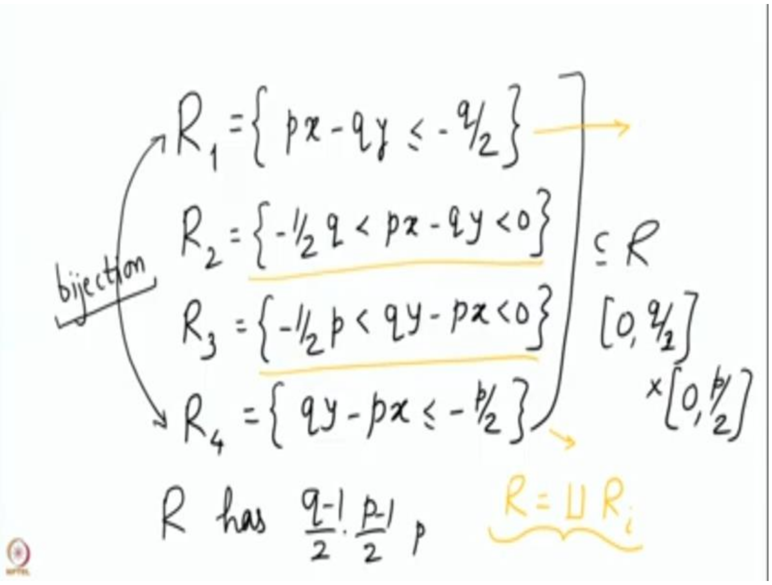
A Basic Course In Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 36
Quadratic Reciprocity Law - IV

Welcome back. We are proving the quadratic reciprocity law and we started with the proof of Gauss lemma in the very first place. After that, we saw a rectangle starting where the x coordinate went from 0 to q by 2, y coordinate went from 0 to p by 2. We called the rectangle to be R and we divided the rectangle into 4 parts. And here are those 4 parts in front of you on the screen.

(Refer Slide Time: 00:47)



$$R_1 = \{ px - qy \leq -q/2 \}$$
$$R_2 = \{ -\tfrac{1}{2}q < px - qy < 0 \}$$
$$R_3 = \{ -\tfrac{1}{2}p < qy - px < 0 \}$$
$$R_4 = \{ qy - px \leq -p/2 \}$$

$\subseteq R$ $[0, q/2] \times [0, p/2]$

bijection

R has $\frac{q-1}{2} \cdot \frac{p-1}{2}$ p

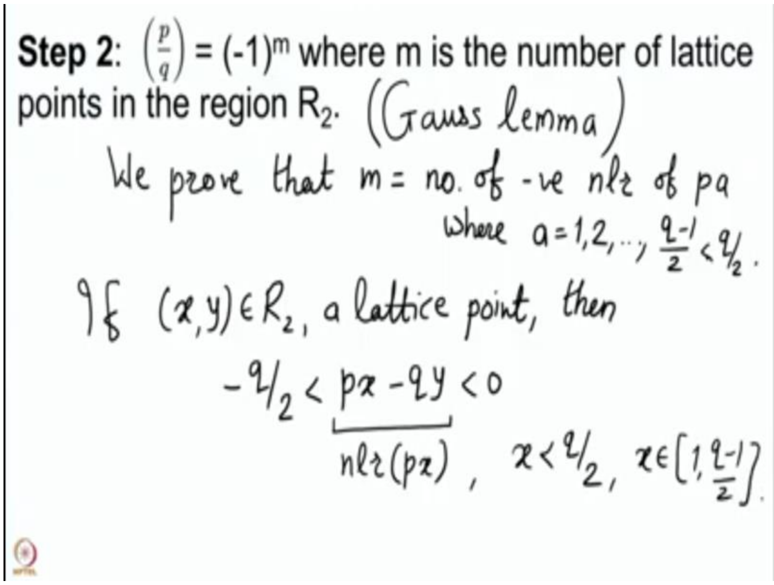
$R = \sqcup R_i$

Where R1 was given by this particular equation. This is R1, this is R2, this is R3 and then we have R4. So these 4 parts together gives you R. So R is disjoint union of R i as far as the lattice points are concerned. Of course, if you are looking at the set theoretic structure of the rectangle R then it is not quite the union of R1, R2, R3, R4 because the lines have been omitted. But without counting, without worrying about the lines, if you are looking at lattice points, then for lattice points, this union is valid.

What we have also seen in the previous lecture itself that the number of lattice points in R1 is equal to the number of lattice points in R4. So there is a bijection between the sets of lattice points in these 2 parts. Therefore if you are counting the number of lattice points in R2, the number of lattice points in R3 then to get the number of lattice points in R, we will need to add twice the number of lattice points in R1. Because the number of lattice points in R1 is the same as the number of lattice points in R4. So, a multiple of 2 needs to be added.

So, when you take power of minus 1, the power of minus 1 is not going to change, whether you keep the power to be only the number of lattice points in R2 and R3, or whether you keep it to be the whole rectangle R. We also noticed that the number of lattice points in the whole rectangle R is q minus 1 by 2 into p minus 1 by 2. This is the number of total lattice points in the rectangle R. Now we go to the rectangle the part R2. Note it carefully it is p (min) p x minus qy to be bigger than minus q by 2 and less than 0. This is the part of the rectangle that we are looking at and we connect it with the quadratic residue symbol p by q.

(Refer Slide Time: 03:24) 10:57



Step 2: $\left(\frac{p}{q}\right) = (-1)^m$ where m is the number of lattice points in the region R_2. (Gauss lemma)

We prove that $m =$ no. of -ve nlr of pa where $a = 1, 2, \ldots, \frac{q-1}{2} < q/2$.

If $(x,y) \in R_2$, a lattice point, then

$$-q/2 < \underbrace{px - qy}_{nlr(px)} < 0, \quad x < q/2, \quad x \in [1, \tfrac{q-1}{2}].$$

This is the second step where we say that p by q is minus 1 power m where m is the number of lattice points in the region R2. And there are no prizes for guessing that we are going to use Gauss lemma. This is going to be used. So we have to look at numerically least residues of multiples of p and see how many of those are negative. That is the number which is m and we are also saying here that m is the number of lattice points in the region R2.

So we have to say, we prove that m is equal to the number of negative numerically least residues of pa where a goes from 1, 2 up to q minus 1 by 2 because remember we are taking the quadratic residue symbol modulo q and it is taken for the element p, so we have to take multiples of p. So these are the multiples of p that we will look at. So we will look at p, 2p, 3p and so on up to q minus 1 by 2 into p. These are the numbers that we look at.

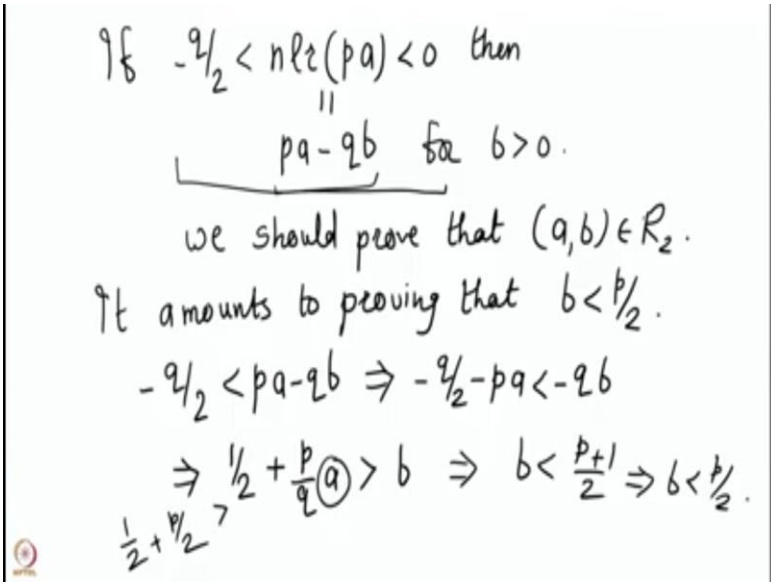
Take their numerically least residues modulo q. See how many of these are negative. So numerically least residues are the residues from minus q by 2 to q by 2 and this is why we had a minus q by 2 in the equation for the region R2. So these are the points which are going from minus q by 2 to q by 2, and the negative ones will be from minus 1 q by 2 to 0. So we prove that there is a bijection between the number of lattice points in R2 and the negative numerically least residues of multiples of p.

We are going to give you a bijection. So if x comma y is a lattice point, then of course, we know the equation of the region R2, we get that minus q by 2 is less than p x minus q y less than 0. So this is your numerically least residue of px and of course x is going from 0 to q by 2. So x can be an integer from 1 to q minus 1 by 2. So the pair x comma y gives you a multiple of p, which has negative numerically least residue namely the multiple px.

This is the multiple px of p with x less than q by 2 but positive such that the numerically least residue modulo q is a negative quantity. So we have a very simple map from the number of lattice points in the region R2 to the negative numerically least residues of multiples of p, sending the pair x comma y to the multiple px. So we have this way map. Now ideally if some multiple p a of p for a between 1 and q minus 1 by 2 has negative numerically least residue, we should get a lattice point, a comma something in the region R2.

Why are we getting it to be a comma something, because the map going from R2 to the numerically least residues is going to give you the first coordinate. So the first coordinate has to tell you what multiple you are taking. So on India the reverse direction if you are taking a multiple a of p by some number say a, which is, which has negative numerically least residue then the corresponding point in the region R2 has to have first coordinate a. That is the lesson we learn from this slide and we go on to try that.

(Refer Slide Time: 08: 30)



$$\text{If } -\tfrac{q}{2} < \begin{array}{c} nlr(pa) \\ \shortparallel \end{array} < 0 \text{ then}$$

$$\underbrace{\underbrace{pa - qb}\ \text{for}}\ b > 0.$$

we should prove that $(a,b) \in R_2$.

It amounts to proving that $b < p/2$.

$$-q/2 < pa - qb \Rightarrow -q/2 - pa < -qb$$

$$\Rightarrow 1/2 + \frac{p}{q}\textcircled{a} > b \Rightarrow b < \frac{p+1}{2} \Rightarrow b < p/2.$$

$$\frac{1}{2} + p/2 \;?$$

So if, so I will write it in this way minus q by 2 is less than the numerically least residue of pa is less than 0. Then what we must get is that this numerically least residue has to be given, it is congruent to pa modulo q. So the difference between the numerically least residue and the quantity pa is a multiple of q, but we should also notice one thing that pa is a positive number. Remember p is a prime. So we are taking p to be a natural number, a is going from 1 to q minus 1 by 2.

So a is positive therefore pa is positive, q is positive. So you cannot add a positive multiple of q to pa to get this negative numerically least residue. So what we do here is that we modify this and get here negative for b positive. So we are actually subtracting a multiple of q from pa. Of course, pa is positive and you want the residue to be less than 0, so you will keep subtracting multiples of q from this. The multiple has to be also unique because the length of this interval is less than q, minus q by 2 to 0.

The length is simply q by 2. So you will have exactly 1 numerically least residue which is of course from minus q by 2 to q by 2, the length is q. So you are going to get 1, you are going to get a unique numerically least residue. So this b that we are going to get is going to be a unique quantity. So starting from this numerically least residue of the multiple pa which is negative, we obtained a positive b and remember on the last page, our equation looked very similar.

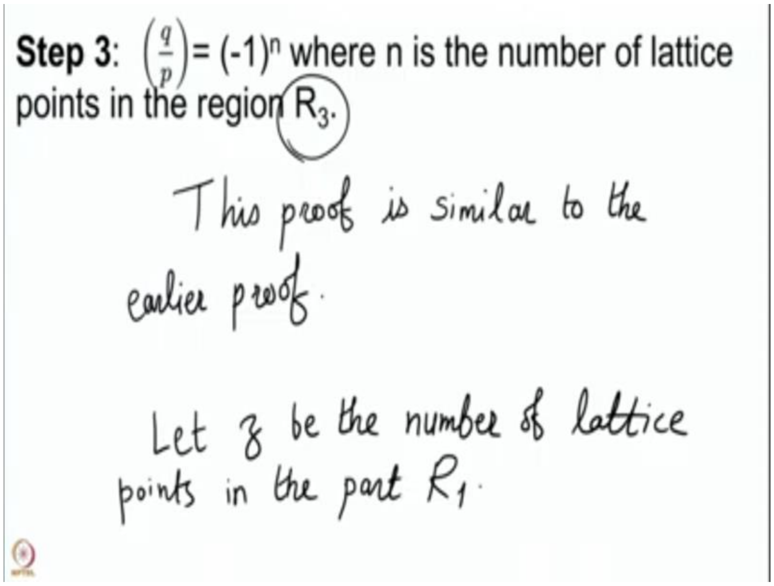
We had px minus qy to be between minus q by 2 and 0. So here if we are getting it to be pa minus q by 2, qb, we should rather prove, we should prove that a comma b belongs to R2. We should prove that it belongs to the region. You may think that indeed this is the equation for the region R2, minus q by 2 less than pa minus qb less than 0, but we should also prove it amounts to proving that our b is less than p by 2. The y coordinate should not go beyond p by 2.

That is the thing that we should prove. That is quite easy actually because we have minus q by 2 less than pa minus qb. We use this side of the inequality to get the result that we want, of course with the proper condition on a. So this will imply that minus q by 2 minus pa is less than minus qb and now you multiply by minus 1 everywhere to get the other side of the inequality. So which gives you and you also cancel out q, so it gives you that 1 by 2 plus p by qa is bigger than b.

And then we notice that since a was less than q by 2, this part is less than 1 by 2 plus p by 2 and therefore b, which is an integer less than p plus 1 by 2 should have the property that b is actually less than p by 2. So what we have proved is the following thing. Let me just say that in words once again, that we took the negative numerically least residues of multiples of p by the numbers 1 to q minus 1 by 2.

This number when put to the power of minus 1, gives you the Legendre symbol p by q. But we also proved that this number is the same as the number of elements in R2. So therefore the Legendre symbol p by q is minus 1 power m, where m is the number of elements in the part R2, the number of lattice points in the region R2. There is a similar step that we will have to do to tell that q by p. This is the other part of the reciprocity. Now you are taking the Legendre symbol of q with respect to p.

(Refer Slide Time: 14:18)



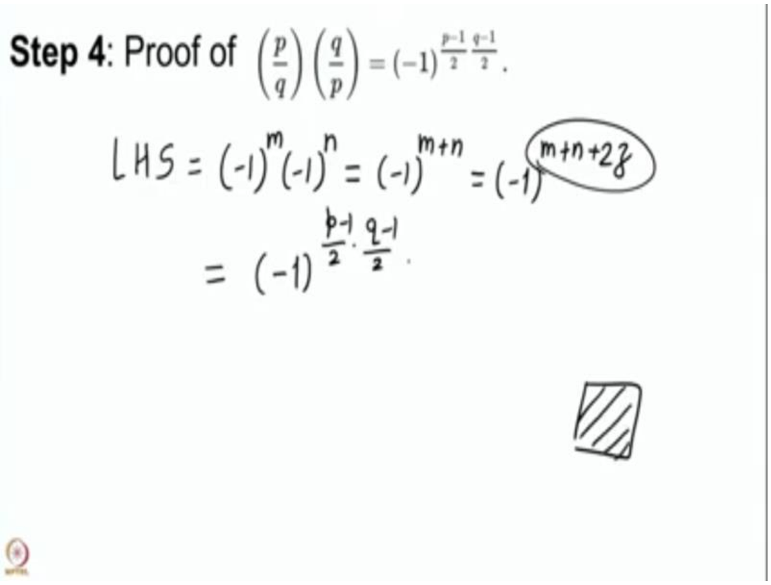
Step 3: $\left(\frac{q}{p}\right) = (-1)^n$ where n is the number of lattice points in the region R_3.

This proof is similar to the earlier proof.

Let z be the number of lattice points in the part R_1.

This is given by minus 1 power n, where n is the number of lattice points in the region R3 and this proof is similar to the earlier proof. So I am not going to do it. Let us just set up one notation that let z be the number of lattice points in the region in the part R1 and we have seen that R1 and R4 have the same number of lattice points. So z also the number of lattice points in the part R4. Now with all this, we can prove the final part of the quadratic reciprocity law as follows.

(Refer Slide Time: 15:39)



Step 4: Proof of $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

$$LHS = (-1)^m(-1)^n = (-1)^{m+n} = (-1)^{m+n+2z}$$
$$= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

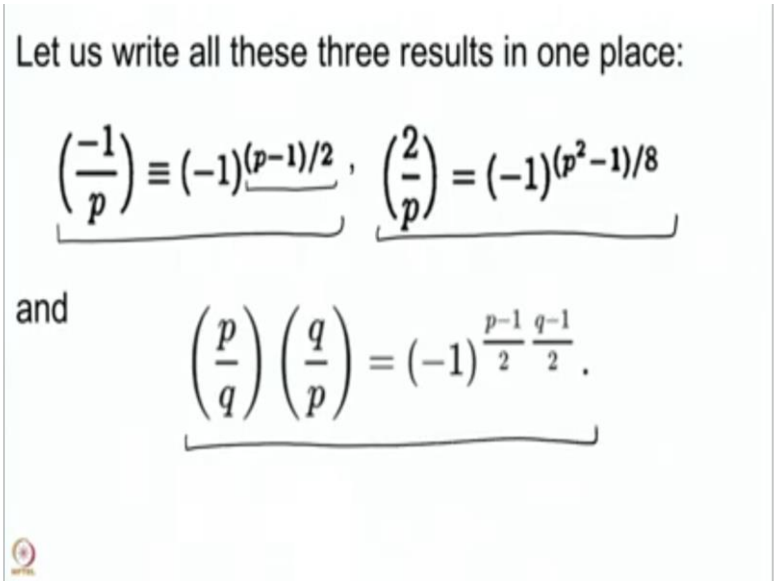
▨

We want to prove this now that p by q into q by p is minus 1 to the power p minus 1 by 2, q minus 1 by 2. LHS if you remember is minus 1 to the power m into minus 1 to the power n, given by the previous two steps, which gives you minus 1 to the power m plus n but if you add an even number to this power, then you do not get anything different. So you get m plus n plus 2z but this is now the number of lattice points in the region R which is equal to the product of these two numbers.

Let me draw a big rectangle here because this was indeed a very long proof but now this is proved. So to quickly recall the proof what we did was that we constructed a rectangle having the number of lattice points to be equal to p minus 1 by 2 q minus 1 by 2. We divided it into 4 parts. The 2 middle parts gave you the number of lattice points where was giving you the Legendre symbols p by q and q by p respectively, and the remaining 2 parts had the same number of lattice points.

So when you counted the number of lattice points up to parity the number of lattice points in the whole region, which is p minus 1 by 2 into q minus 1 by 2 turned out to be the same as the number of lattice points in these two middle regions which gave you the product of the Legendre symbols. So this is the third and the main part of the quadratic reciprocity laws. There are three parts. Let me recall these three for you once again.

(Refer Slide Time: 17:44)



Let us write all these three results in one place:

$$\underline{\left(\frac{-1}{p}\right) \equiv (-1)^{\underline{(p-1)/2}}}, \quad \underline{\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}}$$

and

$$\underline{\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}}.$$

So these are the three results that we have in one place. The first one tells you how to compute the Legendre symbol for minus 1. So the Legendre symbol for minus 1 is obtained by this formula, which is simply the Euler's criterion for any number a, but you can see easily from this part when minus 1 is the square mod p and when it is not a square mod p. This is all for odd primes. For p equal to 2 all the non zero numbers are odd numbers and they are all congruent to 1 mod 2 and therefore they are all squares. So we are only looking at odd primes.

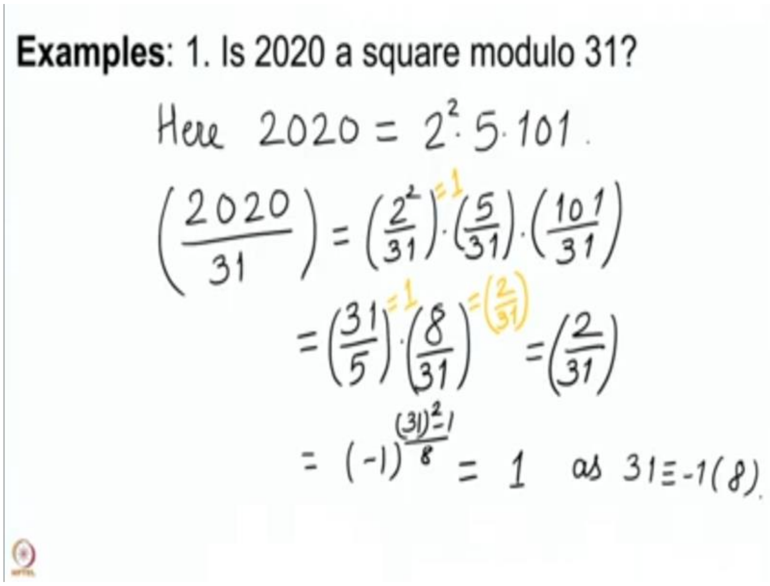
This tells you when 2 is a square mod p and then this is the final part of the quadratic reciprocity law. Let me tell you how we are going to use these 3 laws to do the computation. The computation would typically be a by p where you have a prime p in the denominator and a to be some number. You will go modulo p and get a residue for p for a by modulo p. This residue will lie between 0 to p.

Now, even if you start with a to be a prime or whatever a you have, it is possible that the a that you have obtained, the residue for a that you have obtained may not be a prime. In that case, you will be able to decompose it and we also know that Legendre symbol is multiplicative. Further if there are already some squares in the factorization of a, you can ignore the squares because a square into something is a square if and only if that something is a square.

We are going modulo p which is a prime and you are looking at things which are co-prime to p. So you can divide by the numbers which are co-prime to p so that will tell you that you can cancel the squares, you can ignore the squares while computing the residue symbols the Legendre symbols. So we have a by p which we have written as product of various distinct primes now because once the prime comes with higher multiplicity, you can cancel the even numbers from the multiplicities and so you will be left with only those primes which come with odd powers.

So you have p1 by p, p2 by p, up to say pr by p. If any of these p1, p2, pr is equal to 2, we will use the second law to compute the Legendre symbol 2 by p. And for odd ones, you are going to reduce the case one by one as we have explained in the last lecture to be able to finally compute the Legendre symbol. Let us do an example and since we are in 2020 now, let us try to answer this question whether 2020 is a square modulo the prime 31.

(Refer Slide Time: 20:48)



Examples: 1. Is 2020 a square modulo 31?

Here $2020 = 2^2 \cdot 5 \cdot 101$.

$$\left(\frac{2020}{31}\right) = \left(\frac{2^2}{31}\right)^{=1} \cdot \left(\frac{5}{31}\right) \cdot \left(\frac{101}{31}\right)$$

$$= \left(\frac{31}{5}\right)^{=1} \cdot \left(\frac{8}{31}\right)^{=\left(\frac{2}{31}\right)} = \left(\frac{2}{31}\right)$$

$$= (-1)^{\frac{(31)^2-1}{8}} = 1 \quad \text{as } 31 \equiv -1 (8).$$

So ideally you should reduce 2020 modulo 31 and see what is the residue you get. But here we first of all observe that 2020 has a nice factorization. 20 divides 2020 and 20 is nothing but 2 square into 5 into 101. So when we are computing the Legendre symbol, 2020 by 31 this Legendre symbol is 2 square by 31 into 5 by 31 into 101 by 31. This 1 because this is already a square, so this Legendre symbol is 1. Therefore we can ignore this and do the remaining computation. Here 5 by 31.

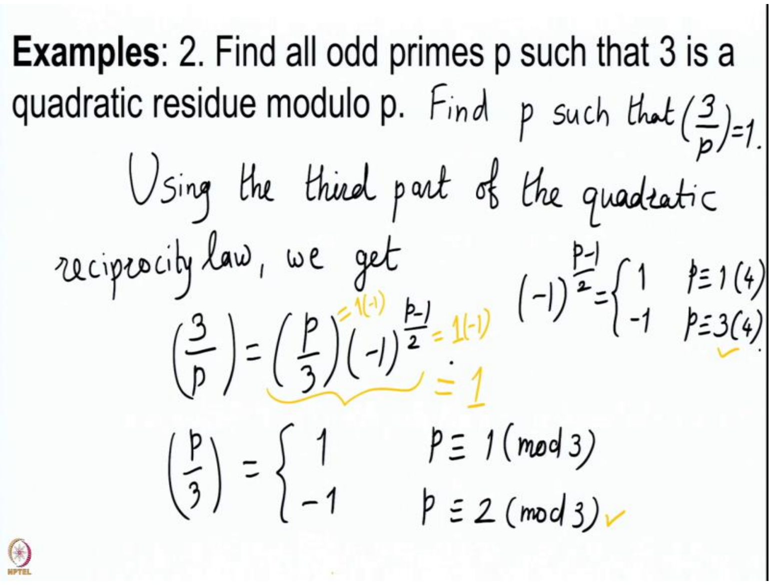
We are going to look at, 5 and 31 are both primes now but 5 is congruent to 1 modulo 4 so we can switch their order without (change) having to change the sign. So we get it to be 31 (up) by 5, the Legendre symbol 31 by 5 into 101 modulo 31. Now we go modulo 31. So 31 into 3 is 93. Once you take away 93 from 101, you get 8 by 31. So our 2020 by 31, the Legendre symbol is the product of these 2 Legendre symbols.

Further modulo 5 31 is a square because it is same as 1, mod 5. So this Legendre symbol is 1. Here 8 is equal to 4 into 2. So this Legendre symbol is simply 2 by 31. The 4 that you have in the factorization of 8 can be ignored because it is a square. So the final computation that we need to do is this, 2 by 31. We use the second law in the quadratic reciprocity law to get this to be minus 1 to the power p minus, p square minus 1 by 8.

So you will have to look at 31 square minus 1 by 8, but this is 1 because 31 is minus 1 modulo 8. So whenever p is congruent to plus or minus 1 mod 8, 2 is a square modulo p, 31 congruent to minus 1 mod 8. So this tells you that indeed 2020 is a square modulo 31. Now, what is its square root? That you may be able to compute by reducing modulo 31 and see where 2020 goes. So this is how we are going to use the three parts of the quadratic reciprocity law, which will tell you whether a given number is a square modulo the given odd prime or not.

We can use this in even better way. We can actually compute all primes p such that 2020 is a square modulo that prime p. That can also be done, because for instance if I wanted to know what are the odd primes such that 2 is a square modulo p. Then the second law will tell me that p congruent to plus or 1 minus 1, plus or minus 1 modulo 8 are the primes where 2 is a square. For the other odd primes 2 is a non square. So if you can do it for 2, why not do it for 3. So let us use the quadratic reciprocity laws and try to find all the odd primes p such that 3 is a quadratic residue modulo p.

(Refer Slide Time: 25:03)



Examples: 2. Find all odd primes p such that 3 is a quadratic residue modulo p. Find p such that $\left(\frac{3}{p}\right)=1$.

Using the third part of the quadratic reciprocity law, we get

$$\left(\frac{3}{p}\right)=\underbrace{\left(\frac{p}{3}\right)^{=1(-1)}(-1)^{\frac{p-1}{2}=1(-1)}}_{\,}\doteq 1 \qquad (-1)^{\frac{p-1}{2}}=\begin{cases}1 & p\equiv 1(4)\\ -1 & p\equiv 3(4)\ ✓\end{cases}$$

$$\left(\frac{p}{3}\right)=\begin{cases}1 & p\equiv 1 \pmod 3\\ -1 & p\equiv 2 \pmod 3\ ✓\end{cases}$$

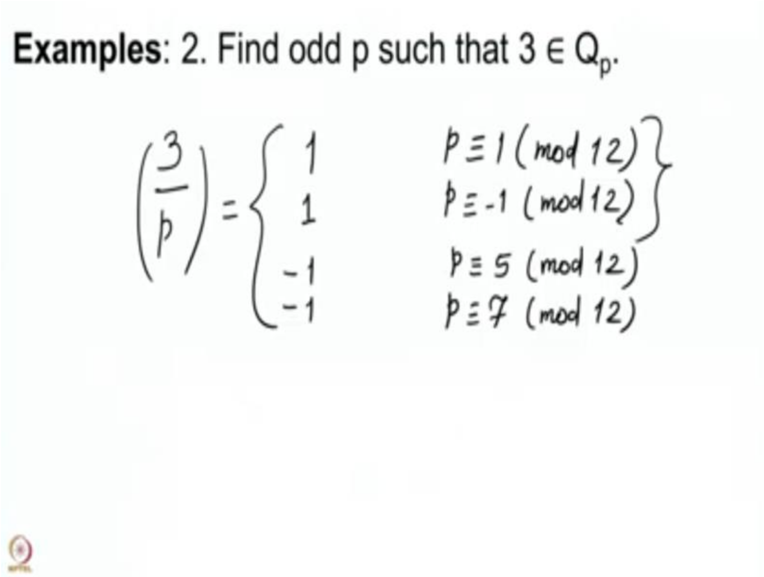
So what we are going to do is to compute. So find p such that this Legendre symbol is 1. This is what we have to do. So of course, if your p is 2, 3 is a square. So we are not going to consider the prime p equal to 2. We are looking at odd primes anyway. So here we have to switch the orders because 3 by p is not very useful whereas p by 3 would be useful because modulo 3 we know what are the squares mod 3.

Modulo 3, there are only 2 non 0 numbers 1 and 2 and out of these 2, 1 is a square 2 is a non-square. So we are going to use using the third part of the quadratic reciprocity law. We get 3 by p is p by 3 into minus 1 to the power 3 minus 1 by 2, which is just 1 and p minus 1 by 2. So this is what we have. Now this, so here p by 3 is equal to 1 or minus 1 depending on whether p is congruent to 1 mod 3, or whether p is congruent to 2 mod 3.

And minus 1 to the power p minus 1 by 2, this quantity is 1 when p is congruent to 1 mod 4. And this is minus 1 when p is congruent to 3 mod 4. So when is this product going to be equal to 1, we want this whole thing to be 1. Then this can be 1 when you have this equal to 1 and this equal to 1. So there are two conditions on p. That p has to be 1 mod 3 and p has to be 1 mod 4 and we use the Chinese remainder theorem.

If you remember the result that we have proved from some earlier parts of our lectures that if you have this congruence modulo 3 modulo 4, 3 and 4 are both co-prime. Therefore modulo 12 there is a unique congruence class, residue class. That is actually the congruence class 1 mod 12. So when p is congruent to 1 mod 12, both the numbers p by 3 and minus 1 to the power p minus 1 by 2 are both 1. So their product is 1 and therefore we get that 3 by 2.

(Refer Slide Time: 28:34)



Examples: 2. Find odd p such that $3 \in Q_p$.

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{12} \\ 1 & p \equiv -1 \pmod{12} \\ -1 & p \equiv 5 \pmod{12} \\ -1 & p \equiv 7 \pmod{12} \end{cases}$$

So 3 by p equal to 1 or p congruent to 1 modulo 12. This is one case. In the second case, you can have both equal to minus 1 and even then we will get the product to be 1. So we have to take this case and this case but here we observe that this is 2 mod 3, here it is 3 mod 4. So modulo 12, we have a unique class which is given by 11 mod 12. For 11, when you go modulo 4 you get 3 and when you go modulo 3 you get 2.

Another way to see this is that both these congruence classes are given by p congruent to minus 1 mod 3 and p congruent to minus 1 mod 4. So we have in the next line that p congruent to minus 1 mod 12 will also give us the same thing that it is 1 modulo. The Legendre symbol is 1. And the Legendre symbol happens to be minus 1 in all the remaining cases which are p congruent to 5 mod 12 and p congruent to 7 mod 12.

There are these other 2 odd numbers modulo 12 which are 3 and 9 but a prime cannot be congruent to 3 or 9 modulo 12 because any such prime will then have to be divisible by 3, but we are looking at the residue behaviour of 3. So we are not going to take the prime equal to 3. So we are looking at all odd primes not equal to 3 such that 3 is a square modulo the prime and the answer is that such a prime has to be 1 or minus 1 modulo 12.

So we actually get a congruence class. We get the solution in a, an arithmetic progression. It can be 1 mod 12 or minus 1 mod 12. So there are two arithmetic progressions 12 k plus 1, 12 k minus 1. In these whatever primes you have will have the property that 3 is a quadratic residue modulo this prime. Similar computations can be done for 5. Then you can do them for 30 because 30 is 2 into 3 into 5.

2 will give you some residue restrictions on P. 3 will give you some residue restrictions. 5 will give you some residue restrictions and then you have to take the LCM of these restrictions to get the answer for 30 60 and indeed for any number a. We will try to see whether we can do any of these either in the next lecture or in the tutorial problems. So with that we will stop at this point and see you in the next lecture. Thank you.