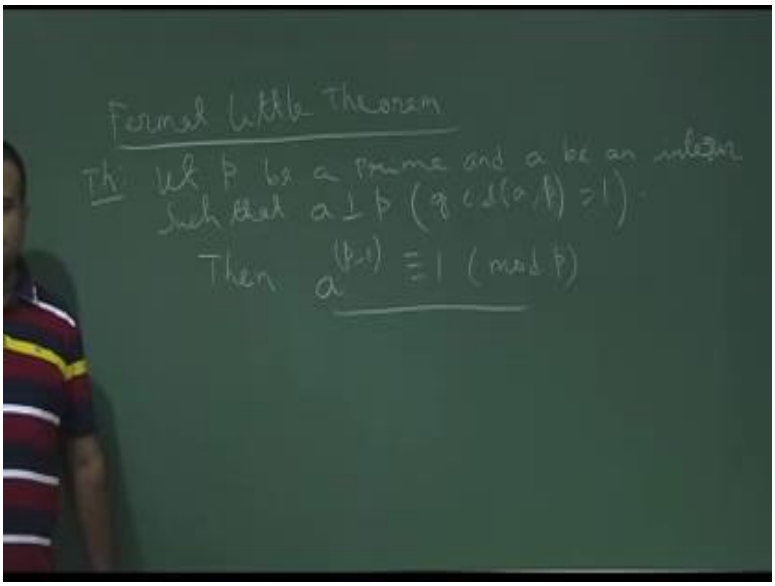
Internetwork Security
Prof. Sourav Mukhopadyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 18
Fermat's Little Thermo,
Euler Phi-Function

We talk about Fermat's theorem, Euler's theorem. Before that we talk about Fermat's theorem Fermat's little theorem and then the Phi-function and then we move to the Euler's theorem in this lecture.

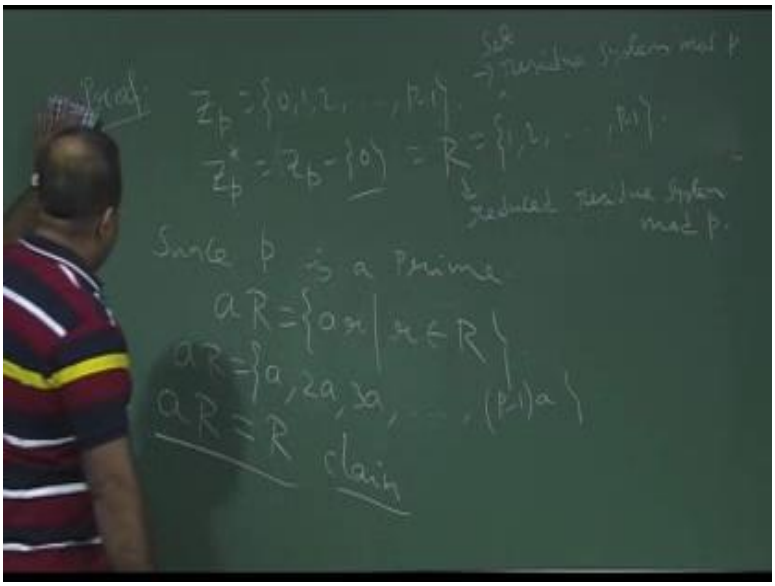
(Refer Slide Time: 00:35)



So, let us just talk first talk about Fermat little theorem. This is a particular case of Euler's theorem, but this independently invented by the Fermat in Fermat long time back before the Euler's theorem. So, the statement of this theorem is let p be a prime and a be an integer such that a is co prime to p; that means gcd of a and p are, a and p is 1, then a to the power p minus 1 if congruent to 1 mod p.

So, this is the statement of this Fermat's little theorem. It is telling if you taken n prime p and if you take a integer a which is co prime to p then a to the power p minus 1 is congruent to 1 mod P.

(Refer Slide Time: 02:23)

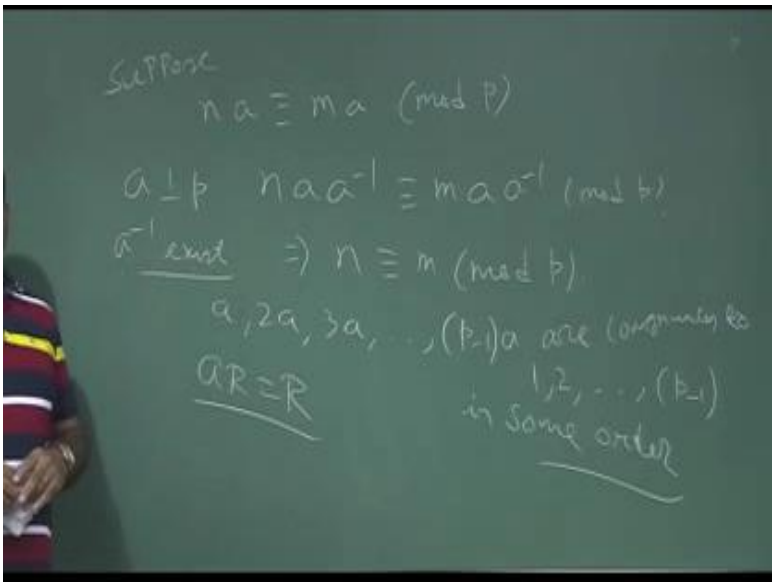


So, how to prove this? So proof of this theorem; the p is a prime so let us consider Z p; Z p is nothing but 0, 1, 2 up to p minus 1. And if you take the Z p star the group cyclic group it is basically Z p minus 0. This is also denoted by r, this is called a residual system modulo p class reduce residue system modulo p, this is called the residue set of the residual system modulo p; residual system mod p and this is called reduce the cyclic group 0 is not there reduce residual system mod p. This we denote by R, R is basically Z p star but cyclic group.

Now, since p is a prime then we can show that a R, a R this is basically set of all element a R such that r is coming from this. So, a R is basically this set. So, a, 2 a, 3 a, dot, dot, dot, like this p minus 1 a; this two set are basically same a R and r. This we have to prove. Our claim is; this is our claim. Our claim is these two set are basically same. That means, number of elements over here is same as number of element over there. So, this r is basically nothing but 1, 2 up to p minus 1.

Basically if you take any two elements from here if we can show that they are congruent then these two set (Refer Time: 04:59) is same. So, how to prove these two set are same. So, let us try to prove that.

(Refer Slide Time: 05:13)

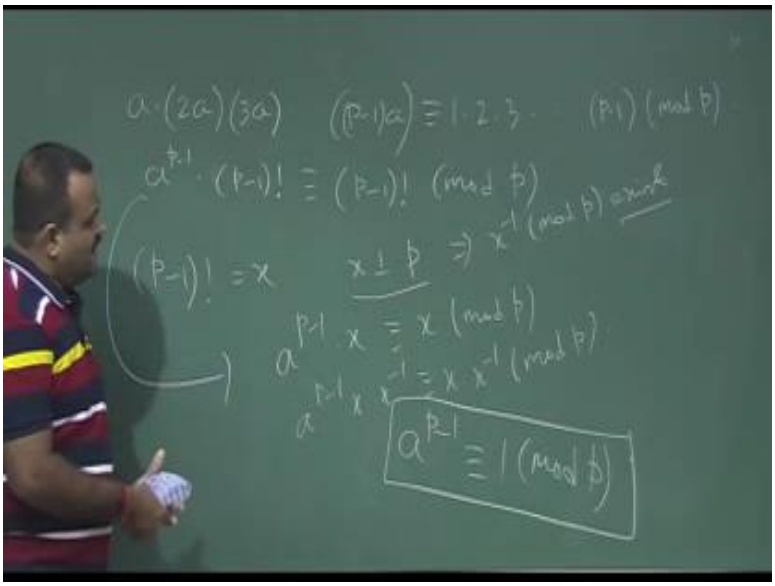


If you take any two element from here say n a, if we assume they are congruent m a mod p suppose. So, n a and m a we are taking from here. So, our claim is that no two elements from this set are congruent. So, these are all distinct element, so if these are all distinct element then that is basically R. So, to prove that suppose they are not distinct; suppose there are two element n and m, n a and m a where a n and a m are less than p minus 1 less than or equal to are same, then what we can say?

Now a is co prime to p. So, a is co prime to p so that means, a inverse exists, a inverse not p exists. So, we will apply a inverse on both side this is congruent to; sorry a and a inverse mod P. So, this incline n is congruent to m mod P. That means, all the elements over here are; so a, 2 a, 3 a, p minus 1 a, are basically are congruence to the set 1, 2 up to p minus 1 in some order. That means, a R is equal to r. So, these two set are same.

Now, since these two set are same so we can multiply the element.

(Refer Slide Time: 07:31)

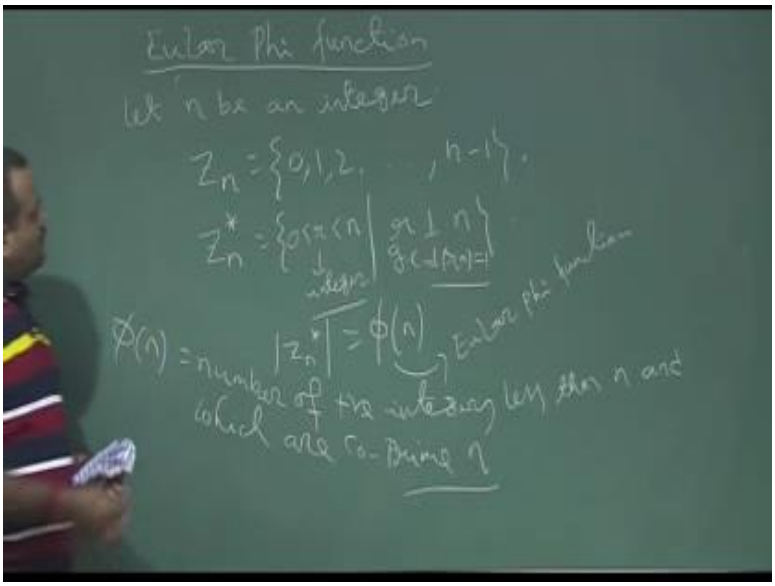


So, if you multiply the all the elements in a R. So, it is basically a into 2 a, into 3, into p minus 1 into a. So, these are the elements in a R, so they are basically same as the element in R, so in congruent cells under mod p operation. That means, this set must be congruent to in some order need not be a is congruent to 1. So, in some order they are congruent to this set 1, 2 up to p minus 1. So, this will give us what? This we can take a common a to the power p minus 1 into this is basically 1, 2, 3, up to p minus 1, so p minus 1 factorial is congruent to p minus 1 factorial mod P.

So now, p is a prime since p is a prime, so p has no factor from this 1, 2 up to p. That means, p minus 1 factorial if we denote by say x. So, x is independent, x is co prime to p. So, from here we can apply, so this is basically a p minus 1 into x is congruent to x mod p. Now since it is co prime this imply x inverse mod p exists. So, we can apply x inverse on both side, x inverse mod p, this will give us basically the Fermat's little theorem congruent to 1 mod p.

So this is the proof of the Fermat little theorem. So, this relationship hold when p is a prime and a is a co prime to p; a is any integer which is co prime to p. This is the Fermat little theorem. So, this was invented long before the Euler's theorem, we will talk about Euler's theorem which is a generalized form of this, but this was independently invented by Fermat; that is why it is called Fermat little theorem.

(Refer Slide Time: 10:31)



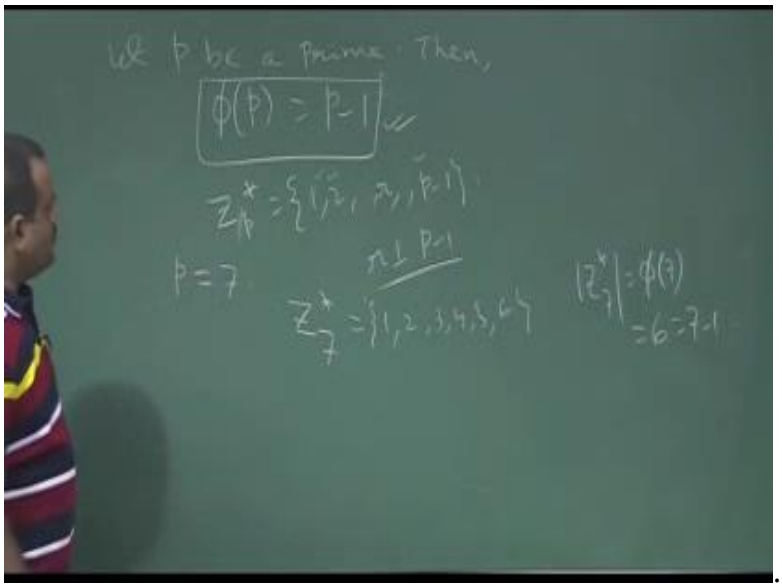
So, now we define Euler Phi function. So, Euler Phi function let n be an integer we take it is in positive integer then we know this set Z n, Z n is basically 0, 1, 2 up to n minus 1. And then we know Z n star; Z n star is basically set of all integer less than n such that positive integer less than n such that they are co prime to n. So, this is the positive integer so maybe we can write it properly 0 less than r less than n; r is an integer. So, set of all integer which are relatively prime to n which are co prime to n.

So, then this set along with this operation can form a group, not for all composite number it will form a group so for some composite number it will form a cyclic group. Now this cardinality of this set is denoted by phi of n; Euler Phi function. This is called Euler Phi function; cardinality of this set that means number of element in this set is denoted by Euler Phi function, it is a number. That means, this is denoted by this is the number of positive integers less than n and which are co prime to n; that means, those integer whose gcd is basically gcd of r and n r 1. So, that number is called Euler Phi function. So, Euler Phi function phi of n is just the number of integer which is less than n positive integer and which are co prime to n. So that means, under Z n under modulo n this n has the inverse.

Now, we want to know the number of element, I mean we want to know phi n in general; what is phi 7? What is phi 8? What is phi 9 in general? So, if n is a prime number then

we know the phi n. So, for a prime number Euler Phi function is basically if prime number is p then it is p minus 1.

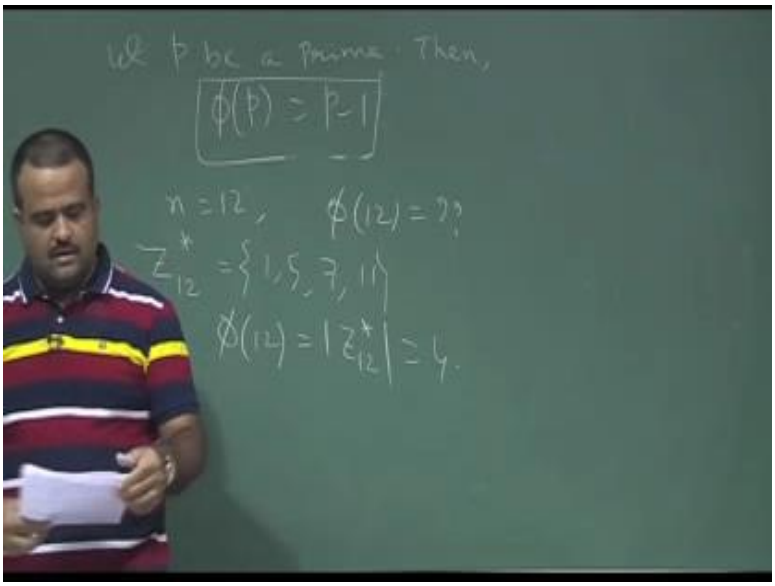
(Refer Slide Time: 14:17)



So, let p be a prime then phi p is basically p minus 1, because if p is a prime then there is no element we should divides p. That means, Z n star is basically; so we will not take 0 so that is r is so 1, 2 up to p minus 1, because p is prime. So, Z p star; p is prime so that means all the elements are, if this is r; all the elements are relatively prime with p since p is a prime number otherwise it cannot be a prime number if it has affected.

So, since p is a prime this is quite straight forward. Then the number of element in here is p minus 1. Say for example, if phi is equal to 7; if phi is equal to 7 then we know 7 star is basically 1, 2, 3, 4, 5, 6 the number of elements which is basically phi 7 is basically 6 which is basically 7 minus 1.

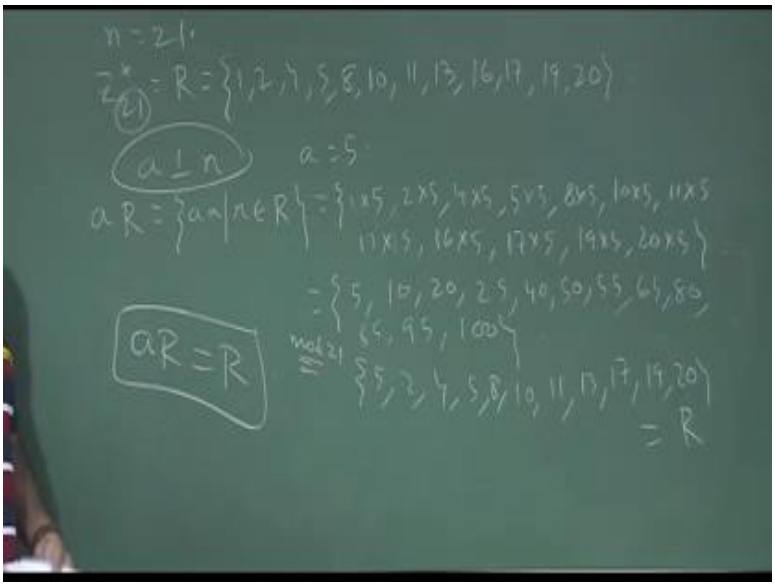
(Refer Slide Time: 16:09)



Now, suppose p is not a prime, suppose n is not a prime; suppose n is equal to say 12 and we want to what is phi 12. So, for 12 what is our Z 12 start? So, Z 12 star is basically set of all integers which are less than 12 and which are relatively prime with 12. So, this is basically 1, 5, 7 11. So, basically phi 12 while on phi function only 12 is basically cardinality of this set which is basically 4.

So, we want to have a formula for finding the cardinality of this set that means phi function in general where n is not a prime. So, we want to have a formula for this phi function when n is not a prime.

(Refer Slide Time: 17:25)

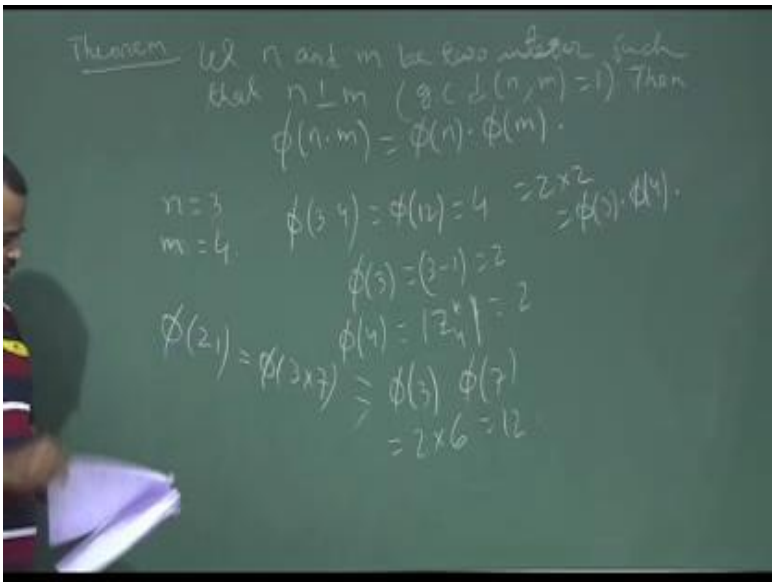


So, this will let n is; so this we will define let us take another example suppose n is equal to 21. So, if n is equal to 21 then that Z n star Z 21 star which is basically R reduced residual class, reduce residual class that means we are taking all the integer which are co prime with this 21. So, this is basically 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 21.

Now if we take a number a which is co prime to n; that means n is 21 so if you take a is equal to 5. Then we want to define this a R; a R is basically set of all, so we multiply a with R so R is coming from this capital R. So, this set if we just for this example it is basically 1 into 5, 2 into 5, 4 into 5, 5 into 5, 8 into 5, 10 into 5, 11 into 5, then 13 into 5, 16 into 5, 17 into 5, 19 into 5, 20 into 5. Now this will basically give us 5, 10, 20, 25, 40, 50, 55, then sorry this is 5, 55 then 65, then 80, 85, 95, 100. Now if you perform the modulo operation mod 25, a 21, n is 25, 21 so if you take mod n on this then it will give us; so if we apply this mod 21. So, it will give us basically 5, 2, 4, 5, 8, 10, 11, 13, 17, 19, and 20. So, this is basically R set.

So, this theorem we have already proved that in general if a is co prime to n then a R is basically R. We have used in Fermat little theorem and this we are going to use for the proving the next result on Euler Phi function. So, this is my example, this is basically we are getting R back. So, this is my example that we have already proved this theorem. So, now let us talk about the general form of Euler Phi function where the number is not a prime.

(Refer Slide Time: 21:18)

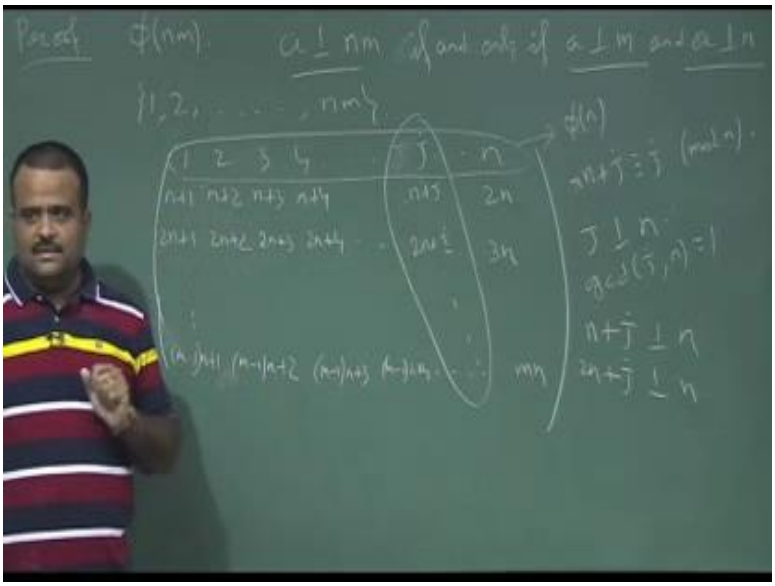


So, this is the theorem. This theorem is telling let n and m be two integer, two integer such that they are relatively prime that this gcd of n and m are 1. Then phi n into m is basically phi n into phi m; phi n into m is basically phi n into phi m. So, this is the theorem we have to prove this theorem.

So, before proving this theorem let us take an example suppose say- n is equal to say 3 and n is equal to say 5; sorry 5. That means, or if you take n is equal to 3 and m is equal to 4. Then we want to find phi of 3 comma 3 into 4, so this is my basically phi 12. So, phi 12 we have seen it is basically 4. Now what is phi 3? 3 is a prime, so phi 3 is basically 3 minus 1 it is 2. Now what is phi 4? Phi 4 is basically cardinality of Z 4 star, so it is basically 2. So, this is basically 2 into 2, this is basically phi 3 into phi 4.

Again for say phi 21 how to find phi 21? Phi 21 is basically phi 3 into phi 7; sorry this is go to here. So, this is the basically phi 3 into phi 7, so if this 7 and 3 are relatively phi so if you use this result then we can say this is basically phi 3 into phi 7. So, this is basically if this is prime this is 2 into 6; 12. So, phi 21 is basically 12, and we have seen the phi 21; the elements of phi 21.

(Refer Slide Time: 24:42)



So, now we need to prove this theorem in general. So, let us try to prove it. So, how to prove this theorem? First just erase this gets more space; so we are looking for finding phi m into n where m n are relatively prime. That means we are looking for all number of integers which are less than m into n, m n and which are relatively prime with n m into n. So, that means if a is relatively prime with n into m this implies this is true if and only if a is relatively prime to both m and n. So, both has to be; so a is relatively prime to m into n if and only if a is relatively prime with m and a it is relatively prime with n; and if this is true this is vice versa.

Now we will write these elements 1, 2 we are looking for number of integer over here which are relatively prime with m into n. That means, which are relatively prime with both n and m. So, we will write this in a matrix form this set like this 1, 2, 3, 4, dot dot dot n. And then n plus 1, n plus 2, n plus 3, n plus 4 dot dot dot 2 n. 2 n plus 1, 2 n plus 2, 2 n plus 3, 2 n plus 4 dot dot dot 3 n like this. So, dot dot dot m minus 1 into n plus 1 then m minus 1 into n plus 2, m minus 1 into m plus 3, then m minus 1 into n plus 4 dot dot dot m into n.

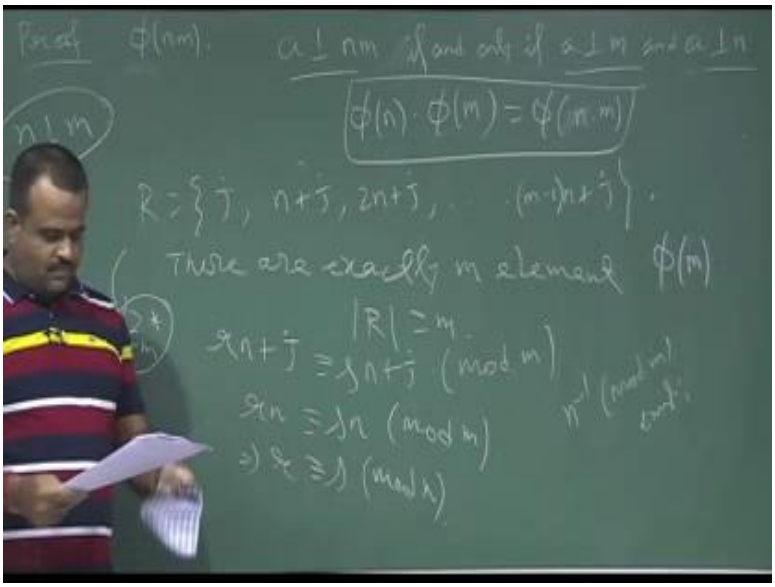
So basically, we are writing this set in a matrix form. Now we take a j over here, this column is basically if you take the j over here this column is basically n plus j 2 n plus j like this. So this is basically telling us; now the first row is basically number of integer co prime with n is basically phi n in the first row. And this is same as in the second row,

because n plus j is congruent to any row because this is r plus j is congruent to j mod n. That means, any row this is basically phi n is the number of integer which are co prime to n.

Suppose j is the integer; suppose j is co prime to n. Now these all are will be co prime to n, because if j is co prime to n then that means gcd of j and m is 1. That means, n plus j must be co prime to n 2 n plus j must be of co prime to m because there gcd also 1, so that means all the elements over here are co prime to n.

So, whenever there is a number which is co prime to n then in that column all the elements in that column; so this is a column j column then all the elements in this column will be co prime to n. And there are phi n numbers. Now we have to see that among these how many are basically co prime to m. So, that we have to see.

(Refer Slide Time: 29:51)



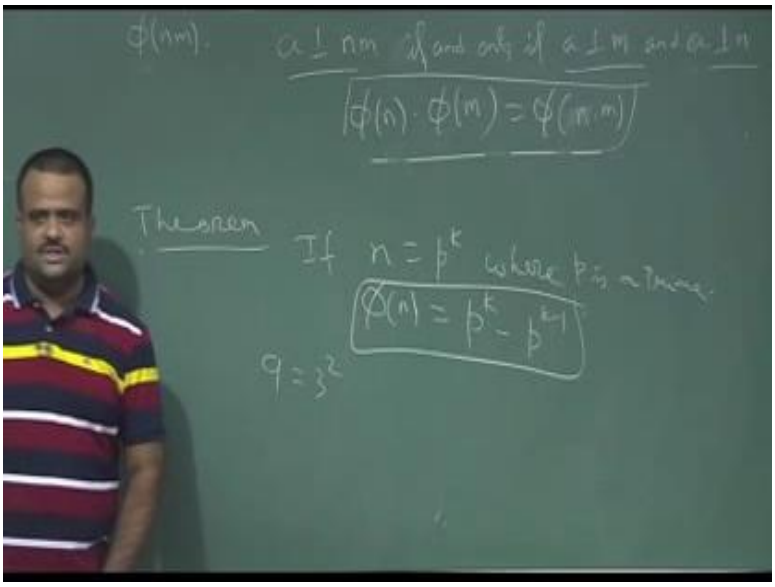
So, for that let us take this set. So, this R, we take J this is one column, n plus J, 2 n plus J this is the jth column; where all the elements are co prime to n. Now we want to see among these how many are basically co prime to m. So, they are exactly n element in this set, so that means this is m.

Now, if you take any two elements from here they are in this form r n plus J and if suppose they are congruent under mod n, we want to see whether this set is eventually Z m star or not; this we want to see. Yes, this is Z m star; so that means there are phi n

numbers of elements which are co prime to n. So, that we want to see under mode operation; mod m operation. So, if they are equal under mod m so that means, r n must be s n under mod m.

Now, n and m we have taken relatively prime; so that means n inverse exists under mod m, this exists under mod m. So, if this exists we can apply an inverse on this. So, this will give us r is congruent to s mod m. That means, they are congruent to s mod m.

(Refer Slide Time: 32:41)



So that means, this is basically this R is basically Z m star. That means number of element which are co prime to m over here is basically phi of m. So, among these there are phi m numbers of elements which are co prime to n and among this phi n there are phi m numbers of elements which are co prime to n. So total, hence the number of elements which are co prime to both m and n are basically phi n into phi m and this is basically phi n m, and this is the proof this is basically phi n m, and this is the proof.

So, just a quick result; so this we will use to calculate the phi function when m is not a prime and we need another result is this is also a easy to proof we are not going to prove this. If n is p to the power k where p is a prime and n is an integer then phi n is basically p to the power k minus p to the power n minus k. So, this result can be easily proved, but we are not going to prove it now. So, this is also used because if we want to calculate for say 9, so 9 is basically 3 square. So, p is prime, so we will use this result to prove that.

Thank you.