A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 34
Quadratic Reciprocity Law - II

Welcome back, we are discussing the Quadratic Reciprocity Law and as such I told you that there are three parts of the quadratic reciprocity law. The first part deals with describing when minus 1 is a quadratic residue modulo and odd prime p. Second part which was done as the last result in the last lecture deals with in describing 2 by p the Legendre symbol 2 by p. So, that will tell you when 2 is a quadratic residue modulo p and now we come to the third important part of the quadratic reciprocity law, which will enable you to compute when one odd prime is a quadratic residue modulo another odd prime.

So, let me go straight away to the theorem, but I should tell you that this is one of the most important theorems and this theorem in particular allows you to reduce the various numbers. So, you have when you want to compute a by p, if your number a is very large you will of course go modulo p and then you have the corresponding residue mod p which is going to be between 0 and p strictly less than p and strictly bigger than 0. Because a is always co-prime to be co-prime to the prime p.

So, now you have this number between a 0 to p but even the prime p can be very big and for big primes to compute the quadratic residues the set q p which we had introduced earlier, which is the set of all quadratic residues modulo p. It would not be very practical to compute this set q p simply by doing all the computations by computing all squares up to the integers from 0 to p by 2 to tell what are the possible quadratic residues that could be very big because your prime p can be very big.

So ideally what we would like to do is the following we have this a, which is now less than p and this is a number between 0 to p, but it may have its own prime factors and we already have seen that Legendre symbol is multiplicative that means the Legendre symbol of ab over p is the product of the Legendre symbols of a by p and b by p.

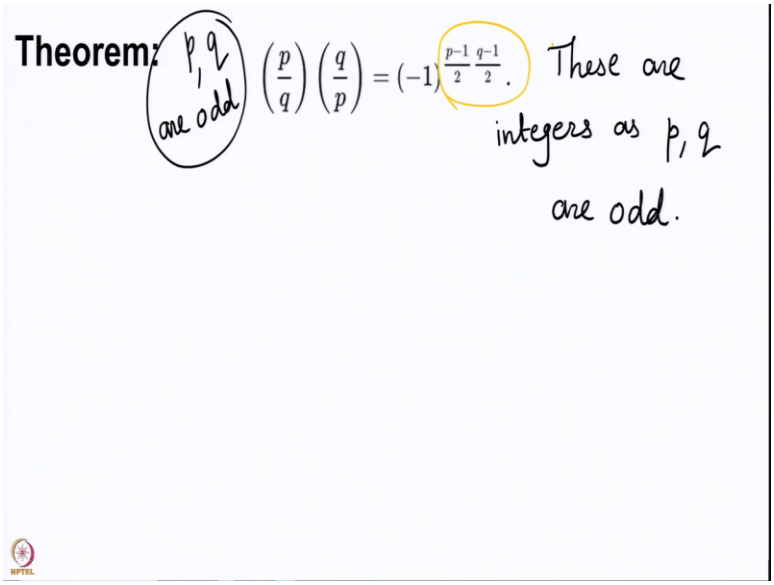
So, we can actually factorize the given number a, which was the residue of the a you started earlier the a you started with earlier and we decompose it into its prime factorization and then for each of the primes which occur there we have to compute whether those primes are squares modulo the given p or not.

But even then you know, what we have done is reduce the problem of determining whether a mod p is 1 or not to q by p is 1 or not where q is some another prime number from 0 to p. This is all the problem has reduced to at the moment. Now, because q is a prime number and q is less than p if you could somehow relate the Legendre symbol p by q with the Legendre symbol q by p then that gives you an advantage because q is less than p. So, when you are computing the Legendre symbol p by q you have the luxury of taking something smaller than q because you will take the residue of p modulo q. So, you are going to now go below q.

Remember you started with a prime q which is from 0 to p and you are interested in finding the Legendre symbol q by p, I am saying that if you relate it to the Legendre symbol p by q by some wave which is going to be our third quadratic reciprocity law then we will need to compute p by q here p is bigger than q. So, I am going to take the residue of p modulo q which is now something which is less than q but now it need not be a prime because I have taken the residue of p the p was a prime, but I am taking its residue modulo q.

So, this need not be a prime. It will have its own prime factors. We will decompose that residue again in terms of the prime factors and so now we have say some r1, r2, rt over q. We want to compute these Legendre symbols. Now these each of the ri are less than q. Once again, if we have the quadratic reciprocity law will be able to write these in terms of q by ri and now q is bigger than ri so further we have to go modulo ri. So, this way we reduce the problem at each stage and then we are able to compute the Legendre symbol. This is the basic idea of getting the quadratic reciprocity the using the quadratic reciprocity law.

(Refer Slide Time: 05:31)

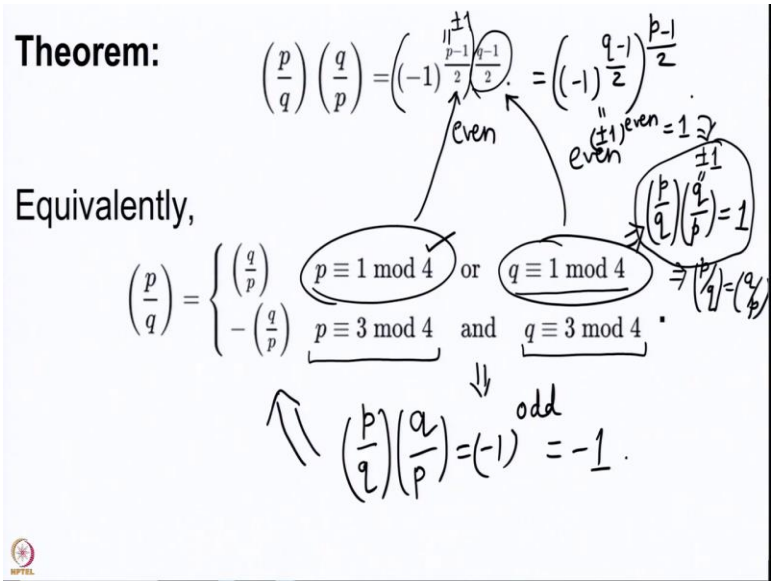


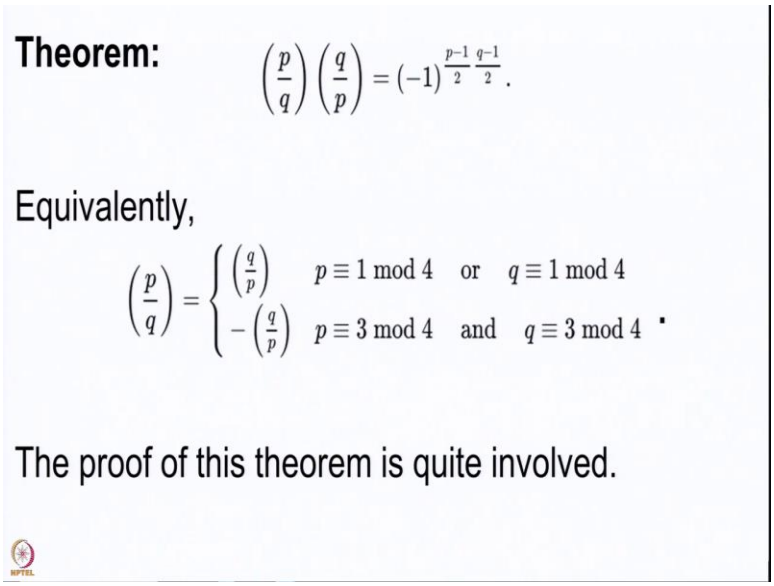
So, let us now go and see this celebrated theorem. The theorem is there in front of you, it says if p and q are odd primes we are now starting with odd primes all the time. If p and q are odd primes then the product of these two Legendre symbols is given by minus 1 to a power and this power is p minus 1 by 2 into q minus 1 by 2.

So, the things that we should always note are the follow following things. This is a standing assumption of course, if you do not have p minus 1 by 2 p and q to be odd, then you are not always going to get each of these to be integers. So, these are integers because we have taken the p and q to be odd primes.

The only other prime we should think about is the prime 2 but 2 by p is something that we have already dealt with. So, here we are taking only the odd prime. So, we have two order primes p and q and then we are able to relate by this theorem the Legendre symbol p by q with the Legendre symbol q by p, this is what we are doing.

(Refer Slide Time: 07:18)





And it has a simpler form equivalently, we have that p by q is equal to the Legendre symbol q by p. So, you switch the places of p and q and you get the same numbers, if either p is congruent to 1 mod 4 or q is congruent to 1 mod 4. Whenever one of these two remember p is an odd prime, so when you go modulo 4 when you take away the multiples of 4 from p the only thing that will be left will be 1 or 3.

So, depending on whether p is congruent to 1 mod 4 or q is congruent to 1 mod 4 you need to have only one of these two to be 1 mod 4. If p is congruent to 1 mod 4 and q is congruent to 3 mod 4, that is okay, if p is congruent to 3 mod 4 and q is congruent to 1 mod 4 that is also okay

or if both are congruent to 1 mod 4 in all these three possibilities the Legendre symbol p by q is equal to the Legendre symbol q by p. This is because whenever p is congruent to 3 mod 4 1 mod 4 this will tell you that this quantity is even and this tells you that this is even.

So, suppose if you have only q congruent to 1 mod 4, then this is an even number. What we are going to do is that we restrict we our attention to minus 1 to the power p minus 1 by 2. This is plus or minus 1. But that to the power an even number is always 1 therefore p by q into q by p will be equal to 1 so this will tell us that the products of these two Legendre symbols is 1 but this Legendre symbol is either 1 or minus 1. So, it is its own inverse in the multiplicative sense and therefore it will tell you that p by q is q by p.

Similarly, whenever p is congruent to 1 mod 4 we get the same result because then we would consider minus 1 to the power q minus 1 by 2 and to this we raise we put the power p minus 1 by 2. So, this number inside is plus minus 1 this two even power will give us 1 and then we are back to this part.

So, whenever p or q any one of them is congruent to 1 mod 4 then you can switch the places without worrying. But if you have that p is congruent to 3 mod 4 and q is congruent to 3 mod 4 this tells you that the product is minus 1 to the power and odd integer, which has to be minus 1 and then it will give us our result that then p by q is minus 1 into q by p.

So, this result which may otherwise seem very complicated does tell us how we are able to get the computation of p by q from the computation of q by p. So, the proof of this result is quite involved meaning even the proof of the last result that we had seen the quadratic reciprocity law 2 by p equal to minus 1 to the power p square minus 1 upon 8 which would tell you that 2 by p is 1 whenever p is congruent to plus or minus 1 mod 8 and p by 2 by p is minus 1 whenever p is congruent to 3 or 5 mod 8.

So, that proof was also involved. If you remember we had written 1, 2, 3, 4 all the way up to p minus 1 by 2 on one side, there were several equations on one side of the equations, we had 1, 2, 3, 4 up to p minus 1 by 2 and on the other side of the equations, we had all multiples of 2, we wrote 1 as minus 1 into p minus 1, which is an even number because p is odd, then we wrote 2 as minus 1 square into 2, 2 is even, then we wrote 3 to be minus 1 power 3 into p minus 3, p minus

3 is even. So, on the other side, we had all even numbers possibly with some sign and on this side we had numbers 1, 2, 3 up to p minus 1 by 2.

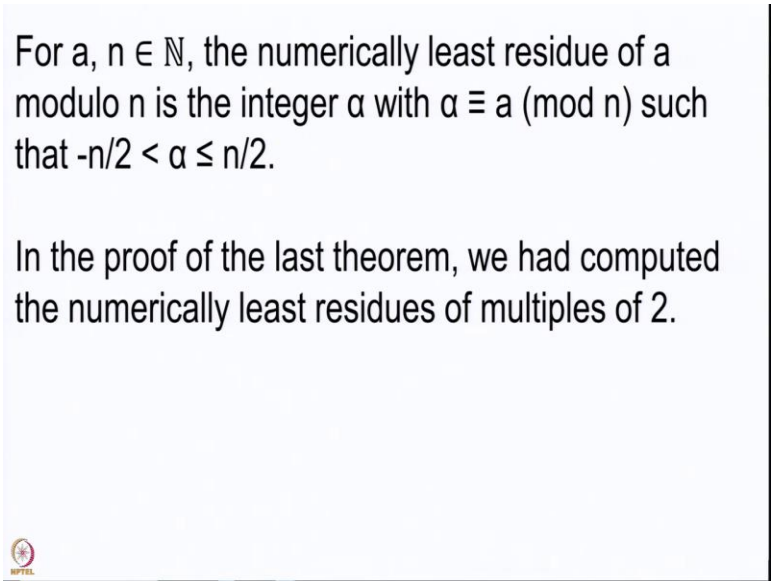
We are going to do the same thing. We are going to look at the so whenever we compute the Legendre symbol for some integer a we will be looking at multiples of a and we have to introduce one technical term here which was easily to see it that that term was hidden in the calculation for the case for 2 by p.

But now we are going to do the general case. So, we have to introduce that technical term that technical term is called the numerically least residue. So, what we are doing is the following thing whenever we have any number a and suppose we are going modulo n and we are trying to find the residues the residue of a modulo n, one standard set of residues where we will take the residue is 0 to n without taking n. So, it will be 0 to n minus 1 this is one very standard set of residues.

But the problem here, is that n minus 1 can be very large. So, when we want to do computations the multiplications et cetera with n minus 1 can be a big competition and so you should replace n minus 1 by minus 1, n minus 2 has to be replaced with minus 2. Because minus 2 or 2 actually is easier to handle when we are doing lots of multiplications et cetera. Even for addition it is quite simple and you are anyway doing the things modulo n so this is what we are going to look at.

So, our ideal set of residuals is not 0 to n minus 1, but it is that set where 0 is actually going to be in this centre you will take half the elements after 0 and half before 0 there will be half negative which will be up to n by 2. So minus n by 2 to 0 to n by 2 that is our set minus n by 2 to n by 2. And here we allow n by 2 because from minus n by 2 and n by 2 we should take only one element there we are allowing n by 2. So when you look at a residue in this set that will be called numerically least residue.

(Refer Slide Time: 14:58)

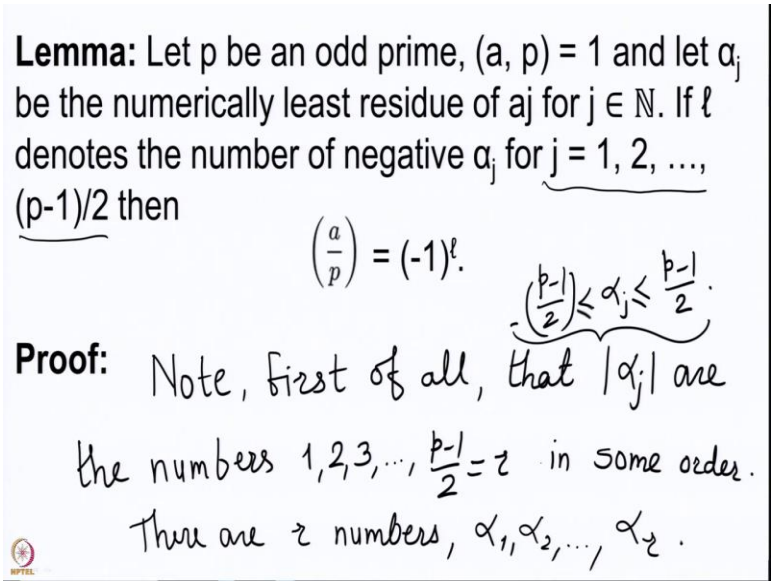


Here is the definition. Whenever we have a and n two natural numbers the numerically least residue of a modulo n is the integer alpha with alpha congruent to a modulo n this has to be there because alpha has be a residue of a mod n with the property that minus n by 2 is less than alpha less than or equal to n by 2.

So, this is the property which is giving it the property of being numerically least this makes our calculations very simple. So, this is what we should be looking at this can be defined for any alpha and any a. And now when I look at the odd prime p and I want to compute the Legendre symbol a by p then I should be looking at multiples of a.

But here is to remind you that when we did the proof of the last theorem where we computed the Legendre symbol 2 by p then we were looking at multiples of 2 and looking at the numerically least residues of them. You may say that you were only looking at 1 to up to p minus 1 by 2, but we had also the sign there. So, we had on the right-hand side all the multiples of 2 and then we had the sign. So, if you were going to put the sign on the other side, you would get the numerically least residues of multiples of 2 modulo p this is what we were getting and here is the small lemma that we have to do before we go on to the major proof.

(Refer Slide Time: 16:51)



So, this Lemma is as follows. Let us read and understand this statement of the Lemma carefully. We start with an odd prime, we start with an element a which is non 0 modulo p. These two are our standard assumptions. Now, let alpha j be the numerically least residue of the product aj for j in N, you take all natural numbers take all multiples of a. So, you would have a 2a, 3a, 4a and so on and for each of them you compute the numerically least residues.

So, you will have alpha 1 which is the numerically least residue of a, then you will have alpha 2 which is the numerical least residue of 2a, then you will have alpha 3, alpha 4, alpha 5 and so on. Now, what we do is that we compute this alpha j for j from 1 to p minus 1 by 2 only for half the elements in z by p.

So, from 0 to so we do not take 0 but from 1 to p minus 1 by 2. So, for these p minus 1 by 2 elements, you take the multiples of a with the correspond with these p minus 1 by 2 elements and then compute the numerically least residues. So, these are all elements which are now lying between minus p by 2 to p by 2 since p is an odd number I can easily say that we are going to have elements strictly between these two.

Some of these can be negative. Some of these can be positive. We count the number of negative such numerically least residues and call that number to be l. This number depends only on a and p because we computed it starting with a and p. So, this number l gives the Legendre symbol a by p this is the statement of the lemma.

The statement of the lemma says let p be an odd prime a be an integer co-prime to p and let alpha j be the numerically least of aj for j from 1 to p minus 1 by 2. Let l be the number of negative such alpha j's then the Legendre symbol a by p is minus 1 power l. In fact, people say that there are no experiments in mathematics, but this is not true. So, I invite you to do this experiment here.

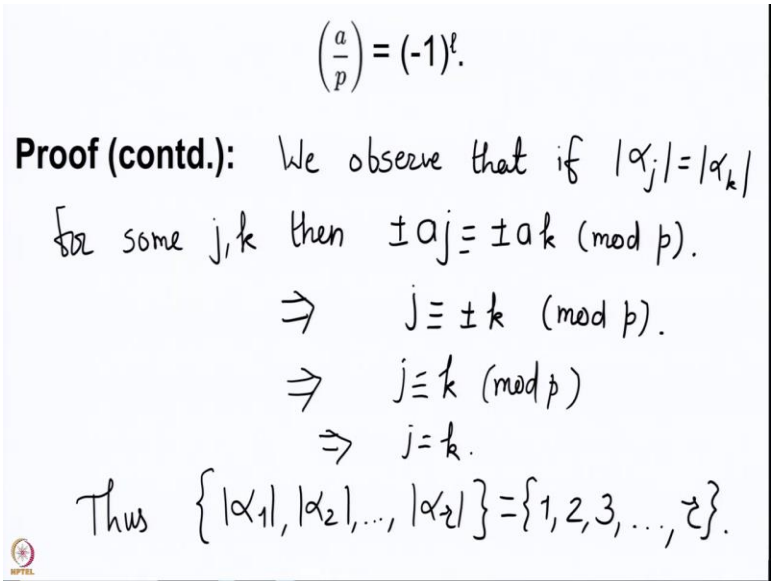
What you do is that you take a prime p say p equal to 11. So that the competitions are not very simple, but also not very difficult. And then you compute these numbers l for various of these a's and do verify that the Legendre symbols a by 11 is actually equal to minus 1 power l for the corresponding l. We will see a proof but seeing a proof and doing actually an experiment on by your own hands these are two different things.

So, we will a proof and we will actually prove this result, but it be nice to do this experiment by hand. So, now let us go towards the proof of this result. So, what we note first of all that mod alpha j are the numbers 1, 2, 3 dot dot dot p minus 1 by 2. Let us call this number r in some order.

Now, why should this be true? So, we note that because of the property on alpha j, we have p minus 1 by 2 negative is less than or equal to alpha j is less than or equal to p minus 1 by 2 this is the property on alpha j, alpha J's are the numerically least residues for these products aj but these are numerically least which means they are from minus p by 2 to p by 2 and now p is odd so alpha j will never be equal to p by 2 or it is negative. So, it will actually be from minus of p minus 1 by 2 to p minus 1 by 2.

So, we have this equation inequality, so we have exactly these many alpha j's moreover we are taking these products for J going from 1 to up to p minus 1 by 2. So, the number of these alpha J's is also r we have these are there are r numbers because you have alpha 1, alpha 2 comma dot dot dot alpha r. So, you have r different numbers, if we could prove that when you put modulus to these r numbers you are going to get different numbers then these will have to be equal to some number from 1 to r.

(Refer Slide Time: 22:54)



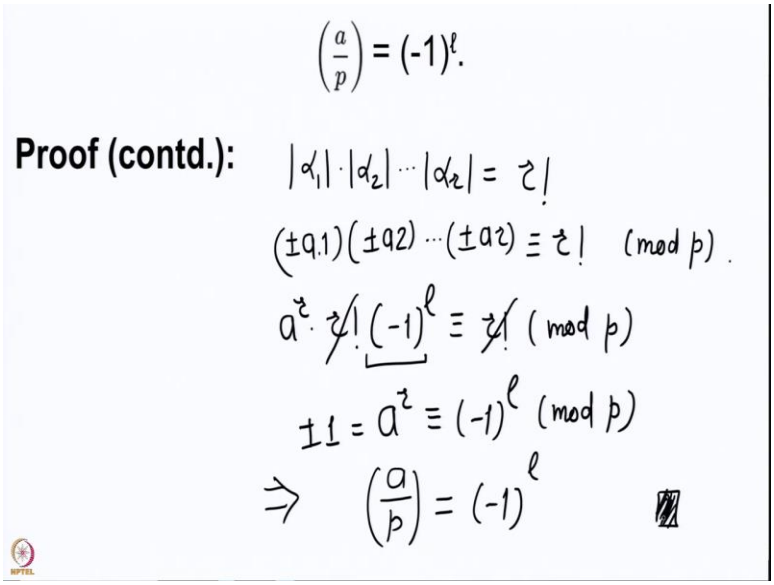
We observed that if mod alpha j is mod alpha k for some j and k, then remember alpha j is the residue for aj with possibly a sign. So, we get this equality modulo p but a is co-prime to p. So, this would then imply that j is congruent to plus or minus k modulo p but both j and k where taken from the set 1, 2, 3 up to r, which is p minus 1 by 2. So, no element of the set 1, 2, 3 up to p minus 1 by 2 can be equal to negative of any other element in the set modulo p.

If you were going beyond p minus 1 by 2 suppose you were taking p plus 1 by 2 then that would be negative of p minus 1 by 2. So, then you would have so once you go one step out of this set, then you would possibly have some non-trivial solution to this equality j congruent to plus or minus k mod p, but since you are taking a very restricted set this has to imply that j is congruent to k mod p but again, this has to imply that j is equal to k because the difference of j and k is if not 0 has to be less than p.

So, if j and k are not equal then you can never have j congruent to k mod of p. So, the mod alpha 1, mod alpha 2, mod alpha 3 these are all positive numbers and because you are taking alpha i to be less than minus r to be bigger than minus r and less than or equal to r you would have that when you take mod these are all now between 0 to r, 0 is not taken, so these are numbers from 1 to r these r distinct numbers from 1 to r. So, in some order the set of mod alpha j has to be equal to the set 1 to r. So, what we then have is this set mod alpha 1, mod alpha 2 up to mod alpha r as

a set is equal to this set. So then take the product on both the sets take the product of elements on both the sets and let us see what we did.

(Refer Slide Time: 26:10)



This is equal to the product 1, 2, 3 up to r. So we get r factorial, but the left hand side is equal to plus or minus a into 1 this is plus or minus a into 2 so on up to plus or minus a into r. So, if I take a out I am going to get a power r then I have 1, 2, 3 up to r so I get r factorial and I have exactly how many negative signs.

So, remember l was our number of negative numerically least residues so this is going to be minus 1 to the power l this is the left-hand side. This is equal to r factorial mod p the right hand, these two can be cancelled because r is less than p. So r factorial is congruent to is non 0 modulo p. So you can cancel them, this is plus or minus 1 therefore you can put it on the other side. But this is also plus minus 1. Remember r is p minus 1 by 2.

So Euler's criteria tells you that a by p which is a power p minus 1 by 2, which now is congruent to minus 1 power l mod p, p is an odd prime you have plus minus 1 congruent to plus minus 1 mod p that tells you that both the sides of this equation will have to be the same. Kind we just complete this proof. So, this is the small lemma which we are going to use in the proof of the quadratic reciprocity law, but we will have to do this proof in the next lecture. So see you until next lecture. Thank you.