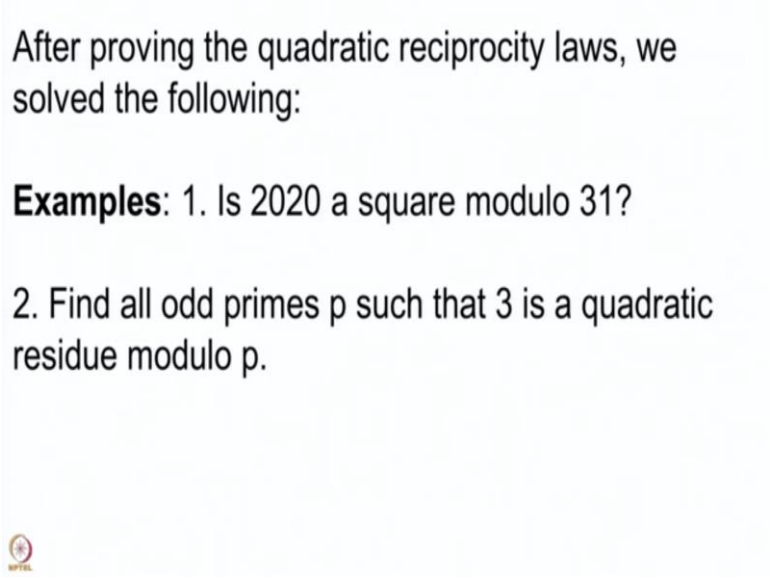
A Basic Course in Number Theory
Professor. Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 37
The Jacobi Symbol

Welcome back. We proved the quadratic reciprocity law the, all the three parts of the law and then we solved some examples. We saw some applications of the quadratic reciprocity law, so here they are.

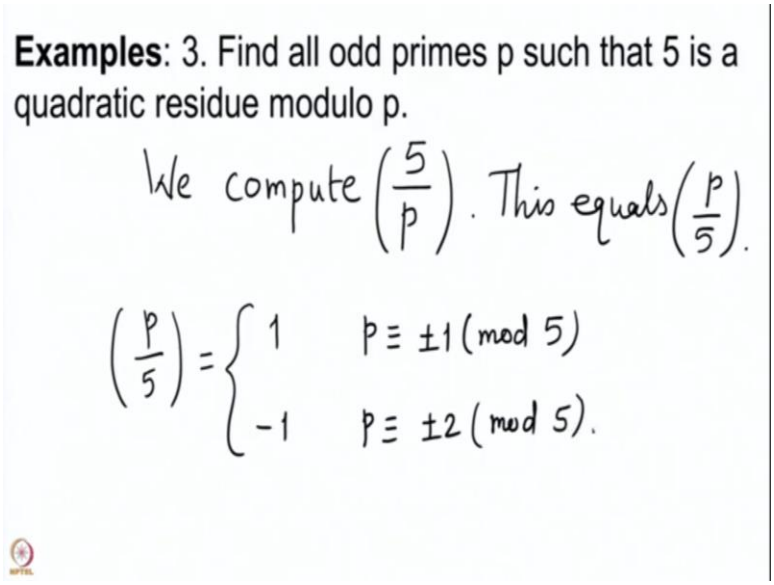
(Refer Slide Time: 00:33)



So, we computed whether 2020, the current year, is a square modulo, a prime, so for example 31. And then we also saw that we could find all odd primes p such that 3 is a quadratic residue modulo p. That means, the, the legendre symbol 3 by p is 1. We found all such primes p, this was given by some certain congruence relation so there were some arithmetic progressions and all the primes appearing in those arithmetic progressions gave us that 3 is the square modulo p.

And there were some arithmetic progressions such that, we had that the primes appearing in those arithmetic progressions had the property that 3 is not a square modulo p. So, we will now do a similar example for 5. We want to compute all odd primes p, such that 5 is a square modulo p.

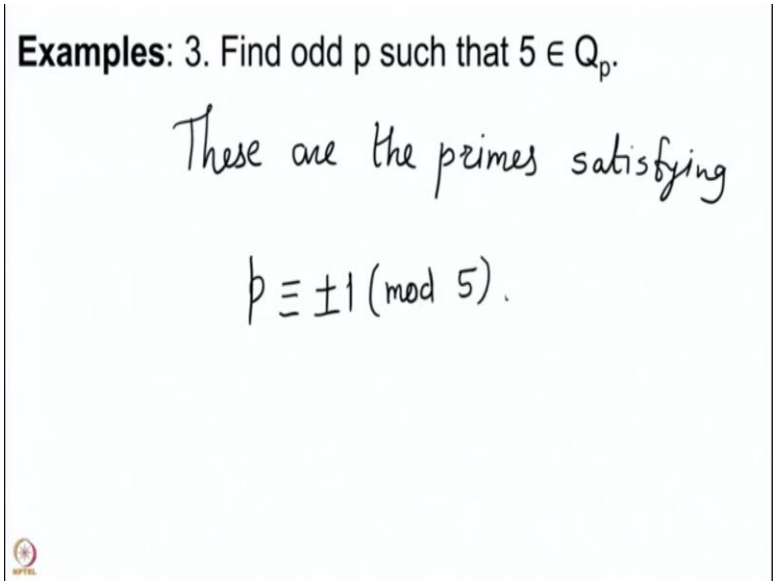
(Refer Slide Time: 01:40)



This is the problem that we now want to think about that find all odd primes, here we are looking at odd primes because we know that if p is 2, then every odd number is congruent to 1 modulo 2, and then of course every odd number is going to be a square modulo 2. So, we have to look at only odd primes to make the actual computation. So, we are interested in, we compute this legendre symbol 5 by p but 5 is congruent to 1 modulo 4.

So, the third law of quadratic reciprocity will tell you that you can switch the places of p and 5 without changing the sign. So, this is equal to p by 5, this legendre symbol. But this is very easy to compute because now we have to go modulo 5 and there are 4 numbers 1, 2, 3, 4 and we need to see which of them are squares modulo 5. So, this is 1 or minus 1 depending on whether p is congruent to plus or minus 1 modulo 5 and the second case is where p is congruent to 2 or minus 2 modulo 5.

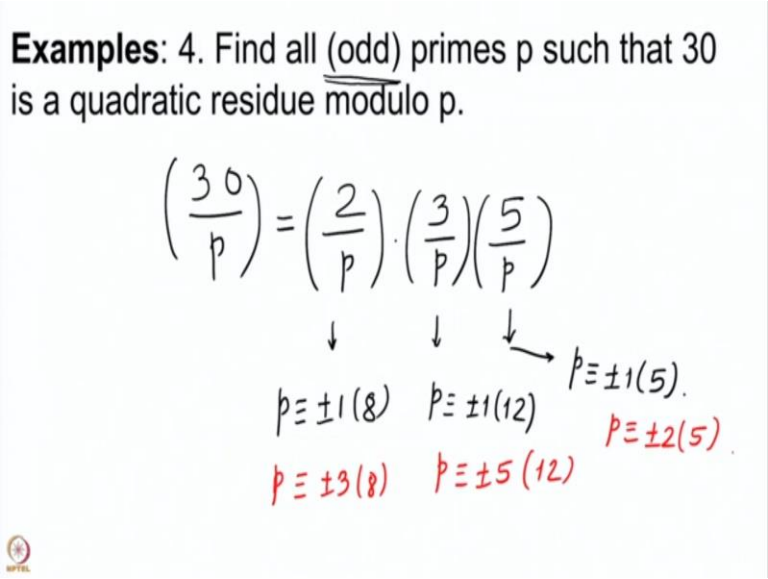
(Refer Slide Time: 03:20)



So, this actually turned out to be a simpler problem because we are now able to answer this question. So, these are the primes satisfying p congruent to plus or minus 1 mod 5. So for instance, 31 is a prime such that p by 31 the legendre symbol 5 by 31 is 1. 5 is a square modulo 31, indeed 6 square is 36 which is 5 modulo 31. Whereas 37 is the prime which is congruent to 2 mod 5 and therefore 37 will not have the property that 5 is a square modulo 37. This is same as saying that 37 is not a square modulo 5 and then we know how to compute the answer.

So, we can find all odd primes p with the property that 5 is a square modulo p. So, we have computed the odd primes p where 3 is the square, we have computed the odd primes p such that 5 is a square. Using these things, we can compute all primes p with the property that 30 is a square.

(Refer Slide Time: 04:57)



So, this is our next problem. Find all primes p with the property that 30 is a quadratic residue modulo p. Here, I am keeping odd in the bracket because the prime p where 30 is a square modulo p, we should have that p comma 30, the GCD is 1 and therefore clearly p equal to 2 will not come. So, it is not necessary now to say that we are only looking at odd primes, we are looking at times where 30 is the square mod p and then of course such primes will be odd.

So, we are interested in computing this legendre symbol but legendre symbol is multiplicative. So, we have that this is 2 by p into 15 by p which gives us 3 by p and 5 by p. Then all these will give rise to some certain conditions, some congruence relations, and we have to put them together to get the correct answer. So, this is equal to 1 when p is congruent to plus or minus 1 modulo 8, this is 1 when p is congruent to plus or minus 1 modulo 12, if you remember from the last lecture and this is something that we have just now computed.

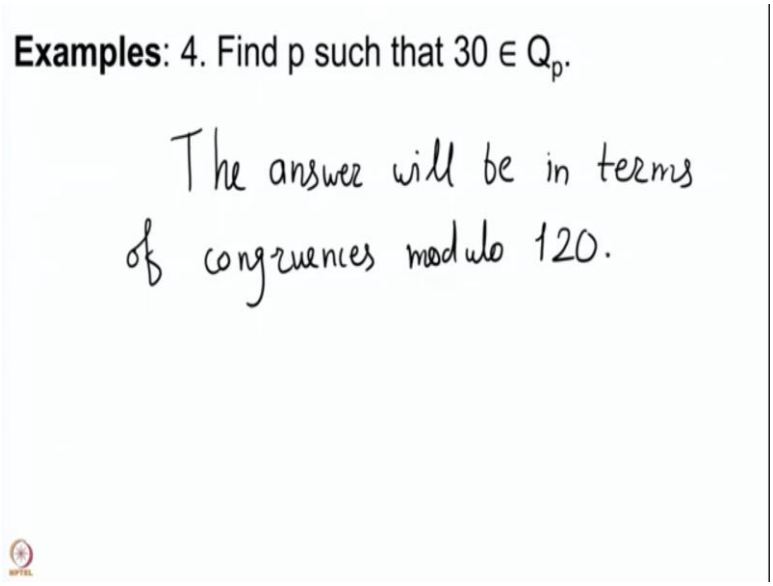
So, these are the computations and of course, there are the remaining computations which will tell you that these signs are minus 1. So, let me put them in a different colour. So, this is when plus or minus 3 modulo 8, this is when plus or minus 5 modulo 12 and this is when plus or minus 2 modulo 5. Now to compute when this legendre symbol is equal to 1, we need to, we will have to compute this product and so this product has to be 1.

So this product of 3 integers will be 1 when 2 of them are equal to 1 and the third one is also 1, 2 of them are minus 1, the third one is 1 and so there are, there is 1 possibility when all are 1 and

there are 3 possibilities depending on the first 2 having negative signs, the last 2 having negative signs and the first and the third having negative signs. So, we will get 4 such cases where the number is going to be 1, the legendre symbol 30 by p is going to be 1 and there will be 4 cases when the legendre symbol is equal to minus 1.

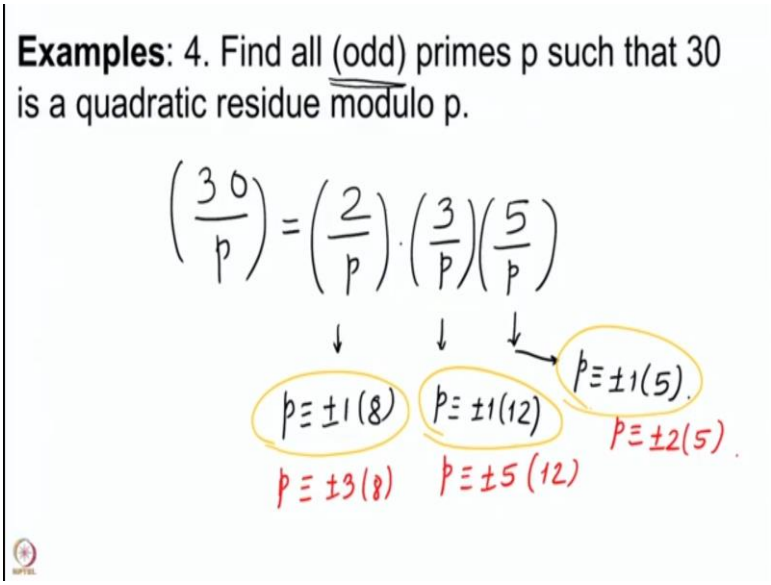
So, these are the cases that we need to compute but these are also the cases modulo, a certain congruence, modulo a certain number and that number is going to be the LCM of the moduli of these congruences. So, we see that for 2 the modulus is 8, for 3 the modulus is 12. So, the LCM of 12 and 8 is 24. So, to combine these 2, we have to go modulo 24 and then the final congruence is modulo 5. So ultimately, we will get a congruence relation modulo 120.

(Refer Slide Time: 08:41)



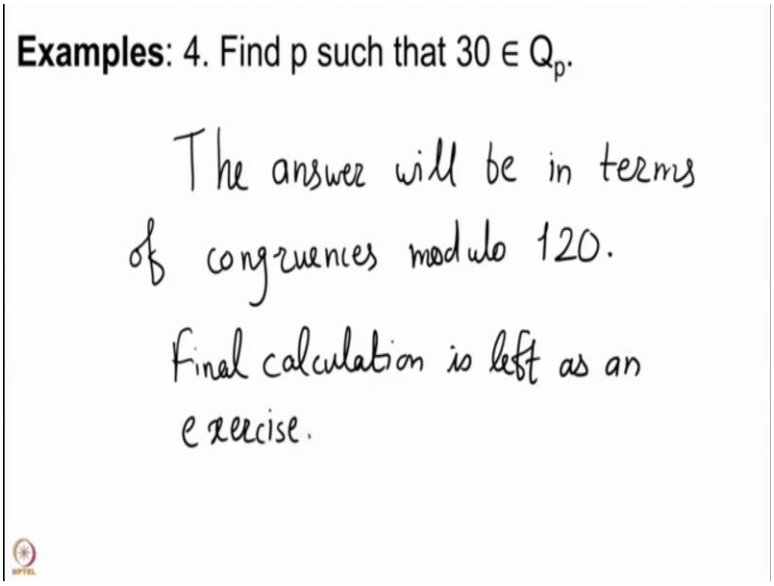
So, the answer will be in terms of congruences modulo 120. I said that there are 4 cases, but actually there are more cases.

(Refer Slide Time: 09:12)



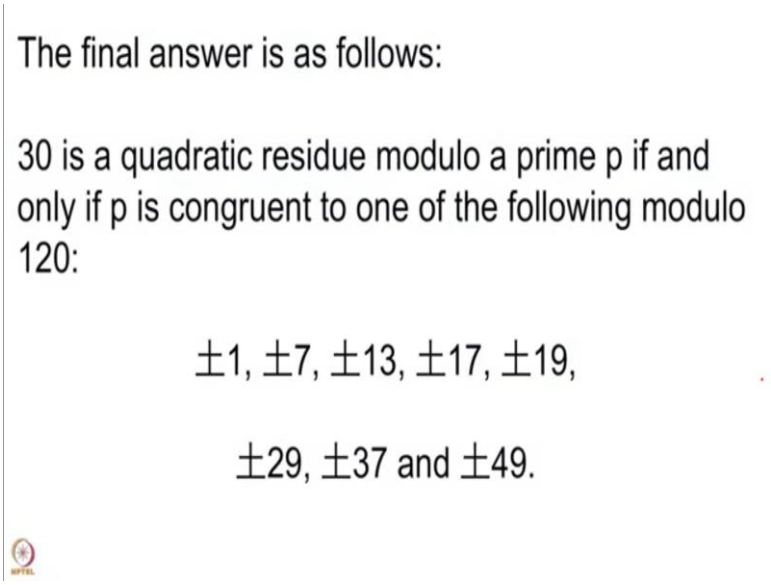
Here when we looked at each of these, I considered each of these to be a single case but each of these are 2 cases each. So, we are going to get more cases and what I am going to do is to leave all these computations to you and this will also be part of our assignments for this week.

(Refer Slide Time: 09:42)



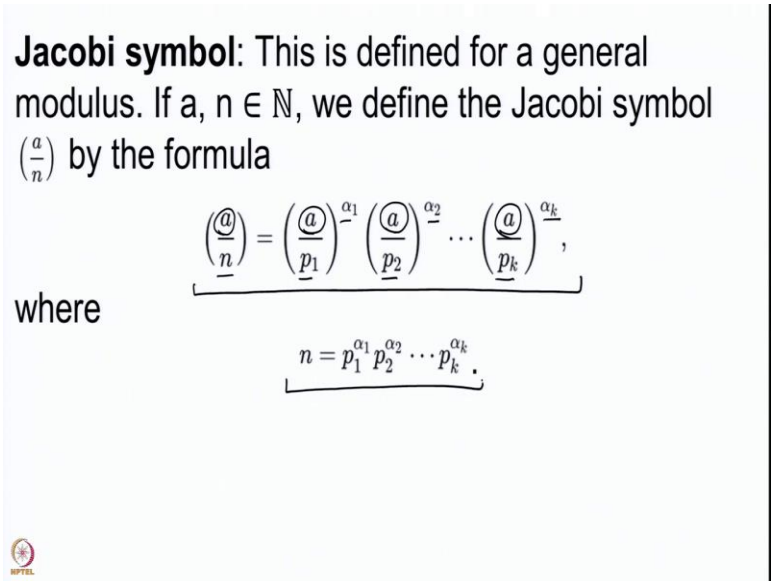
So, this is the final calculation. So, the final calculation is left as an exercise. I have done the most important part in my opinion.

(Refer Slide Time: 10:02)



So, this is how legendre symbol can be very useful and it tells you when a number is a square or not modulo a given prime. Now, there are some generalizations of legendre symbol and the most important generalization is this symbol called the Jacobi symbol.

(Refer Slide Time: 10:37)



So, what does the Jacobi symbol do, how does it differ from the legendre symbol, it differs in the following way. This is defined for a general modulus. The legendre symbol was a by p where that denominator was necessarily a prime. Here, we have that the denominator need not be a prime. It is a natural number. So not negative yet but it is a natural number. So, it is a positive

integer. This is what we have. So, we take a and n to be natural numbers, then we define the Jacobi symbol a by n by this formula that this Jacobi symbol is product of the corresponding legendre symbols.

So, we are looking at a by n. The a is fixed, it is the same a that you have in all these numerators of the legendre symbols. But there is a change instead of n, we have p1, p2, pk and then there are these powers alpha 1 up to alpha k which are given by the prime factors, the decomposition of n into its prime factors. So, when I have a by n, we will take the decomposition of n in terms of primes. So, n will be p1 power alpha 1, p2 power alpha 2 dot dot dot pk power alpha k and then we write a by n to be a by p1 power alpha 1, a by p2 power alpha 2 dot dot dot a by pk power alpha k.

So, this is the way we define the Jacobi symbol. This is now defined for any modulus, any general modulus as long as the modulus is a natural number. And of course, I can change now the a to be from natural numbers to integers, not 0 but to a general integer. Now, we note here that the a by p because I am taking a by n and then I am looking at a by p for all these p's, it is possible that some prime p may divide the integer a and by our definition of legendre symbol, if you remember legendre symbol had values 1 or minus 1 whenever a was co-prime to p but whenever a was divisible by p modulo p a 0 and then we define the legendre symbol to be 0.

So, now whenever I am looking at a by n as product of these a by p's is with various powers, it is possible that there is some legendre symbol in the factorization may give you 0. So, even though a is not 0 modulo n you may get the Jacobi symbol a by n to be 0. When it is not 0, it can be 1 or minus 1 because the numbers on the right-hand side of the decomposition are all 1 or minus 1. So, this is our next observation that the value of a Jacobi symbol can be 0, 1 or minus 1.

So of course, whenever a comma n, the GCD is not equal to 1, the Jacobi symbol is going to give you 0 because there is a prime p dividing both a and n and whenever you look at the legendre value of that a modulo that p you are going to get 0 in the factorization. So, the Jacobi symbol a by n is going to be 0. Whenever a comma n the GCD is equal to 1, then all factors on the right-hand side are going to be 1 or minus 1 because then a comma p is going to be one for every p dividing n and then of course the legendre symbol values are 1 or minus 1.

So, in that case we have the Jacobi symbol value to be 1 or minus 1. So, this is a generalization. Whenever we generalize a concept to a bigger set instead of a smaller set, it is likely that some nice properties of the earlier concept may not hold. That is because now you are taking more and more elements where you are applying the concept. So, it is likely that some of the nice properties that were true earlier, now do not hold.

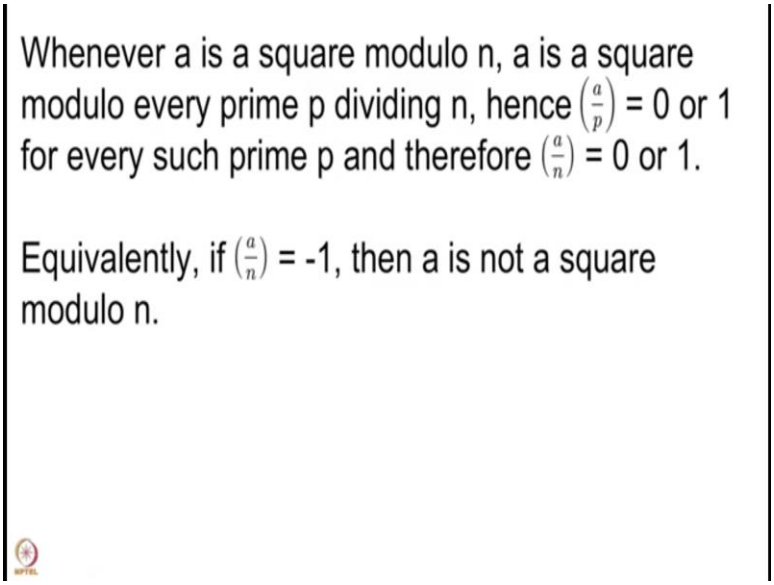
So, one of the property is the following which I am going to now explain. Suppose you start with a being a square modulo n. Then of course a is going to be a square modulo every prime p dividing n and so all the legendre values a by p are equal to 1 and so a comma n is also 1. So, whenever a is a square modulo n, the value of the Jacobi symbol is equal to 1. It can also be 0 whenever the GCD of a and n is bigger than 1.

So, these values can be 0 or 1 and so equivalently, when you have that a comma n is minus 1, so you have that a and n are co-prime and the Jacobi symbol value is minus 1. Then a has to be a non-square modulo n because we saw earlier that whenever a is a square modulo n, all the legendre values are equal to 1, you are raising them to some powers, but all the values are 1. So, the product is going to give you 1.

So, whenever a is a square modulo n, the Jacobi symbol value is equal to 1. And what we say in mathematical terms the contrapositive of this statement says that whenever the Jacobi symbol value is minus 1, then a is not a square modulo n. This is some property which is true for legendre symbol also. However, for legendre symbol you have an, if and only if statement in fact we define legendre symbol with the very motivation of determining the squares modulo a prime p.

So, we started with squares modulo p, we defined the legendre symbol, we defined its generalization called the Jacobi symbol and now we are asking whether these squares behave well with respect to the Jacobi symbol value. So, whenever a is square modulo n, Jacobi symbol value is equal to 1. If the Jacobi symbol value is minus 1, this is not a square. However, it is quite likely that you may have a non-square modulo n and the Jacobi symbol value may still be equal to 1. So, we may not have an equivalent formulation.

(Refer Slide Time: 18:02)



This does not imply, the Jacobi value being equal to 1 need not imply that a is a square modulo n. An example can be constructed in a very simple way. What may go wrong is the following thing. You may have a number a and some number n. Suppose n is product of 2 primes, say p and q, then a by n the Jacobi symbol is product of a by p with the product a, with the legendre symbol a by q. Now it is possible that both a by p and a by q are minus 1. So, a is not a square modulo p, a is not a square modulo q. So, both the legendre values are minus 1 but their product is equal to 1 and therefore the Jacobi symbol value a by n will be equal to 1.

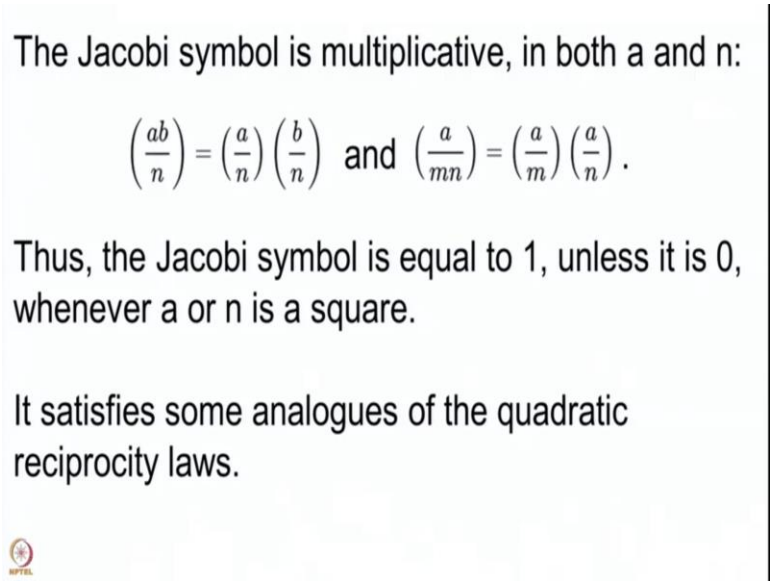
However, a will not be a square modulo n because it is not even a square modulo, the divisor p of n. How do we construct a counter example, this is a good way to construct a counter example this is a thinking which will help us in constructing the counter example. So simplest, let us take odd primes, so the simplest odd prime is 3, 2 is not a square modulo 3, so the legendary symbol 2 by 3 is minus 1. The next prime after 3 is 5. Luckily 2 is not a square modulo 5 as well. So, we have 2 by 3 equal to minus 1 2 by 5 is also minus 1 and therefore to by 15 is going to give you plus 1 but 2 is not a square modulo 15.

In fact, we can compute all the squares model of 15. So, let me call this set gain by Q15, although we have used this notation Q only for quadratic residues modulo a prime. Let me call it again for this non prime modulus. So, 1 square is 1, 2 square is 4, 4 square is 16 which is again 1,

7 square is 49 which gives you 4 and then we have done because 8 is minus 7 and so on. So, we get the same number of elements repeatedly.

Now we observe that the phi 15, the number of elements which are non 0 modulo 15. This is phi 3 into phi 5, so this is 4 into 2 that is 8 and here we are getting 2 squares in this set. So, there are 6 non squares and there are 2 squares. So once again what we had earlier that if you have, if you are looking at the set of squares modulo p, then q p had exactly half the number of elements as there were the numbers of co-prime to p the phi p, this is not true when we are looking at a non-prime modulus. So, this is a way we can construct this example quite easily.

(Refer Slide Time: 21:41)



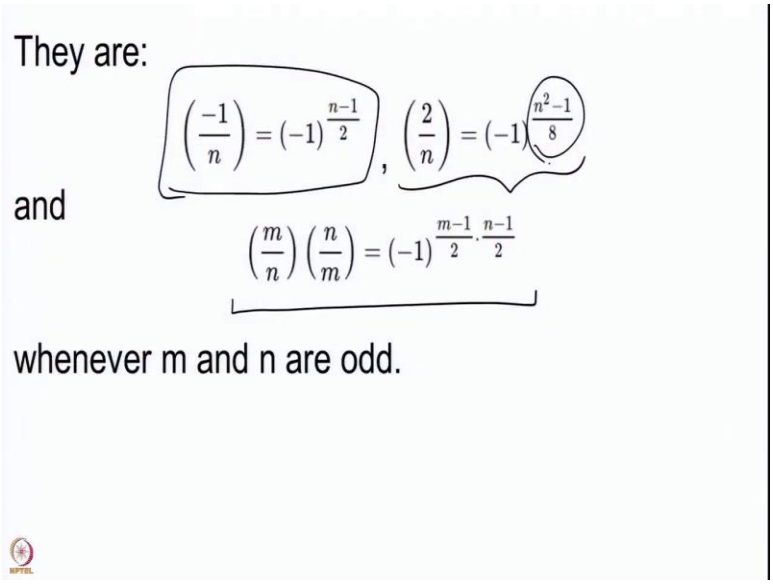
And there are however, other things which are satisfied by Jacobi symbol, which are also satisfied by the legendre symbol, namely that the Jacobi symbol is multiplicative. We know that the legendre symbol is multiplicative when you had ab by p, this was equal to a by p into b by p. So, there was a multiplicativity of the legendre symbol. However, the Jacobi symbol is multiplicative not just in a but also in n. So not just in the numerator, but also in the denominator. What I mean by this is the following thing that ab by n is a by n b by n clearly, but you also have that a by mn is a by m into a by n.

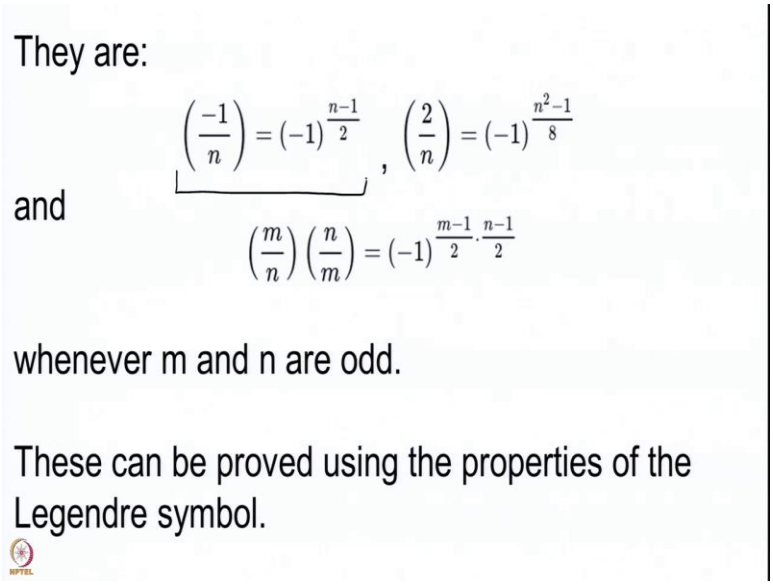
So, this will tell you for instance that the Jacobi symbol is equal to 1 unless it is 0 whenever a or n is a square. Whenever a is a square if you have a to be b square, then a by n is b by n whole square and so depending on whether b by n is 0 or non 0, you get that the value of a by n is 0 or

1. Similarly if your n is m square then a by n is a by m whole square. And once again, the value of a by n will be 1 or 0 depending on whether a by m is non 0 or 0. So the multiplicativity does hold which will help us in computing the values of the Jacobi symbol.

There are some more properties which are true for Jacobi symbol and which were true for legendre symbol, namely that the reciprocity laws are true in some form. So, of course, we cannot expect it to be true in the full generality, but it is true in some form.

(Refer Slide Time: 23:46)





And the form is as follows, that for minus 1 remember once we defined a by n to be a by p1 power alpha 1, a by p2 power alpha 2 dot, dot, dot a by pk power alpha k. I said that we will now extend the values of the Jacobi symbol, to the possibilities where a can be any integer, positive, negative or 0.

So indeed, we can ask for minus 1 and 4 minus 1 we do have this property that for minus 1, we do get the Jacobi symbol minus 1 by n is equal to minus 1 to the power n minus 1 by 2. There will be no question of minus 1 upon n being 0 because no n is going to have a non-trivial GCD with minus 1. So, this is an equation which is always true. This is true whenever n is odd.

So, the Jacobi symbol 2 by n is minus 1 to the power n square minus 1 upon 8. This is always true whenever n is odd. And finally, we have this, a more general reciprocity law. So instead of just having m and n to be primes we have, whenever m and n are odd numbers, we have that this equality always holds. The proofs of these results are not as difficult as they were in the legendre symbol case. In fact, the legendre symbol case will come and help you here. You have to notice some certain things. For instance, when you go to this particular number, you need to notice that this holds whenever it holds for every prime factor of n and so on.

So, these are some small things which you need to observe and then you have the fool proof. So, these can therefore be proved using the properties of the legendre symbol. We will not mention proofs of these facts, but these reciprocity laws do hold. However, I would like to caution you that this equality which is here for minus 1, this need not be true in general.

We had the Euler criterion for legendre symbol, which was a by p congruent to a power p minus 1 by 2 modulo p and that helped us computing the legendre symbol in a nicer way, this need not be true in general. We will talk about this and some other interesting things regarding Jacobi symbol in the next lecture and then in the next lecture, we will also begin our next theme. So, see you soon in the next lecture. Thank you very much.