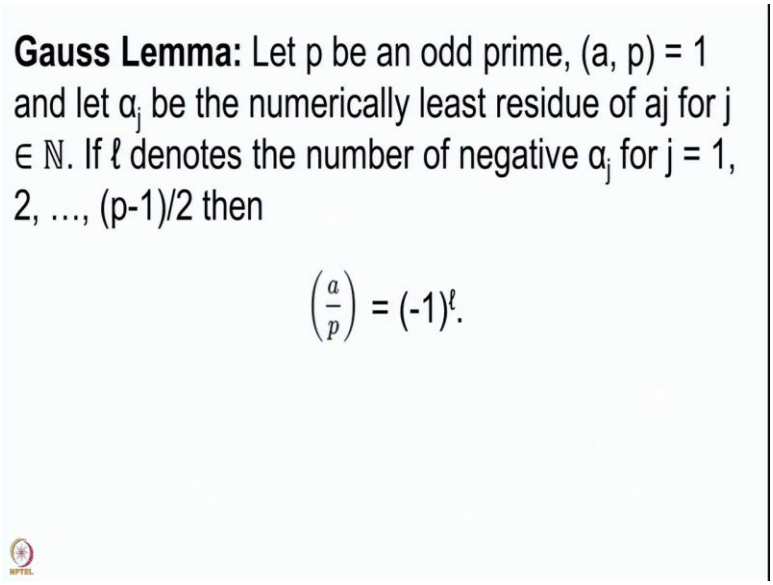
A Basic Course In Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 35
Quadratic Reciprocity Law - III

Welcome back, we are discussing the Quadratic Reciprocity Law and we proved the Gauss lemma in the previous talk. So, here is the statement of the Gauss lemma that we have seen.

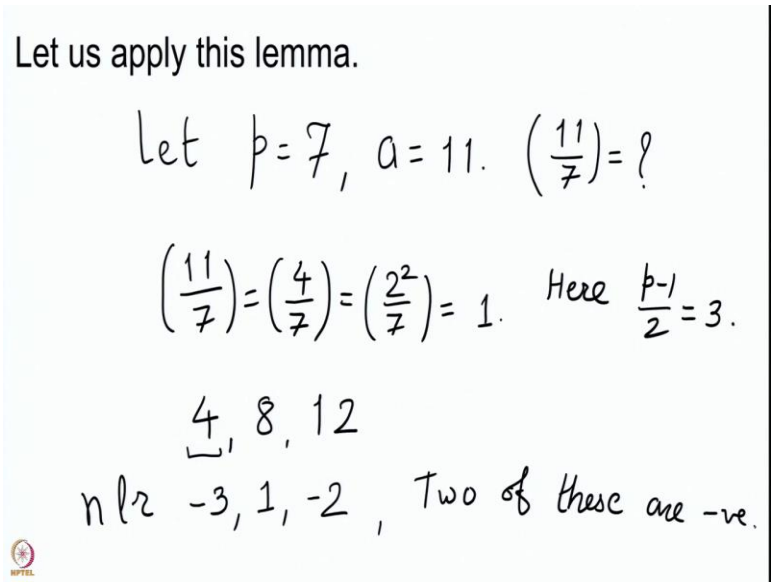
(Refer Slide Time: 00:37)



Suppose we have a prime, an odd prime and take any integer a which is co-prime to the odd prime p and we compute these numerically least residues for various of these multiples of a from j equal to 1 to p minus 1 by 2. So, we compute all these numerically least residues see how many of these are negative. Remember the numerically least residues for a prime p are the residues from minus p by 2 to p by 2.

And so, among these we are looking at how many of the multiples of a starting from a to a so on up to a into p minus 1 by 2 have negative numerically least residues. If that number is l than Gauss lemma says that the Legendre symbol a by p is minus 1 power l. It is a very powerful lemma it is a very powerful statement and it allows you to compute the Legendre symbol very easily very, it allows you to compute it readily.

(Refer Slide Time: 01:49)



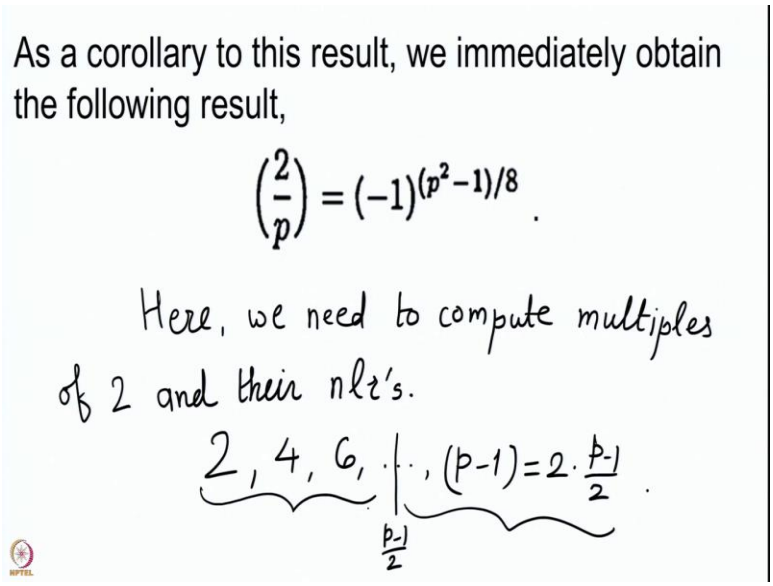
So, let us do some computation and see whether we can apply this result. Suppose p is 7 and say that we want to compute the Legendre symbol for a equal to 11. So, we are asking for this Legendre symbol. Now when you go modulo 7, 11 is 4. So, 11 by 7 is nothing but 4 by 7, the Legendre symbols are same and we know that 4 is the square of 2. So, this is equal to 1 but let us also verify this using Gauss lemma.

So, we look at p equal to 7 and here p minus 1 by 2 is 3. So we have to take first three multiples of 4, they are 4, 8 and 12 and then we take their numerically least residues. So, the numerically least residues, remember 4 is bigger than 7 by 2. So, we take the residue for 4 to be minus 3. So this is minus 3, 8 is equal to 1 modulo 7 so the numerically least residue for 8 is 1. 12 is same as 5 modulo 7 but 5 is also bigger than 3 by 2. So for 5, we have to take minus 2. So, the numerically least residues are these and then we say that two of these are negative.

So, when we want to compute the 11 by 7, or 4 by 7, we will be putting minus 1, we will be taking minus 1 square and which should give you 1. So, you can also do this computation for some another a because we know that modulo 7, 1 is a square being a square of 1, 4 is a square being square of 2, and 9 which is also same as 2 is square of 3. So 1, 2 and 4 these are three squares. Then you may check the, you may compute the Legendre symbol of 3 or 5 or minus 1 and see what we get here.

So, the Legendre symbol can be computed very easily using this lemma called Gauss lemma and we have seen that we were motivated to think about this because we saw the negative numerically least residues for multiples of 2, which came in the proof of the quadratic reciprocity symbol for 2, 2 by p. So, can we obtain that result using Gauss lemma, and indeed we can obtain it quite easily.

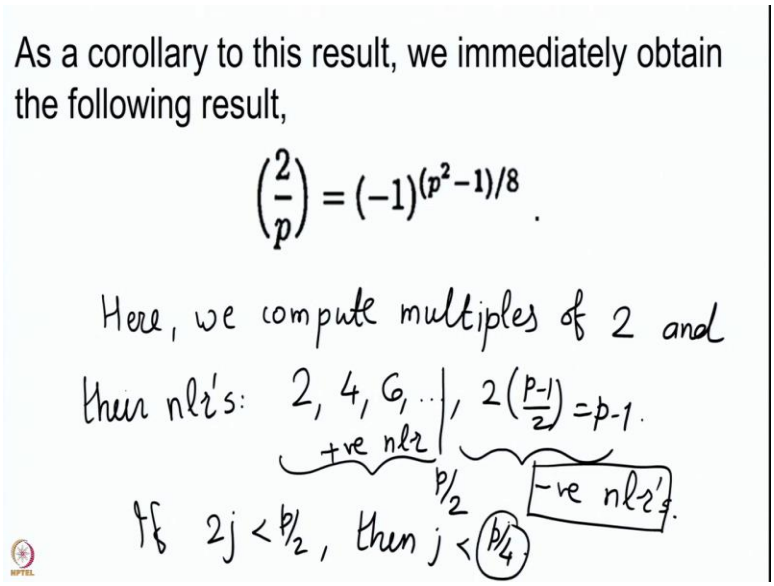
(Refer Slide Time: 04:54)



So, here we need to compute multiples of 2 and their numerically least residues, this is what we need to compute. So, we will be looking at the multiples of 2 which are 2, 4, 6 and so on. And we have to count the, we have to take these multiples up to, we multiply up to, when we multiply 2 by p minus 1 by 2. So, the final number that we get here is p minus 1 which is 2 into p minus 1 by 2. These are the p minus 1 numbers that we are going to, p minus 1 by 2 numbers that we are going to see.

And here somewhere in between we are going to get the number p minus 1 by 2. So, what we are going to do is to see how many of these multiples are less than p minus 1 by 2 and how many of these multiples go beyond p minus 1 by 2. So, this is the computation that we have to do. And so we are going to obtain the quadratic reciprocity law for two the Legendre symbol 2 by p. This is going to be computed using Gauss lemma and for that we need to compute.

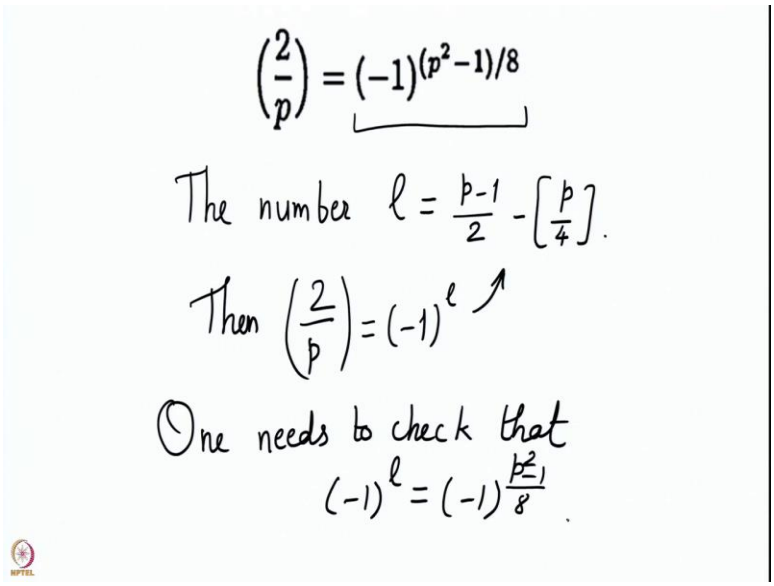
(Refer Slide Time: 06:43)



So, here we compute multiples of 2 and their numerically least residues. So, the multiples are going to be 2, 4 which is 2 into 2, then 6 which is 2 into 3 up to 2 into p minus 1 by 2. So, we get total p minus 1 by 2 multiples of 2. And somewhere here we will have the number p by 2 we should count how many of these multiples of 2 are less than p by 2. So, you see if you have 2j to be less than p by 2 then, then j has to be less than p by 4.

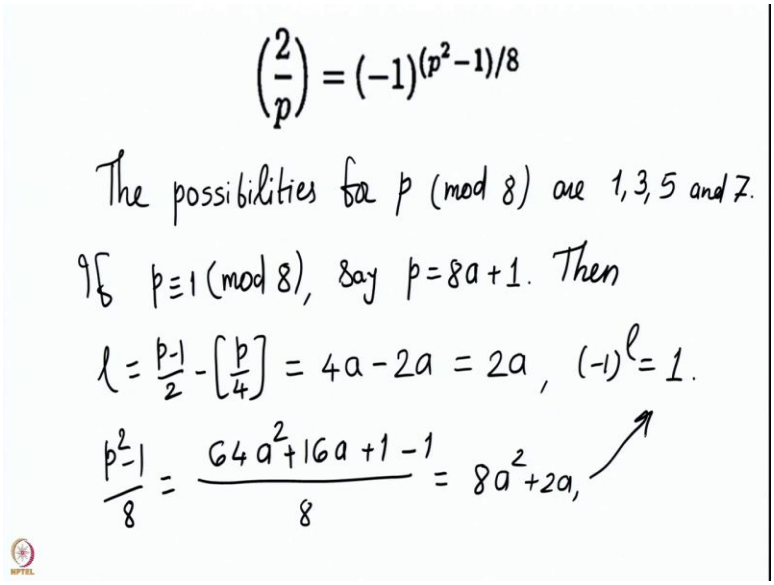
So, the number of numerically least residues which are going to be bigger than 0 is the integral part of p by 4. Because once you go beyond this quantity, these will all give you negative numerically least residues. So, all these are going to be negative. These are the only which are the positive numerically least residues. So we have to remove these, this quantity, the integral part of p by 4, from the total number of multiples that we have.

(Refer Slide Time: 08:30)



So, the number l, the number l is equal to p minus 1 by 2 minus the integral part of p by 4 and then the Legendre symbol 2 by p is minus 1 power l for this quantity. Now to check whether this is indeed equal to the number that we have here, you will have to do the calculation. So we, one needs to check that minus 1 power l is equal to minus 1 to the power p square minus 1 upon 8. And this can be checked by checking various possibilities of primes congruent modulo 8. I will do one case as an example and leave other three cases for you.

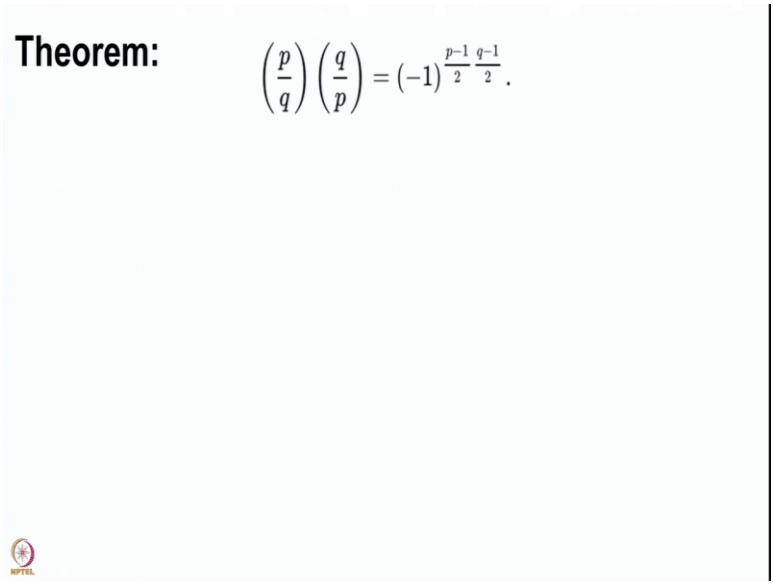
(Refer Slide Time: 09:44)



So, the possibilities for p mod 8 are 1, 3, 5 and 7. If p is congruent to 1 mod 8, say p equal to 8a plus 1. Then l which is p minus 1 by 2 plus integral part of p by 4, since we are taking power of minus 1 plus or minus actually does not make any difference but let us be precise. So, p is 8a plus 1 when you subtract 1 from p you get 8a and you divide by 2 we get 4a minus 8a plus 1 upon 4 is 2a plus 1 by 4 and therefore the integral part will give you simply 2a. So, we do get l equal to 2a and therefore minus 1 power l is 1. On the other hand p square minus 1 by 8 is going to give you 64a square plus 16a plus 1 minus 1 upon 8 and we see that this is 8a square plus 2a and this also gives you the same power.

So, this is the calculation that we need to do for each of these four congruence classes modulo 8 namely p congruent to 1 mod 8, p congruent to 3 mod 8, p congruent to 5 mod 8 and p congruent to 7 mod 8. So doing the computation for these four cases would tell you what the Legendre symbol of 2 modulo p is going to be, once we have the Gauss lemma with us. So we have proved Gauss lemma in last lecture. In this lecture we recalled it and also used it to compute the Legendre symbol of 2 by p.

(Refer Slide Time: 12:24)

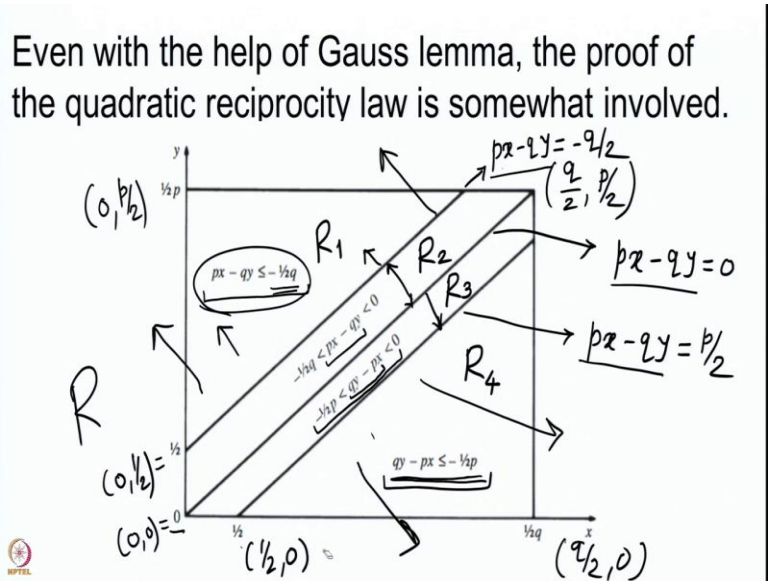


Now, we go towards the main proof of proving the main reciprocity law the main quadratic reciprocity law, which is here in front of you the, in the slide. So the reciprocity law says that the product of the Legendre symbols of for p mod q and that for q mod p is minus 1 to the power p

minus 1 by 2 into q minus 1 by 2. Of course, we are going to use Gauss lemma to prove this but even with Gauss lemma this proof is still somewhat involved.

And this is involved because we will have to do some explicit counting. You will appreciate that even in the last case when we prove the quadratic reciprocity law giving you the value of the Legendre symbol 2 by p there were these four cases where we had to do the computation. So a similar computation will be needed to be done, if you want to do the proof in general.

(Refer Slide Time: 13:15)



So, here the trick is to look at one particular rectangle in R2 and to look at lattice points in this rectangle. So, the rectangle is this rectangle. It has four points, the four end points. This is the point 0 0, here you are x coordinate is 1 by q, 1 by 2 q and y coordinate is 0, so this is nothing but q by 2 comma 0. Here you have x coordinate 0, y coordinate p by 2 and here you have q by 2 comma p by 2. This is our whole rectangle which we denote by R. R stands for rectangle.

We decompose it into four parts. So we have R1, R2, R3, R4 going from top to bottom. These are four parts. We are not taking these slanted lines, but let us look at this slanted line. So, what is the equation of this slanted line, the point 0 0 belongs to this line and the point q by 2, p by 2 is also there on the line. So, you can easily see that this line is given by px minus qy equal to 0. Of course, this is a line passing through 0. So, this is a linear subspace and so the constant term has to be 0. 0 0 belongs to its the constant term is 0.

And the slope can be appropriately counted because you know one non-zero point on this line. So that will tell you that the equation of this line is px minus qy equal to 0. Now, this line is parallel to the diagonal line of the rectangle. So, this will be given by px minus qy equal to some number, it is equation will look the same except that the constant term in the equation of the line will change. And then you can also compute the constant term because you know that this point where the x coordinate is 0, but y coordinate is 1 by 2 lies on the line.

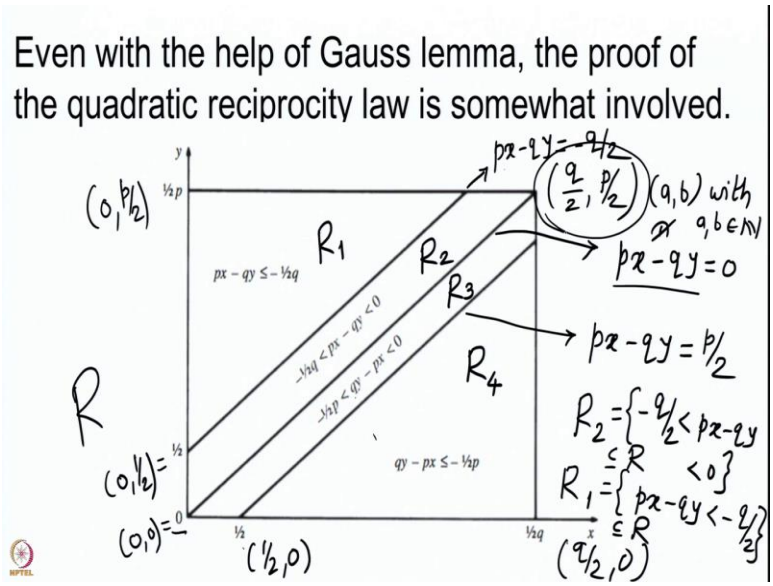
So, this is given by minus q by 2. Because your x coordinate is 0 that will tell you that px will give you 0 and minus 1 by 2 into q. So, the equation of this line is px minus qy equal to minus q by 2. Similarly you can compute the equation of this line where you know that this is the point x coordinate to be 1 by 2, y coordinate to be 0 and so the equation of this line is p by 2, with the constant term in the equation of the line is p by 2.

So, we have now various of these regions, this region is where px minus qy remember it is the same quantity that we are looking at, of as the part in the equation of these lines, which is less than or equal to minus 1 by 2 q. So you are going above this line and therefore the equation of this region now is given by px minus qy to be less equal 1 by 2 minus 1 by 2 q. So anywhere you go above this line that will be the equation. The line gives you a half plane.

So the part which is on the upper side of this line has this particular equation. The part which is on the lower side of this line given by px minus qy equal to p by 2, this part will have equation given by this, where you will have px minus qy to be bigger than or equal to p by 2. And when you multiply it by minus sign, you get qy minus px to be less equal minus p by 2. And of course here, you have that px minus qy goes from 0 to p by 2.

We have multiplied by minus 1 here to get the corresponding inequality and here we are going for px minus qy from 0 to minus q by 2. Here we are going from 0 to minus q by 2 in this direction we go from 0 to p by 2, but the inside part has negative 1 multiplied to px minus qy. These are the four regions. So I will now erase these writings and write the equations for you of these regions.

(Refer Slide Time: 18:31)



So, most important for us are R2 which is given by minus q by 2 less than px minus qy less than 0. And R1 which is px minus qy less equal minus q by 2. Of course, we are treating these as subsets of our rectangle R. So, after having decomposed our rectangle R into these four open sets remember that we are not taking the lines, but there is one thing that we should notice which is that none of these lines will contain a lattice point, now I should tell you what is a lattice point.

So, a lattice point is a point in R2 whose coordinates are integers. And what I say is that there is no point a comma b here with both a and b to be natural numbers. That is quite easy to see because p and q are taken to be primes, these are distinct primes. Whenever we talk about the Legendre symbol of p by q you should take p to be co-prime to q. So, these are primes which are distinct, they are co-prime to each other.

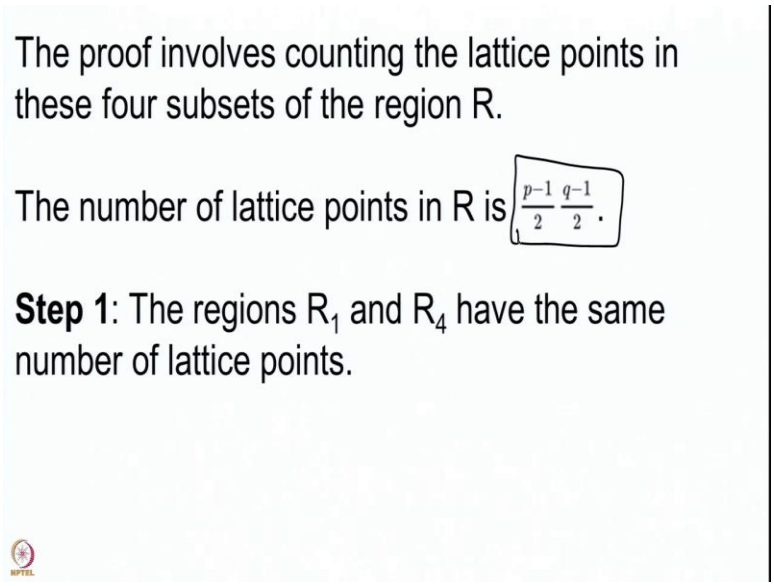
These two primes are distinct and therefore if you had any solution for px minus qy equal to 0, it would tell you that x has to be a multiple of q and y has to be a multiple of p. So, your solution, the points on this line, the diagonal line are multiples of q comma p. In fact, you also see here that this point q by 2 comma p by 2 is 1 by 2 into q comma p. So various, in fact q comma p is the vector which is going to generate this line over the real line.

So, any lattice point that you should have on this line must be an integer multiple of q by p and there is no such integer multiple of q by p in our rectangle R. Similarly I invite you to think about and to prove that the other two lines also have no lattice points. So, the lattice points, that

means the points x comma y with integer coefficients in the rectangle R are the unions of the lattice points in these four parts.

That is because although you have not taken these slanted lines the diagonal line and the two parallel lines to it. There are no lattice points. So the number of lattice points in the region R is equal to the number of lattice points in R1, plus the number of lattice points in R2, plus the number of lattice points in R3, plus the number of lattice points in R4. These, this is the very basic equality that we have here.

(Refer Slide Time: 21:58)

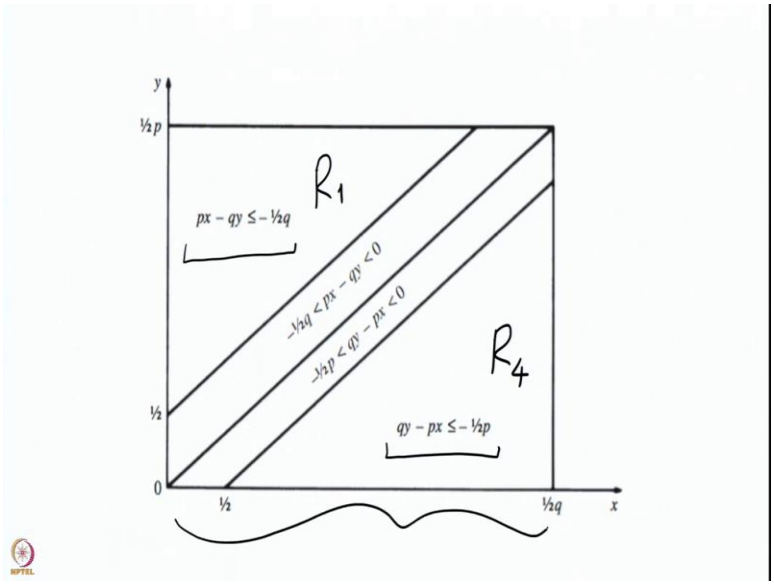


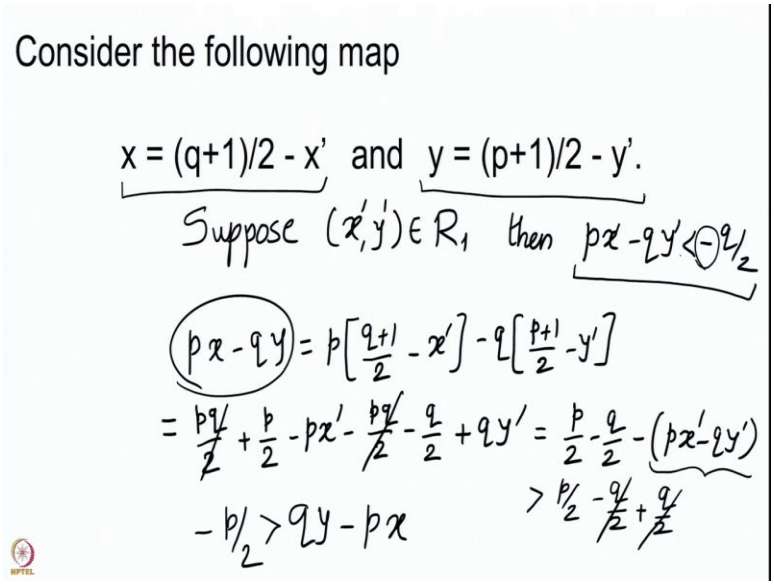
So, now we go to our first step, the proof as I told you involves counting the lattice points in these four subsets. The number of lattice points in the whole rectangle is equal to p minus 1 by 2 into q minus 1 by 2. This is the number of lattice points in the whole rectangle R that is because x is taken to be less than or equal to q by 2 and y is taken to be less than or equal to p by 2. So, what we have is that x can be less than or equal to q minus 1 by 2 because we are taking x to be an integer.

It will go from 1 up to q minus 1 by 2, y goes from 1 to p minus 1 by 2 and therefore the total number of integer points in this rectangle is p minus 1 by 2 into q minus 1 by 2. And now we come to the very first step that the regions R1 and R4 have the same number of lattice points. So, you take out the two slanted parts that we had in the middle. You ignore them. There are those two triangular parts which we had in the corners one on the left top corner and second on the

right bottom corner. These two triangular parts have the same number of lattice points. This is our first step.

(Refer Slide Time: 23:25)





Let us look at our rectangle once again, just to give you a better idea. I will also remind you that this is R1, this is R4. So we are actually going to start from lattice points satisfying this inequality to lattice points satisfying this inequality. We will, to show that the two sets have the same number of lattice points, you should just give a bijection between the two sets. So, here is a map we start with this map, x equal to q minus 1, q plus 1 by 2 upon minus x prime, and y is p

plus 1 by 2 minus y prime. What is the equation for R1, px minus qy is less than or equal to minus 1 by 2.

Suppose I have a lattice point in the region R1, then px minus qy is less than minus q by 2 and I am going to apply this map. So, suppose I start with x prime, y prime first, I apply this map and compute the x and y and now let me look at the equation px minus qy. So, we get p into q plus 1 by 2 minus x prime minus q into p plus 1 by 2 minus y prime, which gives us pq by 2 plus p by 2 minus px prime minus pq by 2 minus q by 2 plus qy prime. So, this pq by 2, pq by 2 are cancelled. What we are left with is p by 2 minus q by 2 minus px prime minus qy prime.

Here px prime minus qy prime is less than minus q by 2. Therefore this quantity in the bracket is less than minus q by 2. So when you put a minus sign to it, it will become bigger than q by 2. So, this is now bigger than p by 2 minus q by 2 and here I will have another q by 2 with a plus sign because this minus sign will be multiplied by another minus sign to give you plus sign. So these two get cancelled. Therefore what we get is px minus qy is bigger than p by 2 or in the other words when you multiply by minus 1 we get that it is be a (le) less than the minus of p by 2.

And this is the equation of our region R4, qy minus px is less than or equal to minus 1 by 2p. So, qy minus px is less than minus p by 2. Of course, we have the conditions on x and y, x is only going from 0 to q by 2, but when you subtract such an x from q plus 1 by 2, the resulting point is also going to have the same, the resulting point is also going to have the same behaviour. Similarly you have the same bound for y. So we have actually given a map from the region R1 to R4, the same map will be the inverse of this map that means you are going to apply the same map again.

If you apply this same map to regions points in R4, you are going to get points in R1. And therefore the map that we have is a bijection because it is its own inverse and starting with an integral point we get integral points. So this map gives you a bijection between the lattice points in the regions R1 and R4 and this proves that the points in R1 and R4, the number of lattice points is the same. We are short with time here. So we stop here and continue the proof in the next lecture. I will see you soon. Thank you.