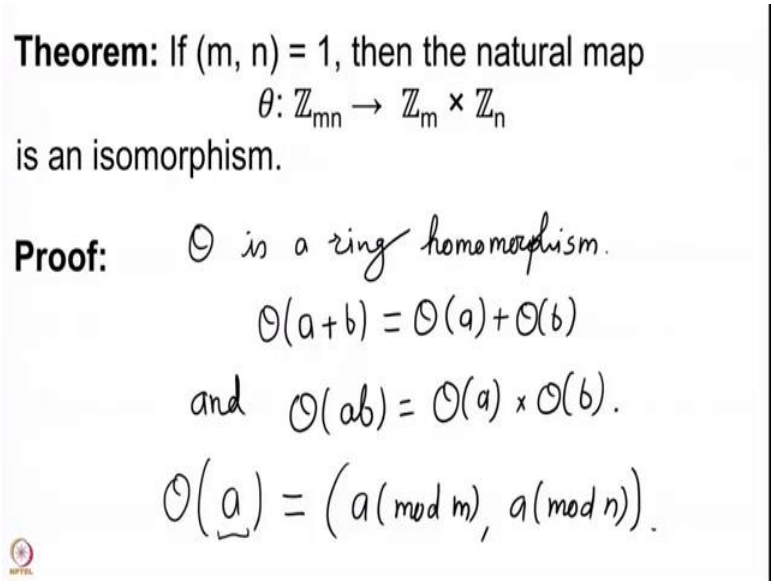


So, the theorem says the following, if you have two co prime elements, two co prime natural numbers m and n, then the natural map which goes from the residue classes modulo mn to the residue classes modulo m cross residue classes modulo n is an isomorphism. What is the natural map? So, the natural map is the map as follows, here we start with an element a mod mn and we send it to the pairs of the same a modulo m and the same a modulo n.

When we write the things in bracket, when we say am, it means that you are looking at the a modulo the natural number m, and the further one is the a modulo the natural number n. So, for instance, if you were looking at Z by 12 Z, then let me just understand this map for you. We will have the map going to Z by 3 Z cross Z by 4 Z. And if I were suppose looking at the element 7, I would send it to 7 modulo 3 which is 1, and 7 modulo 4 which is 3.

Or if I were looking at the number 10, this would be sent to 10 modulo 3, which is 1 and 10 modulo 4, which is 2. This is our natural map theta. Natural map has a very well defined meaning in mathematics, but let us not go into that right now. What we mean here is the most natural map that one could think of given the whole situation. So, this is our natural map.

(Refer Slide Time: 24:09)

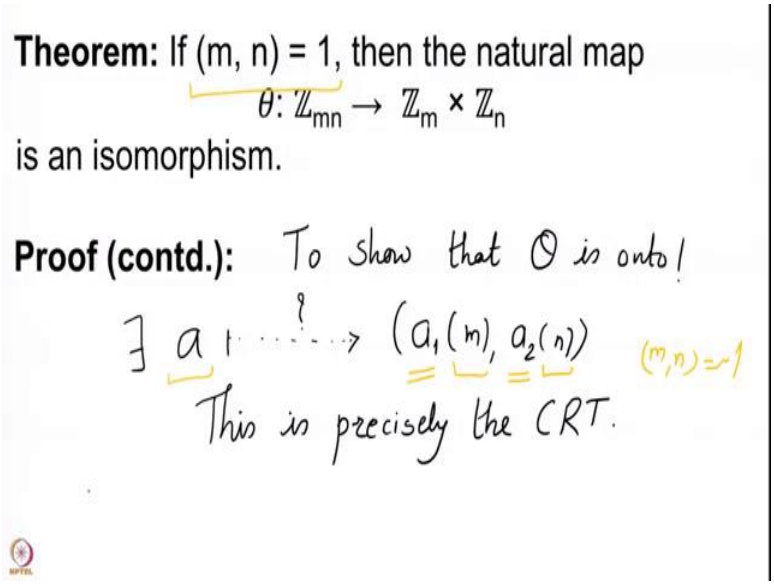


We need to make one observation, that whatever we have discussed here, the map theta is a ring homomorphism. So, I will simply state what we mean by this, we mean that whenever we have 2 elements in Z mn, then phi, sorry we should not call it phi we should call it theta, theta a plus theta b it preserves addition and it also preserves the multiplication which is theta a b is theta a into theta a into theta b. So, these are the two properties of Theta that we will assume.

We will not prove this, but this is clear because what we have defined for U, let me just recall this follows because we are going to define our theta by taking the a modulo m and the a modulo n. There is also the small thing of showing that theta is well defined, because here I start with a modulo residue class of a modulo mn and the same residue class of a may be given by another element b coming from natural numbers.

So, you will then have to show that when a is congruent to be modulo mn, a is congruent to b modulo m and a is congruent to b modulo n. This is a simple checking that that needs to be done or you should at least spare a few seconds to think about this, it is important. So, the takeaway from this slide is that theta is a ring homomorphism. To say that this is an isomorphism, we will need to show that theta is onto and that theta is one-to-one.

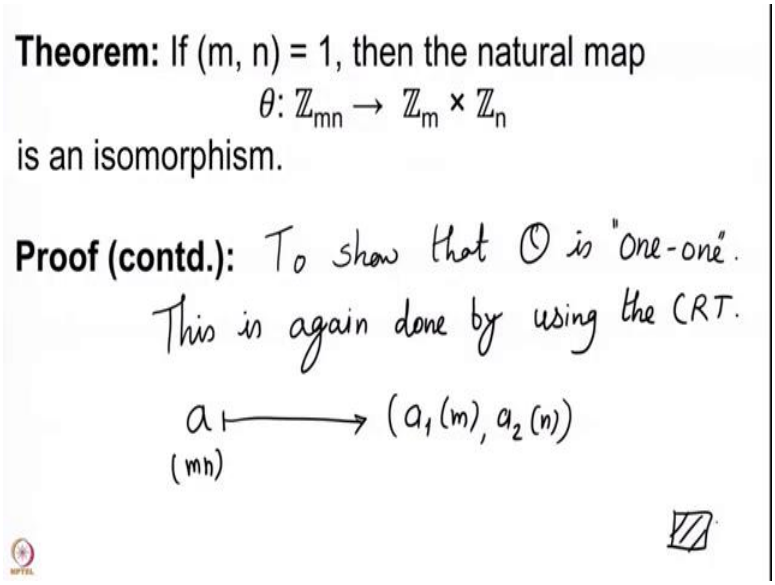
(Refer Slide Time: 26:28)



To show that theta is onto, what do we have to do to show that theta is onto? This is done by showing that whenever I start with any a1 modulo m and any a 2 modulo n, then there is some element a modulo mn which maps to this particular element does there exist some such a much to show that Theta is onto we will need to produce that there is an a with this property, does there exist such an element a, but this is precisely the Chinese Remainder Theorem.

Chinese Remainder Theorem tells you that when you have 2 moduli which is co prime, which here they are m and n, we assume that mn are co prime, this is given to us in the statement already. So, for any a1 and any a2, you have a natural number a satisfying that a is congruent to a1 mod m and a is congruent to a2 mod n and then you will simply look at that a modulo mn. So, the Chinese remainder theorem gives us the ontoness.

(Refer Slide Time: 28:10)



And finally, we need to show that theta is injective or that it is a one-to-one map. So, to show that theta is one-to-one and this is shown again, this is again done by using the Chinese Remainder Theorem. Remember the second part of the Chinese Remainder Theorem told you that when you take any a1 mod m and any a2 mod n, the solution a that you got here is unique modulo mn. The uniqueness is precisely the one-to-oneness that we are looking for. So, in a way, the statement that we have written here is nothing but a reformulation of the Chinese Remainder Theorem.

In fact, if you have this statement, you can deduce Chinese Remainder Theorem as a corollary from here and conversely, this statement also follows from the Chinese Remainder Theorem. We will stop here for this lecture. In the next lecture, we will see how we can use the prime factorization of a given element n in terms of prime powers, use this version of Chinese remainder theorem and get information about the group of units modulo n. See you until then thank you.