A Basic Course in Number Theory

Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay

Lecture 32

The Legendre Symbol

Welcome back, we are now going towards finding squares in u N and as our experience tells us until now, that things are very nice when we are looking at n to be a prime number. And remember also that we are looking at odd N. So, we should be looking at odd primes. So, we begin with trying to compute the squares in u p or what we would like to do is to find how many elements are squares in u p or what are the elements which are squares in u p. So, this was studied quite some time back, 2 centuries back by the mathematician Legendre, who has done lot of other work including work in differential equations, and there is a one particular quantity that Legendre defined that is called the Legendre symbol.

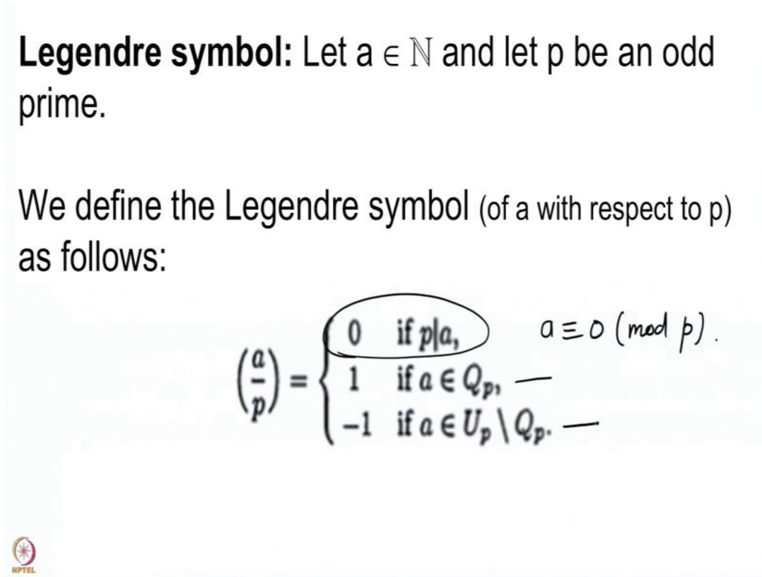
(Refer Slide Time: 01:30)

Legendre symbol: Let $a \in \mathbb{N}$ and let p be an odd prime.

We define the Legendre symbol (of a with respect to p) as follows:

So, we will see the definition of this Legendre symbol, what we have is that we take n, we take an element a in the natural numbers and let p be any odd prime. So, here our N is the set of natural numbers and we are starting with any odd prime p, then we define the Legendre symbol of a with respect to p and this is. So, given any order prime, we are going to define the Legendre symbol for any natural number a and the formula is a complicated formula, let us look at the formula once and we will then try to understand the formula in some detail.

(Refer Slide Time: 02:12)

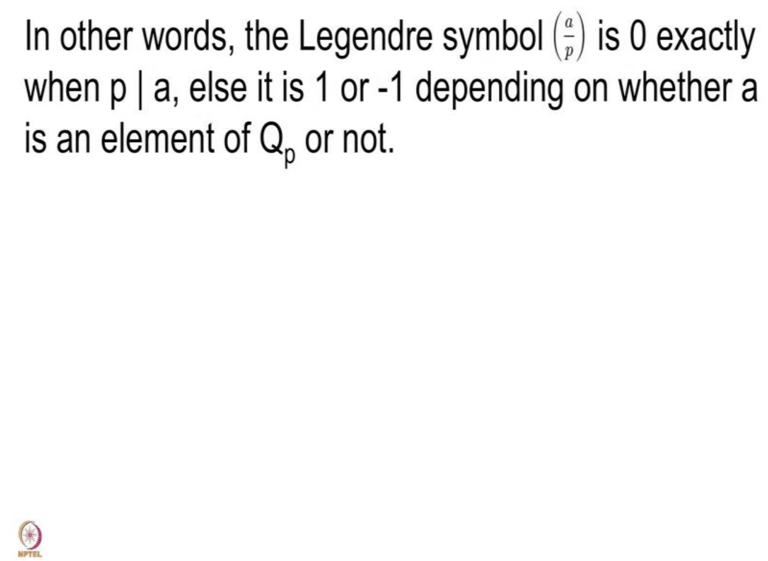


So, the formula is as given here, it says that the quantity is 0 the Legendre symbol is 0 f p divides a. So, for all the natural numbers a which are divisible by p the Legendre symbol is 0 and for the non0 elements, the elements which are so, this is of course, to say that when a is congruent to 0 mod p, that is a that is what we are going to have here. So, whenever you have a not to be congruent to 0 mod p, the Legendre symbol can be one or minus one depending on whether a is a square modulo p or whether a is not a square modulo p.

So, this Legendre symbol has 3 values, it will be 0 for all the natural numbers which are divisible by p. So, 0 and if you are looking at natural numbers we will start with p. So, p 2 p 3 p 4 P and so on for all these numbers, the Legendre symbol is 0. Then for the squares modulo p Legendre symbol is one. So, this is a computation that we will have to do separately for each prime very carefully.

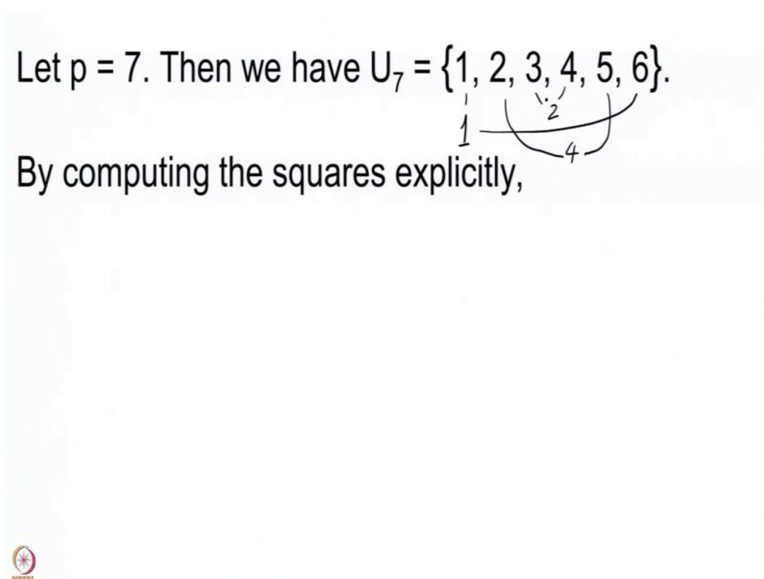
We already observed that in the case where p was 7, we had 3 squares, one, 2 and 4, these were the 3 squares. So, when you are going modulo 7, the Legendre symbol will be one for these 3 elements, for the remaining 3 elements in new 7 the Legendre symbol will be minus one and whenever 7 divides, some particular a the Legendre symbol will be 0, okay. This is the understanding of Legendre symbols.

(Refer Slide Time: 04:26)



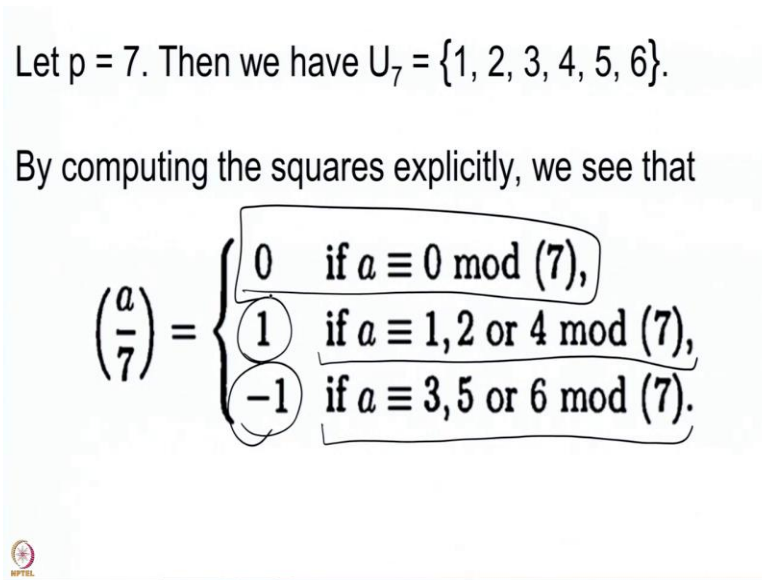
So, in other words, what we have is that this symbol a by p this is our definition of Legendre symbol we will call it a by p, this is the symbol we are looking at. So, this is 0 exactly when p divides a just as the last slide also told us else it is one or minus one, depending on whether a is an element of Qp or not whenever a is a square modulo p, Legendre symbol is 1, whenever a is not a square modulo p, the Legendre symbol is minus 1. So, let us do some computation of Legendre symbols, let B be 7. And suppose now we want to do the computation of Legendre symbols.

(Refer Slide Time: 05:12)



So, we want to compute a by 7, that is what we want to compute. So, we have that U 7 is one 2 3 4 5 6, the invertible elements modulo 7, are exactly one 2 3 4 5 6. So, among these, we have computed the squares explicitly. And let us just do it once again. So, 1 will give you one as the square and 6 also gives you 1, 2 will give you the square 4, and minus 2, which is 5, that will also give you the square to be 4 because 5 squared is 25, which is 4 modulo 7, and 3, as well as 4 will give you the square to be 2. So, we have exactly 3 squares in U 7 or there are exactly 3 elements in Q 7. And when you write them, by order, you will write them as one comma 2 comma 4.

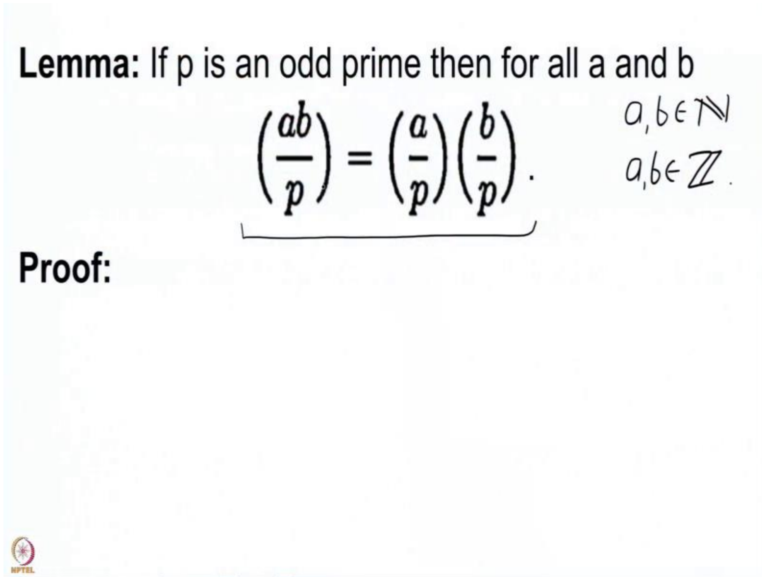
(Refer Slide Time: 06:19)



And so, this is exactly what we have. So, whenever these element is one 2 or 4 modulo 7, then you have that the computation of Legendre symbol modulo 7 is one, the remaining 3 elements, which are 3 5 6 mod 7, there the Legendre symbol value is minus 1 and of course, whenever a is divisible by 7, we have that the Legendre symbol is 0.

Now, this computing the squares explicitly is not going to work all the time, there are some very high numbers, very large numbers, which are primes and we would like to find a way to do these computations effectively. So, there are some laws that we will require to do these competitions. So, we will prove these laws in due course. Right now, what we will do is to try to get some hang of how these Legendre symbols behave.

(Refer Slide Time: 07:34)



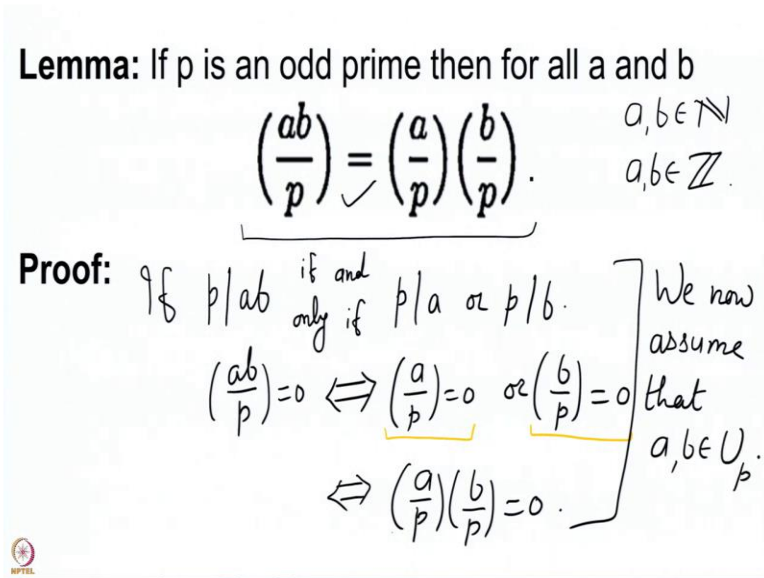
So, this is the first lemma that we have in that direction, that we will start with an odd prime p, then for every a and b in the set of natural numbers. So, you are taking a and b coming from N then we always have that the Legendre symbol of a b with respect to p is the product of the Legendre symbols of a and b with respect to p.

So, when you want to compute, suppose you wanted to compute the Legendre symbol modulo 23, 23 is a prime prime, if you wanted to compute the Legendre symbol of say 15 modular 23 it would be difficult to see whether 15 is a square or not, but if you know whether 3 is a square or not, and 5 is a square or not, you will have the information about 15 being a square or not.

So, whenever you know the value of the Legendre symbol 3 by 23 and 5 by 23, that will allow you to compute the Legendre symbol for 15 by 23. So, this way, we can compute from the small elements we by taking products, we will be able to compute the Legendre symbols for all elements modulo p. And of course, we know that you will then have to compute it only for primes. And you can actually start with these a comma b to be elements in integers, not necessarily only in natural numbers.

So, you will look at negative numbers, you will look at positive numbers. And among the negative numbers, if you know how to compute the Legendre symbol of minus 1, then you can just do the calculation for positive numbers. And with minus one you have the calculation for all integers and among positive numbers also, once you know how to compute Legendre symbol for each prime with respect to a given prime p, then you have lot of freedom then you have lot of tools at your hand to compute these Legendre symbols.

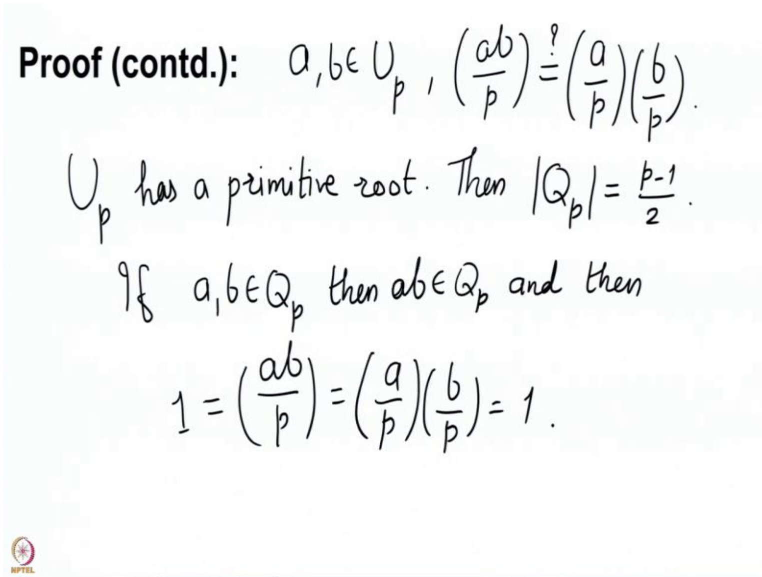
(Refer Slide Time: 09:48)



So, let us prove this statement right now. We want to prove that this a b by p is a by p, b by p. So, first possibility is that if p divides a b then p divides a or p divides b this is one statement that we know quite well by now. And this is in fact also true if and only if. So, you will in fact have that this happens if and only if you have that p divides a or p divides b. So, we will get that a b by p is 0 if and only if a by p is 0 or b by p is 0. So, here on the right-hand side of the if and only if symbol I have 2 numbers.

And I am saying that this number is 0 or that number is 0. And when you have 2 numbers and you have the possibility that one of them can be 0, this is the return in terms of having the product being 0. So, we have the equality a b by p equal to a by p, b by p, whenever we have the equality to be 0. So, now, we will assume that we do not have any of these 3 values a b by p, a by p and b by p, we assume that none of these are 0. So, what we will have is that a is in Up, b is in Up and therefore a b is also in Up and then we will compute these Legendre symbols and see whether we get the equality, okay. So, we are we can therefore, assume now, so, we now assume that a comma b is an element in Up this is our standing assumption now.

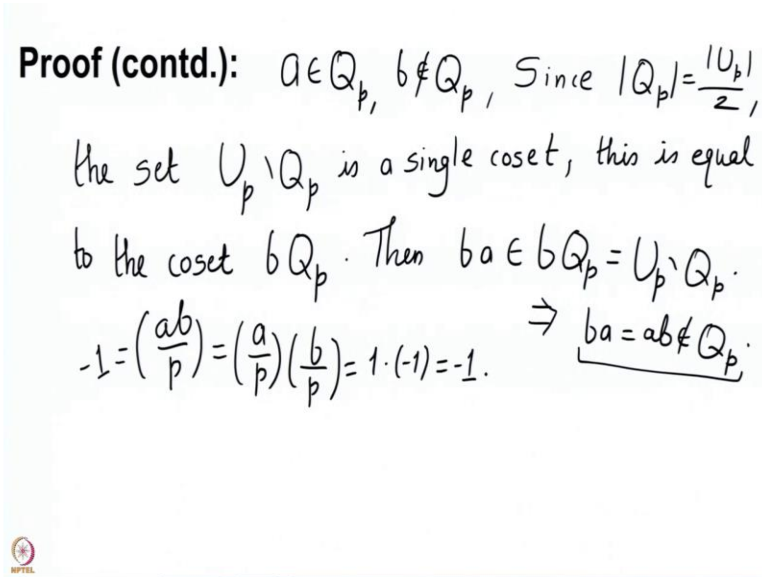
(Refer Slide Time: 12:18)



So, a comma b are in Up and we want to check whether a b by p is same as a by p, b by p. Now, we observe that Up has a primitive root. We have proved in fact, that when p is an odd prime Up power a has a primitive root. So, in particular Up has a primitive root. And then, we also saw that the number of squares will have cardinality exactly p minus one by 2. The subgroup consisting of all squares has cardinality p minus 1 by 2 exactly half the elements are squares. So, clearly if a b belong to Qp then a the product a b is also in Qp because it is a subgroup. Remember, I had said that this fact is going to play an important role. So, if a comma b both are in a Qp, then the product a b is in Qp and then we get the equality quite easily. Because all these legendary symbols are one.

Now, we have to deal with the case where one of the 2 is in Qp and the other is not in Qp. And then finally, we will have to deal with the case where none of those 2 is in Qp. So, those are the only 2 conditions that we need to verify our proof in.

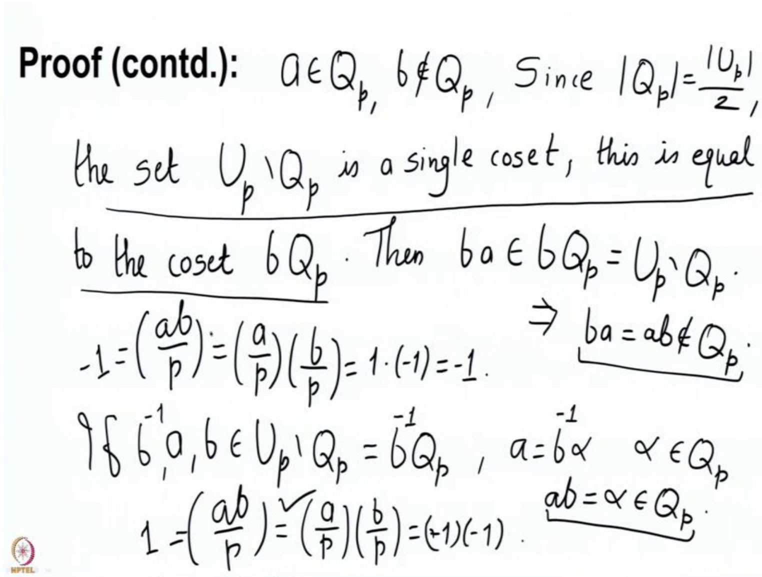
(Refer Slide Time: 14:36)



So, we start with a in Qp and b not in Qp, but observe that the cardinality of Qp is exactly 1 by 2 of the cardinality of Up. So, Qp which is the subgroup of Up has exactly half the elements and the remaining set of elements is therefore going to be a single co set. We have observed that whenever you have a normal subgroup here, the groups are a availian. So, we have the subgroup Qp inside Up and then you have take you will take the cosets of Qp in Up you will take the cosets of Qn in Un in general, then each coset will have cardinality equal to the cardinality of Qn, but since Qp has cardinality exactly half of that of Up the elements which are outside Up will form a single coset.

So, since cardinality of Qp is cardinality of Up upon 2 these set Up minus Qp is a single coset and since b is not in Qp this is equal to the coset b Qp. Now, we have that a is in Qp and then b a also belongs to the coset b Qp which is actually equal to Up minus Qp. So, here we get that when you have a in Qp b is not in Qp it will tell you that b a or a b is not in Qp. So, the competition's will tell you that a b by p which is now minus one because a b is not in Qp is also equal to a by p b by p which is one into 2 minus one which is minus 1. So, the case a being in Qp and b not in Qp is now done because then a b is also not in Qp And now, we have to deal with the final case, where we will take both a and b not in Qp.

(Refer Slide Time: 17:36)



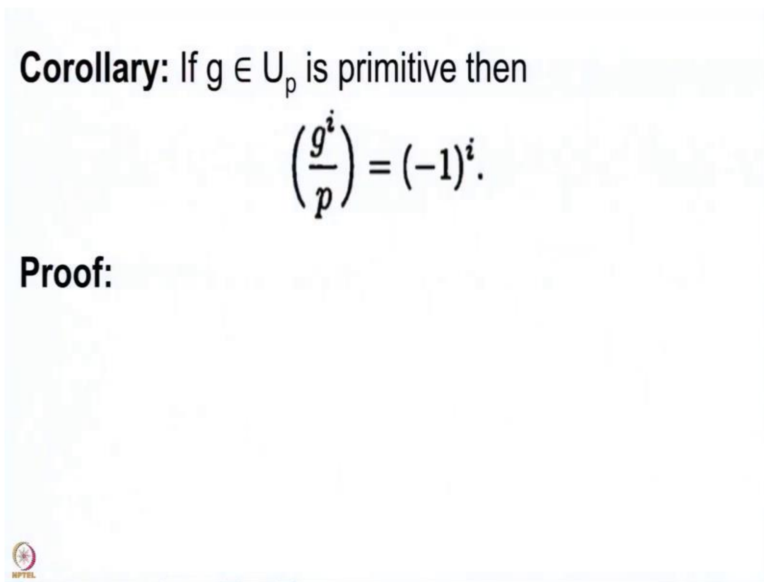
If a is not in Qp and b is not in Qp then by our earlier as an observation, we have that Up minus Qp is a single coset. So, we have that b is in b Qp and a is also in b Qp. So, that will tell you that a is equal to b times some element alpha where alpha belongs to Qp and similarly, whenever b is not in Qp you will have that b inverse is also not in Qp and so, b inverse will also give you the same coset and therefore, a is b inverse alpha Qp being the subgroup if b inverse was in Qp then b would also have to be in Qp.

So, we get a equal to b inverse alpha which says that a b is alpha which is in Qp. And therefore, we get that the product a b by p which is now one because a b is in Qp, a is equal to the product of 2 minus ones. So, we get equality in all the cases once again what we have observed is only the following thing when you have p dividing a b that is true if and only if p divides a or p divides b. So, a b by p can be 0 precisely when one of the a by p and b by p is 0 okay. So, if a by p and p by 2 are both non 0, then a b by p cannot be 0.

So, whenever p divides a or p divides b, then we have the equality for a b by p equal to a by p into b by p and therefore, we are now going into the case where a comma b are in Up these are invertible modulo p when these are invertible modulo p, the possibilities are that a and b will belong to Q p or not. But there is a you know there would be 4 cases a and b in Qp, a in QP, b not in Qp, a not in Qp but b in Qp. Actually, this is the same as the second case, because then you can just replace a by b and b by a.

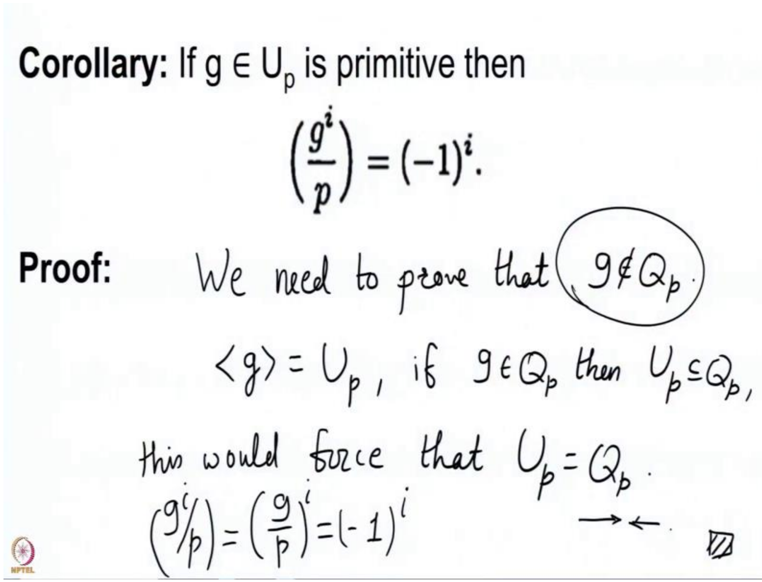
And the third case now, for us is when none of the a b is in Qp, and what we observe is that a comma b belong to Qp implies a b belongs to Qp. So, we have the equation that the equation holds if a is in Qp and is not in Qp, then we prove that a b is not in Q p. So, indeed you get one into minus 1 to be minus 1 and finally, we see that whenever a is not in Qp, b is not in Qp a b has to be in Qp. So, you get minus 1 into minus one equal to 1. So, the equality of the a b by p the Legendre symbol of the product is the product of the Legendre symbols that equality holds in all cases and that completes our result for us. However, our Up is also have primitive roots.

(Refer Slide Time: 21:14)



So, with respect to the primitive roots, we can actually have this result quite nicely that whenever g is a primitive root in Up, then the Legendre symbol of g power i is simply minus 1 to the power i and the only thing that we have to prove here is that the Legendre symbol of g is minus 1 that g cannot be inside Qp once we prove this, then the Legendre symbol of g has to be minus 1 and this result will follow by whatever we have proved earlier. So, that is the only thing we have to see.

(Refer Slide Time: 21:50)

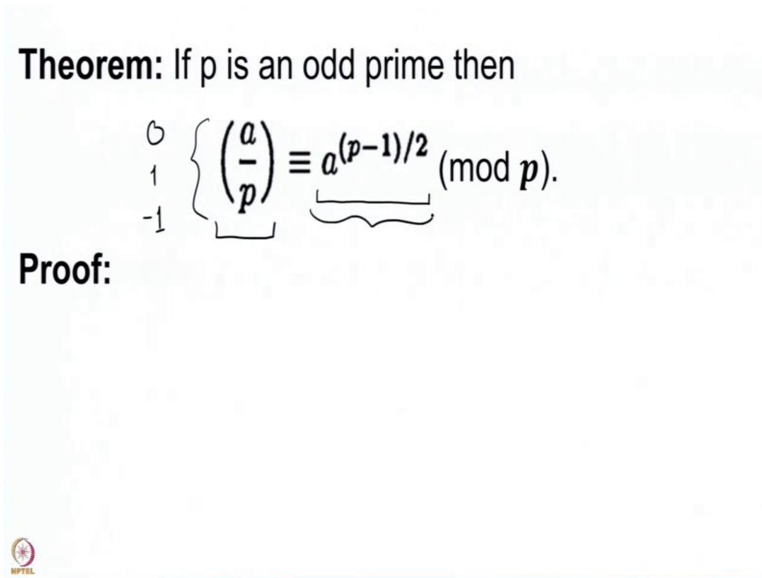


So, we need to prove that g is not in Qp but this is quite clear, because the group generated by g is the group Up. If your g was sitting in Qp then the whole Up will be sitting in Qp but Qp is also a subset of Up, so, this would force that Up equal to Qp but this is a contradiction by the computation of the order of Qp that we have seen earlier, we have seen that whenever we have a primitive element, there are exactly 2 square roots of one namely 1 and minus 1 we are taking p to be an odd prime. So, 1 and minus 1 are distinct elements modulo p.

So, one and minus one are 2 square roots of one therefore, the map with sense I have every element to its square the homomorphism that we saw in the last lecture that has a non trivial kernel of cardinality 2. And therefore, by looking at the cardinalities we get a contradiction. So, we have that g is not in Qp and therefore, the Legendre symbol of g by p is minus one and then it will follow quite easily that the Legendre symbol of g power i with respect to p is the Legendre symbol of g with respect to p to the power i, because we have seen that it is a homomorphism Legendre symbol is multiplicative. And so, we get this to be minus one to the power i.

So, very simple fact will tell you that you can compute the Legendre symbol of every element once you know the Legendre symbol of the primitive element. Or in other words, once you know a primitive element, once you know a primitive element, you can write every element as power of this primitive element. And then you will be able to compute the Legendre symbols for every element quite easily using these 2 things. This is also another simple result, but it is a big theorem, because it will help us computing lots and lots of Legendre symbols.

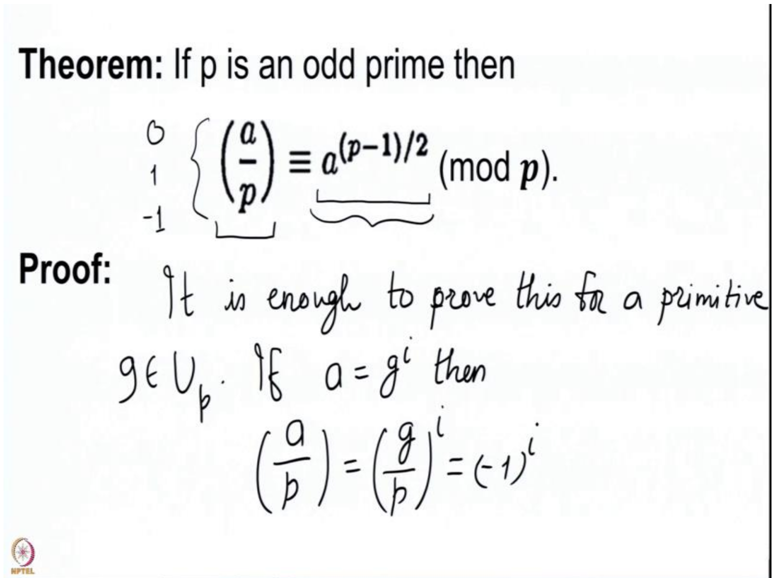
(Refer Slide Time: 24:39)



The basic thing that is different here is that on the left hand side we have the Legendre symbol which can be 1 or minus 1 or 0. But on the right hand side we have something which is purely in terms of a. So, when you are feeding this as an algorithm to computer it would be very easy for a computer to tell that given an a compute the a power p minus one by 2.

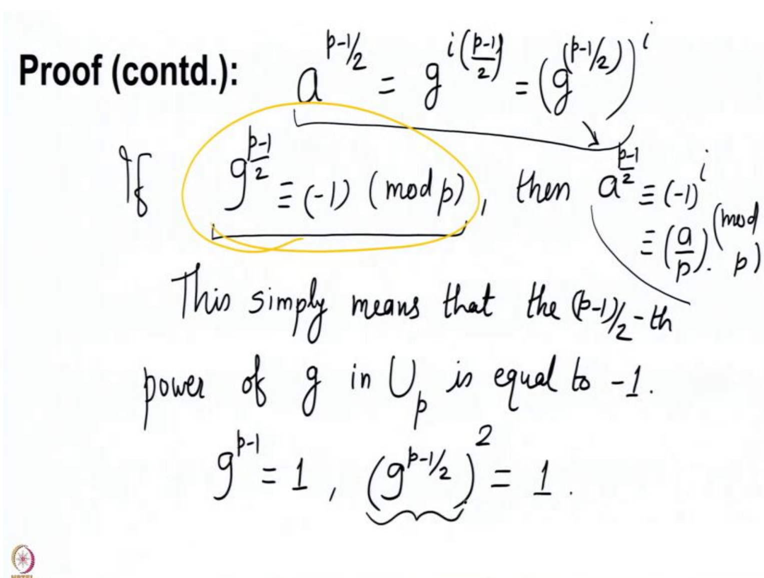
Whereas, if you were to tell the computer to check whether a is a square or not or whether p divides a or not and so on, then that would be more difficult things to prove or to implement on a computer program whereas, this is something which is quite feasible, this is something which is quite doable. So, this is one of the very important theorems, let us see a proof of this very quickly. And once we have a proof of this, then we can also do some computations and try to compute Legendre symbols for various other elements.

(Refer Slide Time: 25:48)



So, the basic step here is that it is enough to prove this for a primitive g in Up this is because, so, I will give a reason to tell why this is enough. So, if a is g power i then we know that the Legendre symbol a by P is the ith power of the Legendre symbol g by p and this is also minus one to the power i and further we have that a is g Power i.

(Refer Slide Time: 27:00)

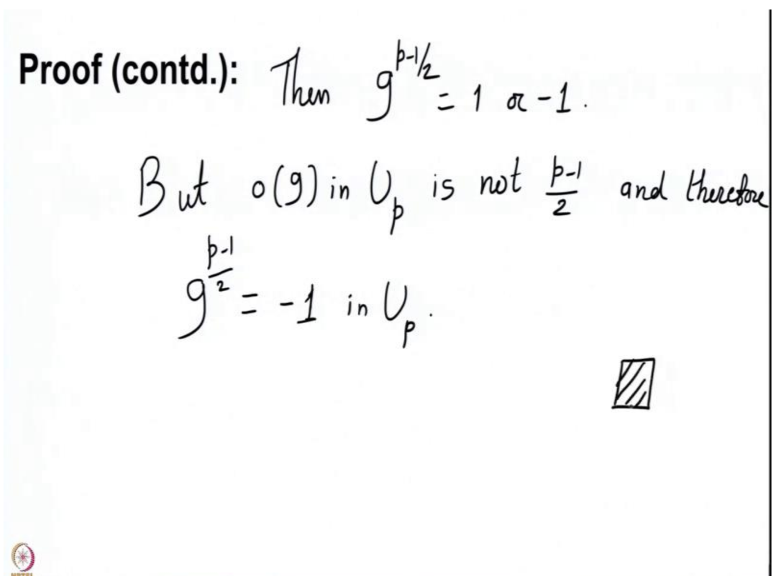


So, a to the power p minus one by 2 is g to the power i into p minus 1 by 2 and this is nothing but g power p minus 1 by 2 the whole thing to the power i. So, if we prove the result for the primitive element, which would tell you that g power p minus 1 by 2 is congruent to minus 1 modulo p then here we would put the value and get that a to the p minus 1 by 2 is congruent to minus 1 to the power i and from the previous step this is nothing but the Legendre symbol a by p.

These are both mod p so, when we have a by p to be equal to minus 1 to the power I and once you prove that g power p minus one by 2, once you prove this equality, then using this formula, we will get directly that modulo p a raise to p minus 1 by 2 is simply the Legendre symbol a by p. So, what we need to show is that g to the power p minus 1 by 2 is not equal to 1 in the group Up. So, this simply means that the p minus one by 2 th power of g inside Up is equal to minus one this is what we want to show when we want to show that modulo p g to the p minus 1 by 2 is minus 1.

So, we are going to take these powers of g in Up and we want to show that when you raise it to this particular power you made it to the minus one. So, first of all we note that g to the p minus one has to be one because the order of g, g being primitive the order of g is the primitive, is the cardinality of Up which is p minus one. So, g to the p minus 1 is 1, which says that if you were to take this power g to the p minus one by 2 and take the square then you get one.

(Refer Slide Time: 30:25)



So, this element here is a square root of one. So, the possibilities are that we get the element g to the p minus 1 by 2 equal to 1 or minus 1. But, the order of g in Up is p minus 1. So, it is not this number which is smaller than p minus 1 and therefore, the power p minus 1 by 2 of g has to be minus one in Up. So, this completes the proof.

So, what we have proved once again I should recall this for you that the Legendre symbol can be computed very easily simply by taking the p minus 1 by a 2 th power of your natural number a and going modulo the prime p. So, we will see some more such things which will help us computing the Legendre symbols in the coming lectures. See you until then thank you.