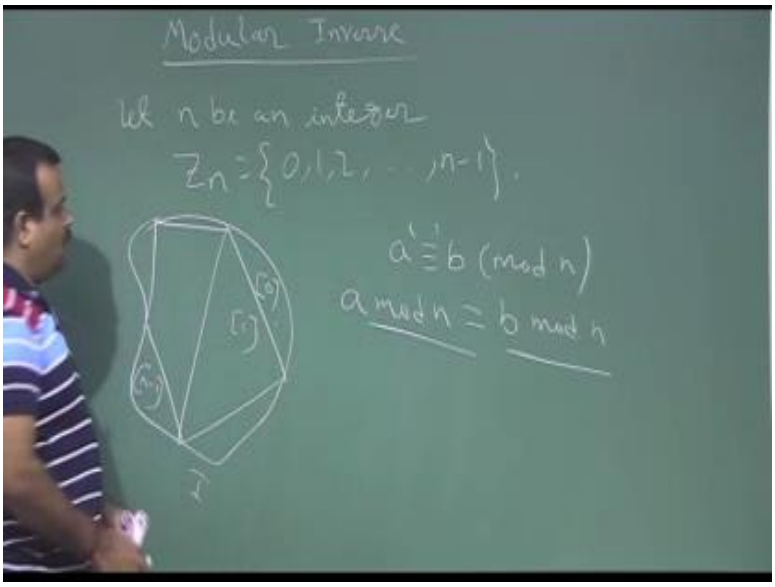
Internetwork Security
Prof. Sourav Mukhopadhyay
Department of Mathematics
Indian Institute of Technology, Kharagpur

Lecture - 16
Modular Inverse

We talk about inverse, Modular Inverse on mode operation on Z p. So far we have seen the additive operation on Z n.

(Refer Slide Time: 00:34)

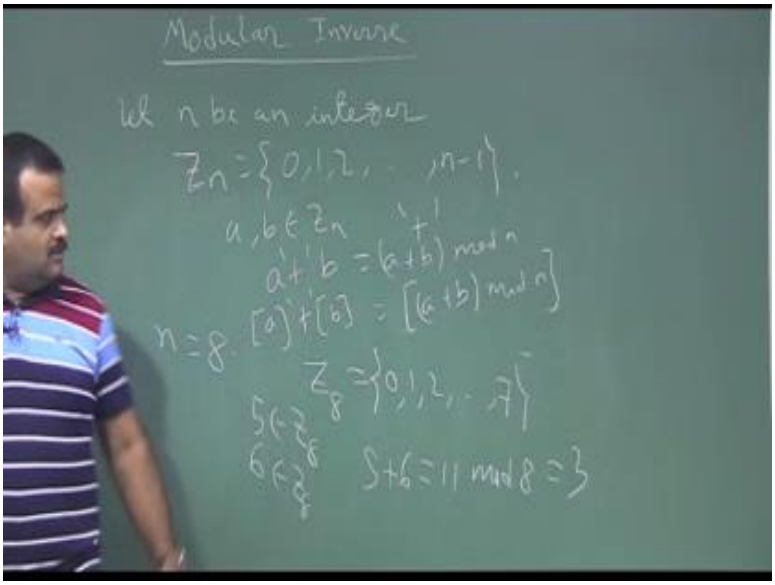


Let n be an integer then we have seen the Z n is basically the residue class if we take any integer if you try to divide by n. So, remainder will be from 0 to n minus 1 so that class of that class will give us the Z n. So, this is basically the, we have seen this is the residue class or the equivalence class because this, if a b, a is convenient to b mod n if a mod n is equal to b mod n. So, there are belongs to the same class. So, this relation we have seen is the equivalence relation and so, this will form, this is I set of integers. So, this will come, the partition over the integer set disjoint partition equivalence classes. So, this is 0 class, 1 class, dot, dot, dot, up to n minus 1 class.

In each class all the elements are under same under mod operations so; that means, if we take element form here if we divide by n the remainder is same as if you take any other element the remainder will be same. So, these are our equivalence class these are for

simplicity we will write this as this 0 to n minus 1. Then we have seen the operation on this if we take 2 element from this Z n.

(Refer Slide Time: 02:11)

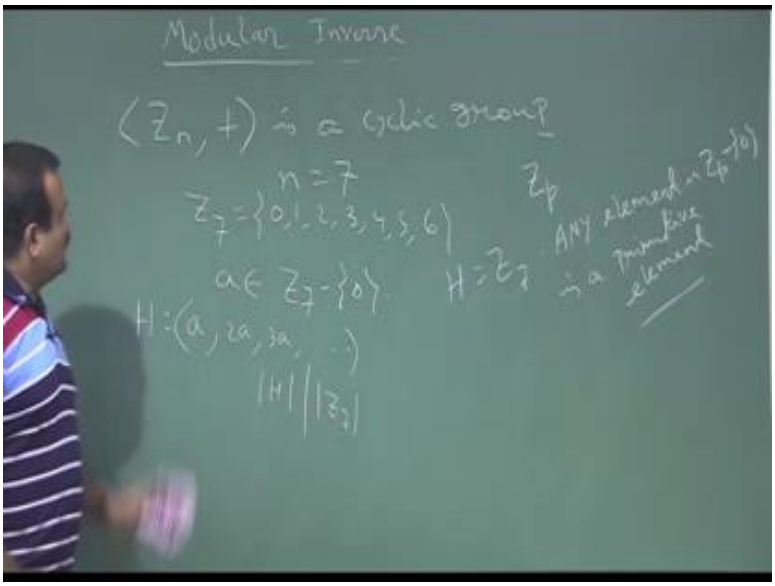


Then we have seen how to define. So, if you take 2 the element of Z n then a plus b. So, these class operations have defined like this a b mod n.

Basically if it is in box form, so, box form we are not writing for the simplicity, this is basically a b box or a b mod n anyway for simplicity, we just write not writing in the box form, but this is the way we define the addition so; that means, if you take Z say n is equal to 8. So, what is Z8? Z8 basically 0, 1, 2, up to 7, that means, if you take any integer, if you divide by 8 then the remainder will be from 0 to 7.

So, now, how we define addition, if you take 2 element from this say 5 and say 5 belongs to a Z 8 and 6 belongs to Z 8 d a b. So, 5 plus 6 which is basically if we do the integer addition it will give us 11, but 11 mod 8 which is basically 3. So, this we have seen and under this operation. We have seen this Z n is a cyclic group and 0 is the identity element of that group and every element has the inverse and 1 is the generator of this group, 1 can generate another group.

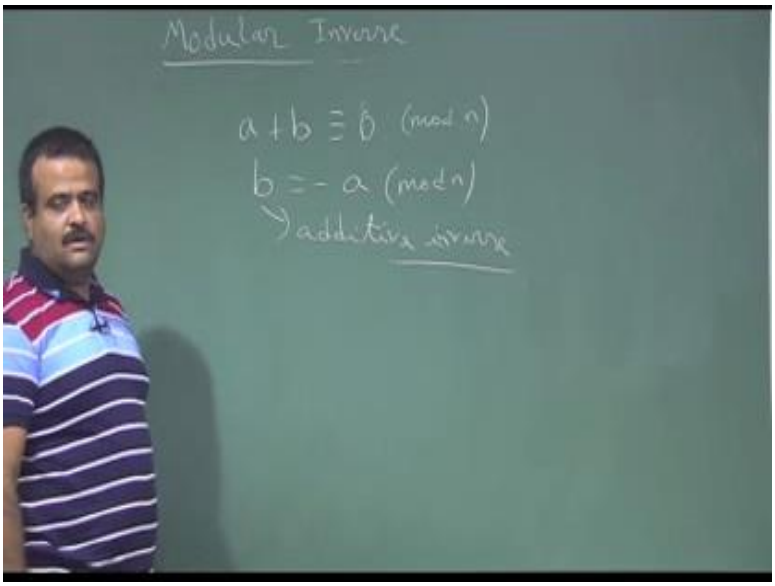
(Refer Slide Time: 03:38)



Now, if n is equal to say n is prime then say n is equal to 7. So, when n is prime then what is Z 7? 0, 1, 2, up to 0, 1, 2, 3, 4, 5, 6, then if you take any element a from this say it could be any of this other than 0, 0 cannot generate the group because if we operate 0 plus 0, it is always give us 0.

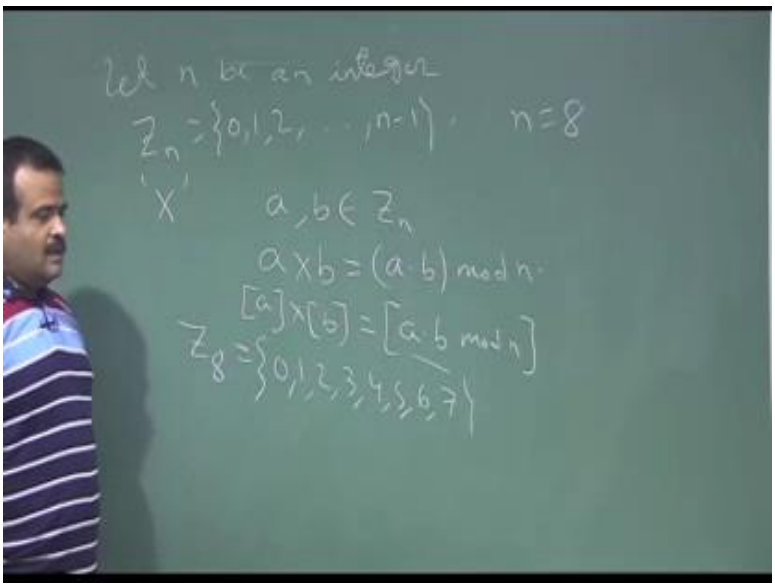
If you take any element other than 0 then the group then if we generate a group by this a so; that means, a a plus a that is 2 a we define 3 a like this. So, this will form a group and if we say this is H. So, we know the order of the group must divide order of the order of the subgroup must divide order of the group, but order of the group is 7. So, 7 is a prime number. So, 7 should not have any factor so; that means, this will be the H should be equal to the whole group Z 7; that means, if it is if p is prime then if we consider Z p then any element other than 0 in Z p minus 0 is the primitive element or is the generator primitive element in additive sense. So, for the operation we have defined the addition.

(Refer Slide Time: 06:02)



Now, we will define another operation and modular inverse under additive sense is the inverse. So, a, b will be called inverse of a if b is equal to 0 mod n then the additive sense b is denoted by minus a mod n. So, this is the additive inverse because the operation is addition. Now we define another operation on this said Z n which is basically multiplication operation.

(Refer Slide Time: 06:44)

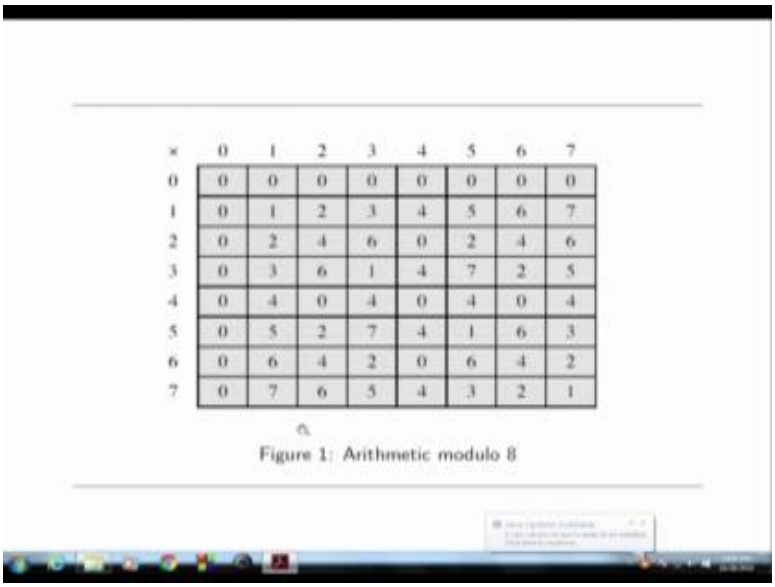


Again let n be an integer then we consider the said Z n which is basically 0, 1, 2, up to n minus 1, now we define this operation; multiplicative operation as follows, if we take 2

element from Z n then we define a cross b is basically a into b mod n. So, in a box form if we write, this is basically a into b mod n. So, this into is basically the real number multiplication. So, for simplicity we will just remove the box, this is basically a into b is basically a into b the integer multiplication or real number multiplication mod n. So, this is how we define the multiplication.

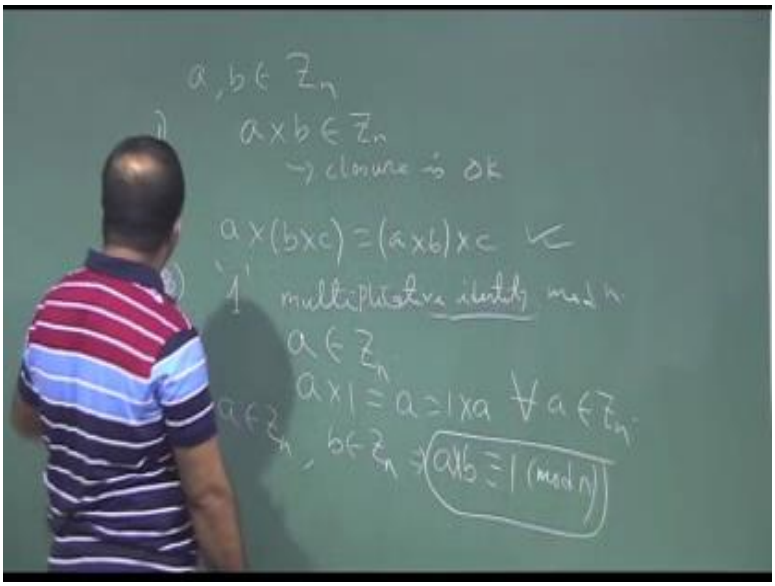
Now, we can take an example suppose n is equal to 8, if n is equal to 8 then what is Z 8? 8 is basically 0, 1, 2, 3, 4, 5, 6, 7, so, there are any 8 elements up to 0 to 7. Now let us define this operation. Can you please come to the slide?

(Refer Slide Time: 08:21)



So, this is the arithmetic operation on a multiplicative multi multiplication on Z 8 elements of Z 8. So, the elements of Z 8 are written as 0, 1, 2, up to 7, this is a say, this is b, now this is a into b. So, if it is 0 all are 0 if it is 1, so this is a, this is b, if it is 1. So, a into b, so, this show you all give us 0 one like this 2, 2 into 1 is 2, 2 into 2 is 4 and, but 2 into 10, 2 into 8, 2 into sorry 2 into 4 is 8, but 8 mod 8 is 0. So, 2 into 5 is basically 10 and 10 mod 8 is 2. So, that is why it is like this. So, similarly we can verify the other. So, suppose a is 4 and b is say 5. So, a into b is basically 20 mod 8. So, 20 mod 8 is base basically 4. So, that is why a it is 4. So, this is the table where we are performing this multiplication operation on the Z 8.

(Refer Slide Time: 09:55)

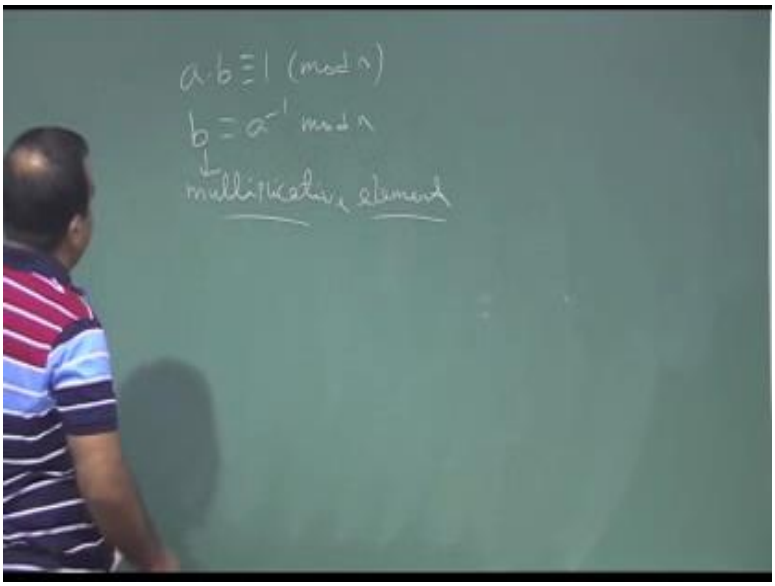


Now we see whether under this operation we can have a group. So, for group we need to have few properties like closure property which is quite obvious if we take any 2 elements from Z n then a cross b is also belongs to Z n because we are multiplying and taking the mod. So, it will also belong to Z n. So, so closer property is done closer is Ok.

Now second property is associativity property; that means, if you take any 3 element a b c this is also can be easily verify. So, this is also this is can be easily verified by the associative property of the real number multiplication now the inverse. So, existence of inverse we have any element. So, '1' is the basically serve as the inverse we called it multiplicative inverse multiplicative inverse mod n because if we take any element a from this Z n then if we multiply this by 1. So, this will give us basically a which is minus one into a and this is true for all a belongs to Z n. This implies sorry multiplicative identity this is not inverse multiplicative identity sorry this is multiplicative identity.

So, 1 is served as a multiplicative identity of that operator this multi under the multiplication operation so, but inverse. That means, for let a b an element in Z n. So, a then b will be said as the inverse of a. So, if we multiply this it should give us the identity element under mod n. So, this should give us, a dot b should be congruent to one mod n. So, then it is called b is called a inverse mod n.

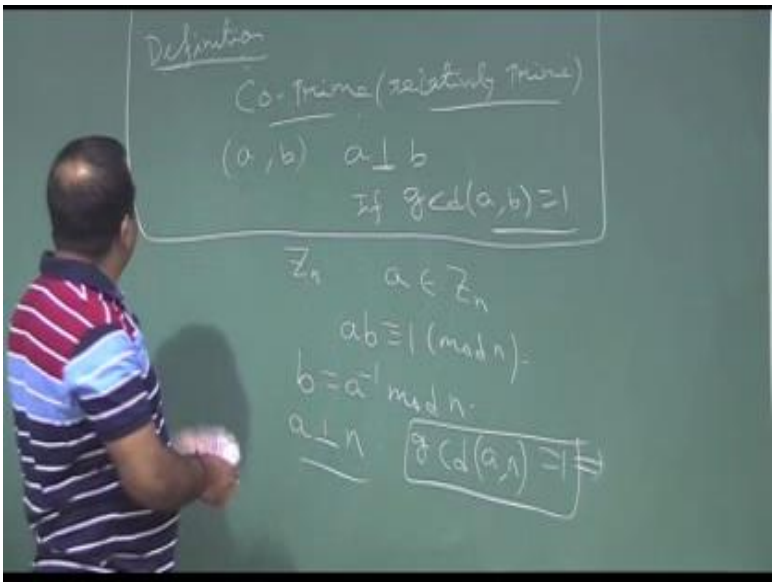
(Refer Slide Time: 12:21)



If a dot b is congruent to 1 mod n then b is called a inverse mod n this is the multiplicative inverse it may exist, may not exist, if it is exist for all the elements then we call inverse exists then it could be a group because all the other properties are there. So, a b mod n means so a b mod; a b, a into b is congruent to 1 mod n.

Let us look at this table. So, here if you see 1 is served as identity element multiplicative identity element because if you multiply one with any other element it is give us that element. So, one into 3 is basically 3 one into 5 is basically 5. So, 1 serves as identity element of this group under the multiplication. But if we take 2 as a whether to has inverse or not. If we have to have a inverse then there should existed b here such that 2 into b should give us one, but there is no one exists. So, 2 has no inverse under mod 8. But if you consider 3 then we see here is a one so; that means, 3 has a inverse. So, that is also that is also 3. So, 3 have a inverse under mod 8 and if you take 4, 4 has no inverse under mod 8 if you take again 5. So, 5 has inverse under mod 8 which is again 5. So, 6 has no inverse because there is no one in this row, but 7 has a inverse which is 7. So, if a is equal to 7 then b is equal to 7 is the inverse mod 8. So, for inverse we need to have a into b is congruent to 1 mod 8. So, it is not necessary that every element will have inverse. So, that is the multiplicative inverse.

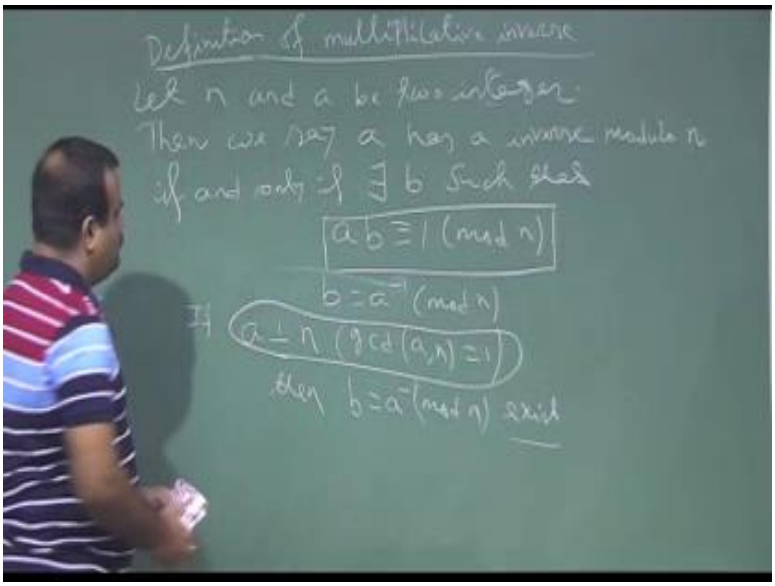
(Refer Slide Time: 14:55)



Now, we define when we say 2 elements are co prime or relatively prime this is the definition; definition of co prime or relatively prime. We say 2 element a b are co prime we denote this by this is a co prime to b this is, at this is the notation we can use if gcd of a b is 1, if the gcd of a b is 1 then we say that a is a, a b are co prime or in other word a b are relatively prime. So, this is the definition of co prime.

Now we will, that means, so, suppose we are considering Z n and we say that if a if you take a element a belongs to Z n and a will have a inverse if there exited b such that a b is congruent to 1 mod n then we can say that then b is the basically a inverse mod n then we can say that a is co prime with n, so that means, if the gcd of a and n are 1 then only inverse exists then only a inverse exists and this is the condition of having the inverse under mod n. So, we take integer n which we take another integer and we say a is having a inverse this is the definition of inverse multiplicative inverse under mod n. So, what is the definition? So, you can just write the definition of multiplicative inverse.

(Refer Slide Time: 17:17)

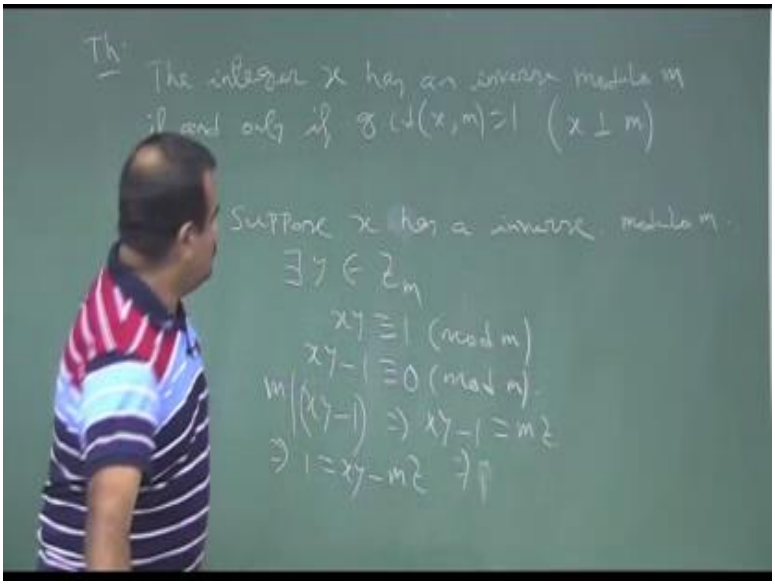


Definition of multiplicative inverse so, let n be a, n and a be to integer then we say we say a has a inverse, this inverse is basically multiplicative inverse, inverse under modulo n if and only if there exists a b such that. So, a here a b are belongs to Z n there existed b such that a b is congruent to 1 mod n. So, this is multiplicative operation. So, inverse means if we multiply with that inverse element with that original element we should give the identity element and 1 is the identity element under multiplication under the multiplication so; that means, under our multiplication operation it should give us 1 basically. So, this is the modular operation. So, then we say b is the inverse of a and we and will see if a is co prime with n then only inverse exists this theorem will prove in a theorem if and vice versa if there exist inverse then this will be co prime if this; that means, gcd of a comma n is one then only inverse exist then we have a b then only b exist otherwise not exist.

For the existence of the inverse, we need to have this condition, this is the condition; that means, a must be co prime with n. So, if you look at this table here in the slide, if you look at the table in the slide. So, n is here 8 now if you take any element a which is co prime with n like 3 is co prime with n. So, if you look at 3 then 3 has inverse again what the element co prime against 5? 5 is co prime with 8, so 5 has a inverse 7, 7 is co prime with 8, 7 as the inverse, but any other element like 4, 4 is not co prime with 8 because gcd of 4 and 8 is not one they have a factor other than one. So, this is not basically having no inverse. So, for the existence of inverse we need to have, n must be gcd of a

and n must be 1. So, this will prove in a theorem which is basically. So, let us have the theorem.

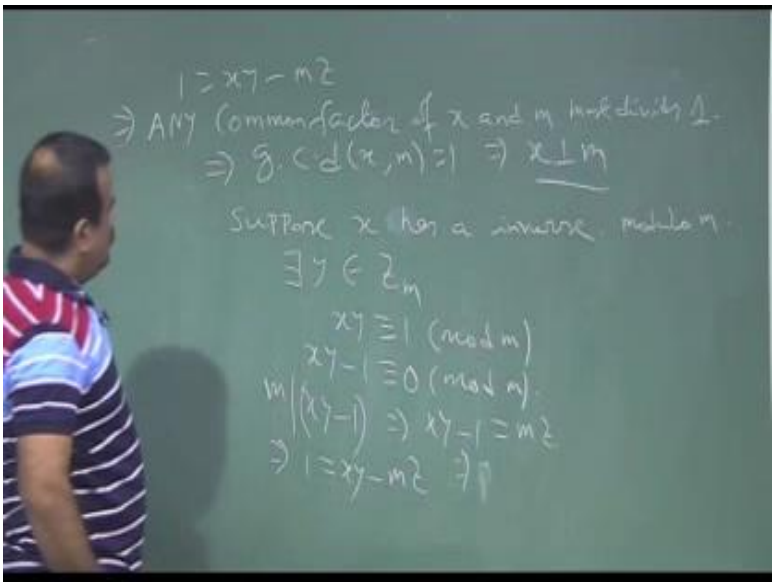
(Refer Slide Time: 21:19)



This theorem is telling the integer x has an inverse modulo m and m is 8 x say a if and only if they are relatively prime gcd of x comma m is one so; that means, they are relatively prime or they are co prime.

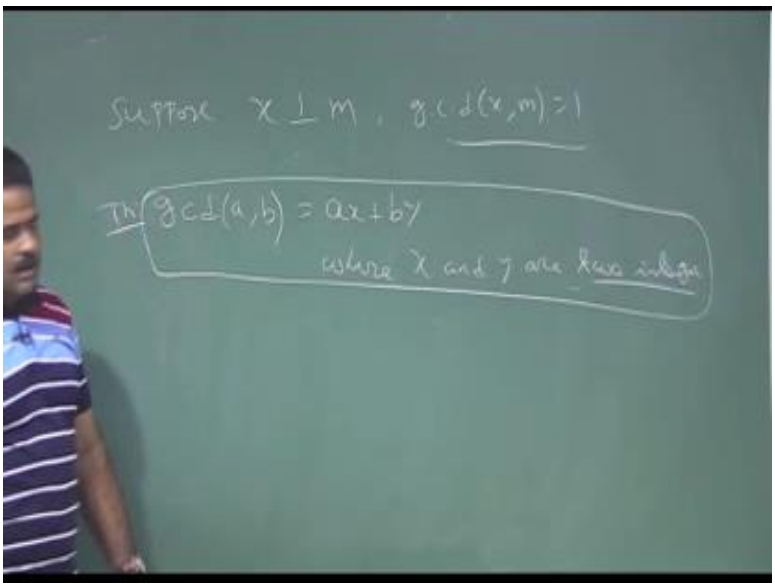
How to prove this? Suppose x has a inverse. So, this has 2 parts if part and if and only if part. So, suppose it has a inverse suppose x has a inverse. So, x has a inverse means there exists a y x has a inverse modulo under this modulo m multiplicative sense so; that means, there exists a y belongs to Z m such that x y is congruent to 1 mod m. We have to prove that gcd of x and m are 1 so; that means, x and m are relatively prime. So, from here we can write x y minus this is 0 mod m. So, from here we can write m divides x minus x y minus 1 so; that means, x y minus 1 should be written as sum m into Z.

(Refer Slide Time: 23:58)



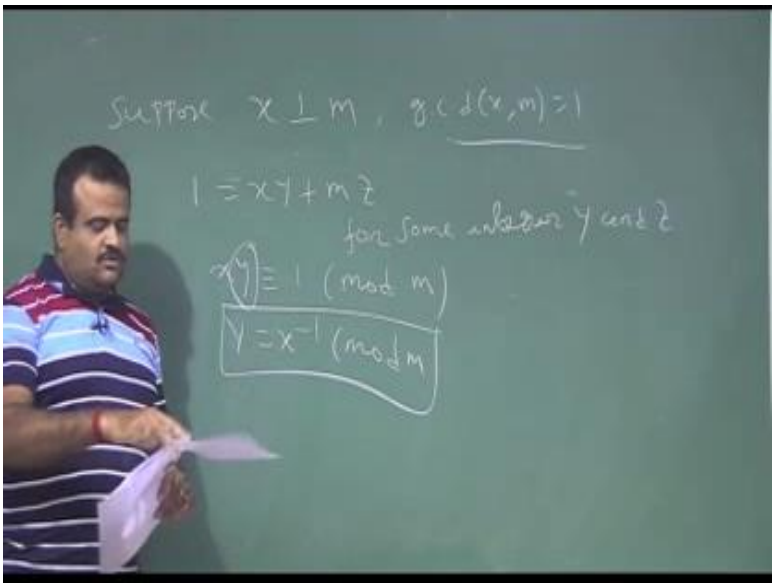
These implies 1 is equal to x y minus m Z so; that means, any common factor of x and y must divides one. So, this implies, it is this implies, so we got this one is equal to x y minus m z. So, this implies any common factor any common factor of x and m must divides 1. So, this imply gcd of x and m must be 1 so; that means, x is co prime with m this is the one part of the proof. So, if x has a inverse then it is it must be co prime. Now the other part if x is co prime with m then it has a inverse. So, that part you have to prove now. This is the other way round.

(Refer Slide Time: 25:02)



So, suppose x is co prime with m so that is gcd of x comma m is 1, now we have to show that x has a inverse multiplicative inverse mod m. So, how to show this? So, if the gcd of one this you have to. So, this we will use the theorem which will prove in the next class like gcd of any 2 integer a b can be written as a x plus b y where x and y are 2 integer. So, this will prove actually this will this is basically gives us the extended Euclidean algorithm to find the inverse, but this we have to prove it. So, gcd of any 2 integer a b should be written as a x plus b y form is linear form. So, this we have to proved. So, for the timing we are taking this as a theorem, this theorem this will prove in the next class. So, suppose we take this theorem then. So, gcd of this is one means. So, there must exist a x y such that x is already there. So, there must exist a. So, gcd of this is 1. 1 is equal to some x y plus m Z. So, these for some integer y and Z from that theorem gcd of a b should be written as x plus b y form.

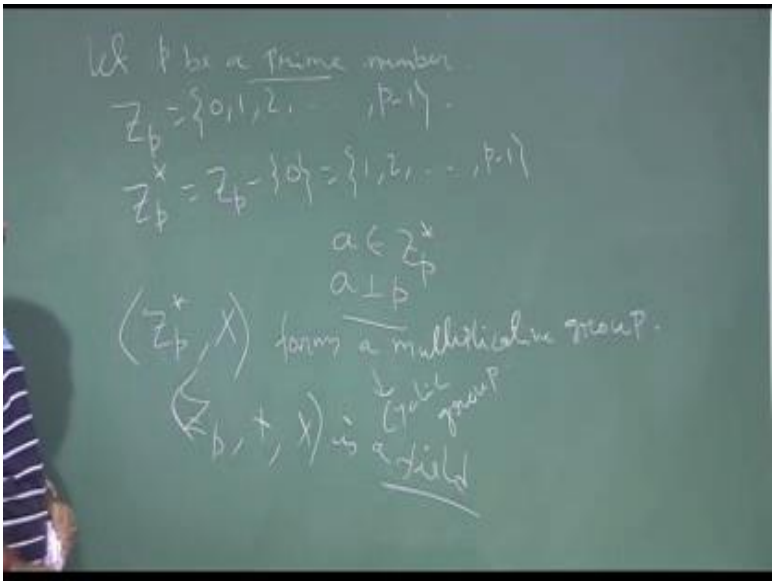
(Refer Slide Time: 26:40)



From here what we can say x y is equal to basically x y is basically congruent to 1 mod m because if we divide this by mod m. So, this is having m. So, this part is gone. So, x y is basically congruent to 1 mod m say that y is basically inverse of x and this y will find by the by algorithm which is called extended Euclidean algorithm. So, basically you will try to get this sum form. So, then this y is basically x inverse y is basically multiplicative inverse of x. So, the inverse exists if the relatively prime.

It is not that inverse is always exist, inverse exists if a x is relatively prime with n. So, now, let us talk about what is called; now will see whether it is from a group.

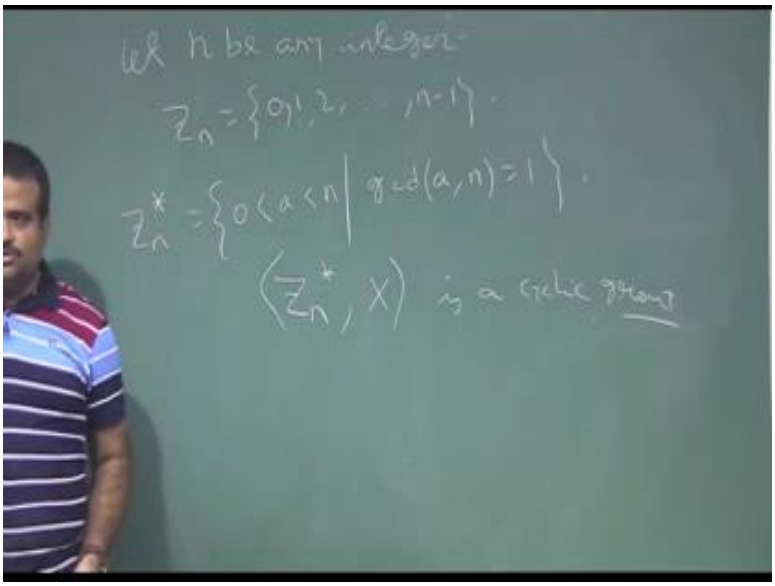
(Refer Slide Time: 28:15)



Let n be an integer. So, now, if n is p n is a prime suppose n be a prime numbers let in that the p be a prime number prime integer then we know Z p is basically 0, 1, 2, 3, up to p minus 1, now if we omit 0, this is basically Z p minus 0 . So, now, if p is a prime then each of this element is since p is the prime then if we take a element from Z p star then a must be relatively prime with p because p is a prime number. So, p is not having factor other than 1 and p; that means, if you take any element from here they are relatively prime with p; that means, each element here will have a inverse multiplicative inverse.

This means Z p star this will form a on a multiplicative group and basically this is cyclic group this is a cyclic group. So, we are just removing the identity additive identity element so; that means, this Z p plus dot is a field and this is a finite field because number of element is basically this finite set. So, this is a finite field because this is we know this with addition there is no issue because every element has inverse with multiplication. So, other than 0 other than 0 element every element has a inverse provided p is prime.

(Refer Slide Time: 30:51)



This is the field, this is finite field because numbers of elements are finite; now what will be the case if p is not a prime. So, suppose general case let n be a any integer need not be a prime then we define Z n then we in our table we have taking n is equal to here in the slide we have taking n is equal to 8.

So, then we have seen all the elements are not having the multiplicative inverse only those elements were relatively prime to n. So, that element said we define Z n star, Z n star is basically set of all element less than n such that gcd of a comma n are 1 then for n is equal to 8 we have seen the 4 3 5 7 are the belongs to Z n star. So, this Z n star will form a group under multiplication is a cyclic group. So, this is how we define Z n star, Z n star is basically set of all integer less than n nonzero integer positive, positive nonzero integer less than n which are relatively prime with n. So, in that case, if we define like this for each of such a inverse will exist. So, it will form a multiplicative group and this is a cyclic group.

Thank you.