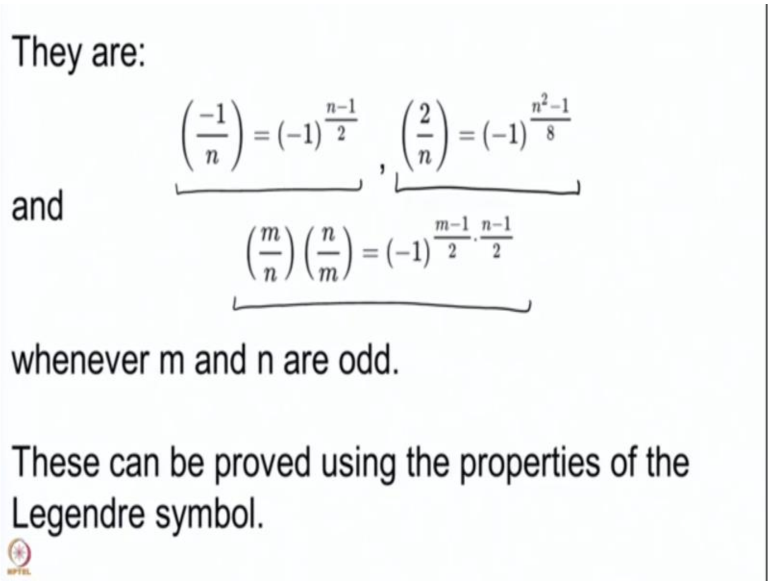
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 38
Binary Quadratic Forms

Welcome back. We are studying the Jacobi symbol, which is a generalization of the Legendre symbol. So remember that we had the notation a by n, a can be any integer, n is a natural number to begin with. And then we define this Jacobi symbol a by n by using the prime factorization of n. If n was p1 power alpha 1, p2 power alpha 2, pk power alpha k, we defined the Jacobi symbol a by n to be a by p1, the Legendre symbol power alpha 1, a by p2 power alpha 2 dot dot dot a by pk power alpha k. This was our definition of the (Legendre) Jacobi symbol and then we saw that there were several properties that the Jacobi symbol satisfied in line with the Legendre symbol. The most important of those were the quadratic reciprocity laws which are here in front of you in this slide.

(Refer Slide Time: 01:22)



They are:

$$\underbrace{\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}}, \underbrace{\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}}$$

and

$$\underbrace{\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}}$$

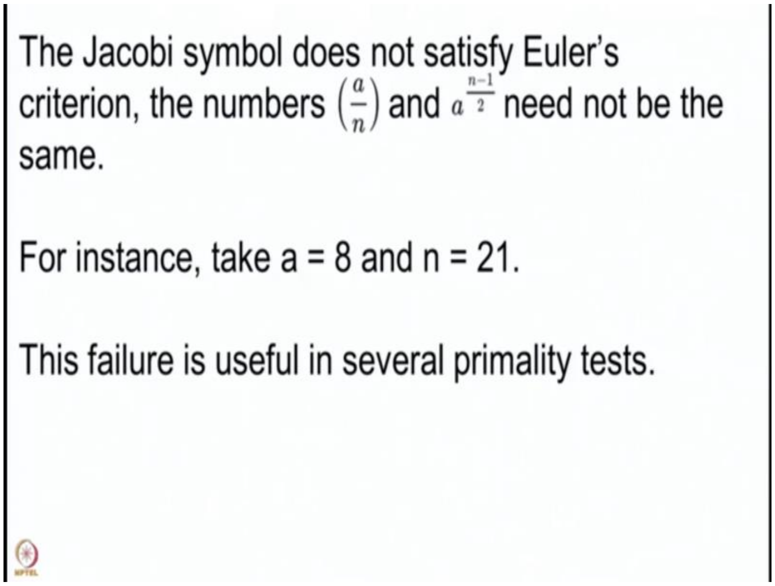
whenever m and n are odd.

These can be proved using the properties of the Legendre symbol.

So we have that minus 1 power minus 1 sub n the Jacobi symbol is equal to minus 1 to the power n minus 1 by 2. So the Jacobi symbol can be computed for minus 1 in the line with the computation for the Legendre symbol. If n is odd then 2 by n has the same formula as was in the prime modulus case in the Legendre symbol case that the Jacobi symbol 2 by n is congruent to minus 1 is equal to minus 1 to the power n square minus 1 upon 8 and finally we have that whenever m and n are odd integers, odd numbers natural numbers then m by n and n by m satisfy this generalized reciprocity law.

So these 3 properties can be proved using the similar properties for the Legendre symbol so we are not going to give their proofs. However, note that for minus 1 we have used the Euler criterion. There was the Euler criterion for the Legendre symbol which was that minus 1 sub p, minus 1 upon p was minus 1 to the power p square minus p minus 1 by 2. So that Euler criterion which was true for any integer a provided your modulus was a prime p now, need not be true for the Jacobi symbol in general.

(Refer Slide Time: 03:00)



The Jacobi symbol does not satisfy Euler's criterion, the numbers $\left(\frac{a}{n}\right)$ and $a^{\frac{n-1}{2}}$ need not be the same.

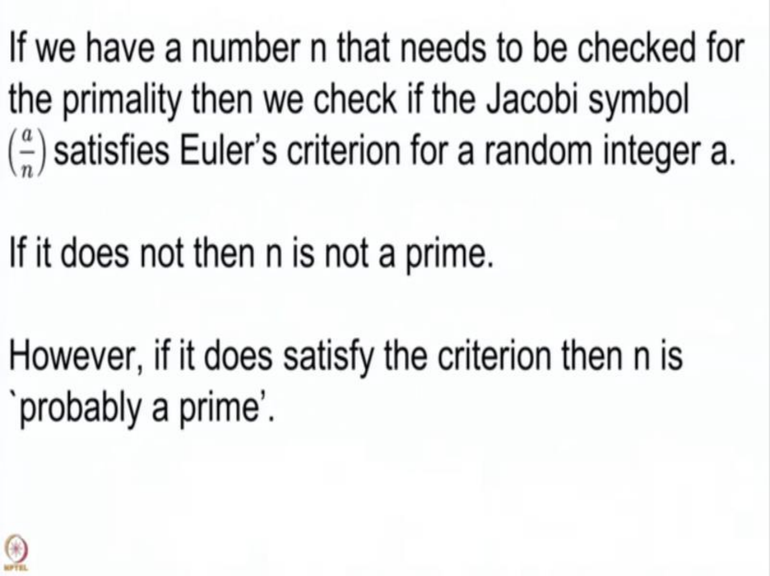
For instance, take a = 8 and n = 21.

This failure is useful in several primality tests.

So the Jacobi symbol does not satisfy Euler's criterion, which is to say that these 2 numbers, the Jacobi symbol value a upon n and the value a power n minus 1 by 2, they need not be same and they need not even be same modulo n. So, of course we see here that a by n has the value 0, 1 or minus 1, and a power something is going to be much bigger if a is positive or it will be on the negative side if a is negative. So we cannot hope these numbers to be same but these are not even same modulo the number n.

For instance, you may take a to be 8 and n to be 21, and you can check that these 2 numbers 8 by 21 and 8 power 21 minus 1 by 2 which is 8 power 10. These are not same modulo 21. So this is a failure of the Euler's criterion in general for Jacobi symbol. However, mathematicians have a knack of turning failures into very useful things. So this failure of the Euler's criterion in the case of Jacobi symbol can be used very effectively when we are doing primality tests. So this is useful in several, in fact it may be called the basis of primality tests for several of them. So, how do we go about this?

(Refer Slide Time: 04:43)



If we have a number n that needs to be checked for the primality then we check if the Jacobi symbol $\left(\frac{a}{n}\right)$ satisfies Euler's criterion for a random integer a.

If it does not then n is not a prime.

However, if it does satisfy the criterion then n is `probably a prime'.

Suppose you have a number n. It is a large number let us say and you want to know whether this is a prime number. So you want to check the primality of this natural number n. Then what you do is the following thing that we then check whether the Jacobi symbol satisfies Euler's criterion for some random integer a. So now you may ask whether we can compute the Jacobi symbol without knowing the factorization of n. Remember, we are going to test the integer n for primality.

So we do not know whether n has a factorization or not. If we already knew that n has a factorization then we would not need to check n for primality. However, we can use quadratic reciprocity laws. The analogues of the reciprocity laws to compute a by n without knowing the prime factorization of n. That is where those analogues of the reciprocity laws are useful. So you, we will compute the Jacobi symbol a by n without knowing the prime factorization of n. We will then also compute a power n minus 1 by 2. Computing powers of some certain integer is a very, is not a very difficult thing for a computer.

So what the computer does is that it can quickly compute various squares. So if you are given a, it will compute a square, it will compute the square of a square which is a power 4. It can compute a power 8, a power 16 and then whenever you want to compute any power of a you have to take product of these various squares that you have competed in a suitable order. If you wanted to compute a cube, then you have to take product of a with a square. If you want to take a power 15, then you should take product of a, a square, a power 4 and a power 8 because 8 plus 4 plus 2 plus 1 will give you 15.

So computing powers is a relatively simpler thing when you are using computers and similarly computing congruences is also a relatively simpler thing. So number 1 is that you can compute Jacobi symbol using the reciprocity laws, number 2 is that you can compute powers of a and go modulo n and then you simply check whether these 2 quantities are the same. So what we do is that we compute the Jacobi symbol and see whether the Jacobi symbol a by n satisfies Euler’s criterion for this integer a.

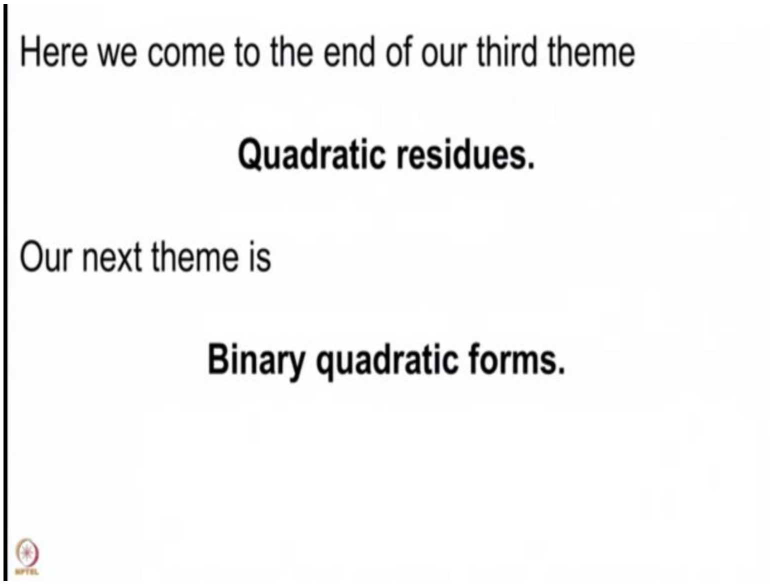
This is a randomly chosen integer a. If it does not, then n is not a prime because the prime modulus case will give you Legendre symbol and Legendre symbol does satisfy Euler's criterion. So if a by n is not congruent to a power n minus 1 by 2 modulo n, then n cannot be a prime. So this is a very nice primality test. However, unfortunately, you may happen to choose a, for which the Euler’s criterion may hold. Can we then say that n is a prime? No, but what we will then say is that n is probably a prime.

So this is where advanced things among primality tests come into the picture. So the tests will tell you how many integers you should check, for how long you should go checking meaning if you start from 1, the most natural thing is to check the Euler’s criterion for a equal to 2. If that holds then those numbers have some certain names, then you will check for n a equal to 3 and so on.

So how far do you need to go to check these criterion and this is where some probabilistic things will come into picture that when can you see that it is a prime, by what probability and so on. So these are the things which do not come into our syllabus and we will not discuss. However, I just want to add one more thing. So we started with Legendre symbol which was a by p where a was any integer and p was a prime number. Then we went to Jacobi symbol which was denoted by a by n, a is any integer and n is a natural number and there is a slight generalization of this which is called Kronecker symbol.

So there is this mathematician Kronecker in the 19th century who introduced this symbol where you allow n also to be any integer, non zero integer. If n is 0, then there is some certain value which we take by convention. So the Legendre symbol, Jacobi symbol and Kronecker symbol can be studied and there are relations of these with some character values, the Dirichlet L function and so on which we are not going to discuss in this course.

(Refer Slide Time: 10:22)



Here we come to the end of our third theme

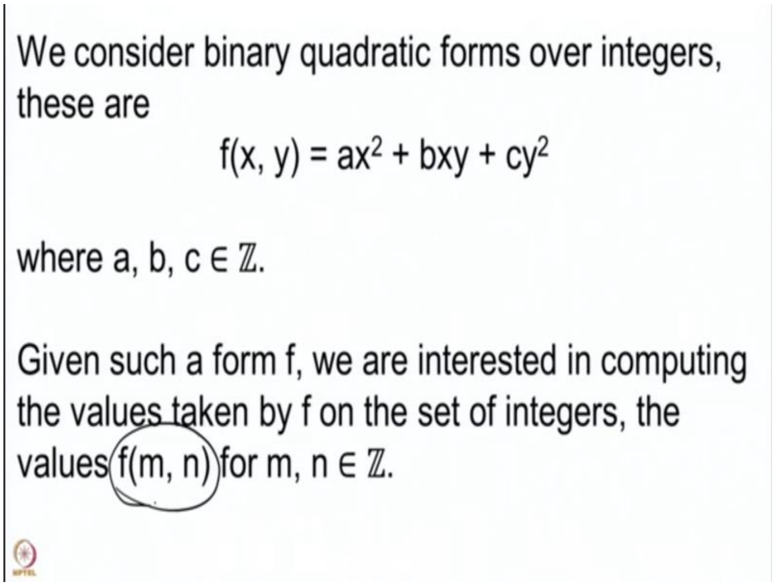
Quadratic residues.

Our next theme is

Binary quadratic forms.

So with this we come to the end of our third theme, which is broadly called the theme of quadratic residues where we determined whether a certain integer is a square modulo, a prime p or not using various other things. We were able to compute it very effectively for many primes and many integers. Then we (generalise) generalized the Legendre symbol to the Jacobi symbol and we saw one application of the Jacobi symbol in the primality tests. Our next theme is a very interesting theme. It is on binary quadratic forms. So this is a slight generalization of what we were studying in the last theme. So remember, last theme started with finding equations solutions to the quadratic equation. So these were equations in 1 variable. Now we are going to take 2 variables.

(Refer Slide Time: 11:22)



We consider binary quadratic forms over integers, these are

$$f(x, y) = ax^2 + bxy + cy^2$$

where a, b, c $\in \mathbb{Z}$.

Given such a form f, we are interested in computing the values taken by f on the set of integers, the values $f(m, n)$ for m, n $\in \mathbb{Z}$.

So, we consider binary quadratic forms over integers which means that we are going to take these expressions. So here we have so let us start noting various things. We have 2 variables now, x and y and this is why we call them binary. So the (nome) name binary comes because we have 2 variables, namely x and y. Quadratic comes because the degree of the polynomial here is 2 and form comes because the polynomial is a homogeneous polynomial. And where do integers come, integers are there because the coefficients of this polynomial are taken from integers.

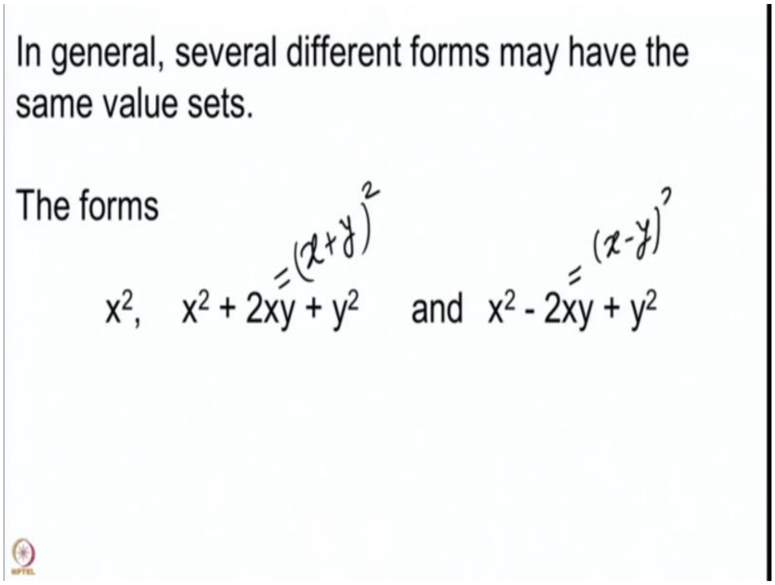
So these things therefore as you would expect are true in more generality, you can take forms not necessarily quadratic, but you can take cubic forms, quadratic forms, quantic forms and so on. You may take binary forms, ternary forms, quaternary forms and higher number of variables in the forms and you may take them over not necessarily over the set of integers. You may take them over a general sets. What we are then going to do is to evaluate these forms.

So here since we have taken a, b, c to be integers, we will be easily able to put values for x and y from the set of integers and compute the value. So when you take a, b, c from a general set, a set general than integers, we expect that the set b such that you can take products over the set, you can take additions over the set and so on. So this is the structure what is called a ring. We have earlier studied the structure called a group and we saw some applications of that. Here we will not use but let me just tell you that you can take forms, the generalized versions of these forms over rings.

So here we are going to take them over the ring of integers. So we have this set z of integers, which is a ring and over these ring of integers we are going to take binary quadratic forms. We are not going to take higher order forms. We are not going to take forms in higher number of variables. This, these are enough for us. These are going to give us lot of interesting properties. So at the moment these are quite good for us. So, these are the forms that we are going to study and given any such form f, the thing that we would like to compute is the set of values taken by this form f. So given any such form what we are interested in computing is the set of values f m comma n where m comma n are integers.

So these are the numbers that we want to compute. So not one number. that would be a very easy thing if I want to just compute f of 0, 0 that would give me 0, it is a homogeneous form. If I want to compute f of 1, 1 that would simply be, a plus b plus c. So those are easier things but I would like to compute the set of values where m and n are taken to be all integers. This is the set that I would like to compute. Now, it is quite possible that you may have 2 different looking forms and the set of values given by them may turn out to be the same sets.

(Refer Slide Time: 15:32)



In general, several different forms may have the same value sets.

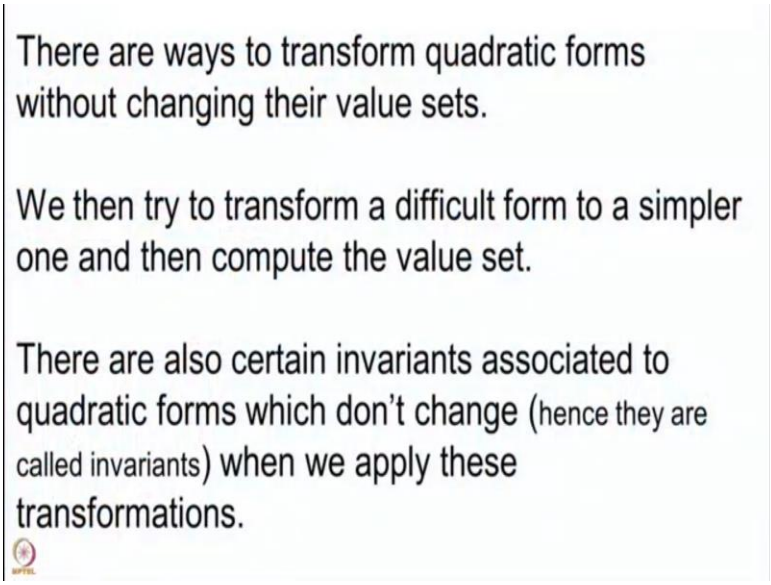
The forms

$$x^2, \quad \overset{=(x+y)^2}{x^2 + 2xy + y^2} \quad \text{and} \quad \overset{=(x-y)^2}{x^2 - 2xy + y^2}$$

So, this can actually happen many times. It happens quite often. So, there might be several different forms, which may have the same value sets and an example can be readily given. You may take these forms. So these are 3 forms. The first form is f of x comma y equal to x square. There is no x y term, there is no y square term. So the coefficients b and c are both 0, but we have the form to be x square. So you are going to get all squares. Whenever you put value for x, any integer in the place of x, you are going to get the square of that integer.

So all squares are represented and the whole set of values is the set of squares. Similarly, the second form that you see here is nothing but x plus y whole square. So once again, whatever value of x and y you choose, the value of the form is a square and you can put y equal to 0 and x to be any integer and all squares are represented. So, the value set is the same as the set of squares. Similarly, this is x minus y whole square. So it is the same computation. So, these are 3 different forms and even then we have that their value sets are the same.

(Refer Slide Time: 17:15)



There are ways to transform quadratic forms without changing their value sets.

We then try to transform a difficult form to a simpler one and then compute the value set.

There are also certain invariants associated to quadratic forms which don't change (hence they are called invariants) when we apply these transformations.

So what we would like to do is to put some kind of equivalence relation on the set of binary quadratic form. So I will not keep mentioning the word binary or sometimes I will even forget to use the word quadratic but we should remember that we are always going to look at binary quadratic forms over integer. So we are going to look at homogeneous polynomials of degree 2 in 2 variables with coefficients coming from the set of integers. So we are looking at these forms, and we would like to say that in some way one form is equivalent to another form.

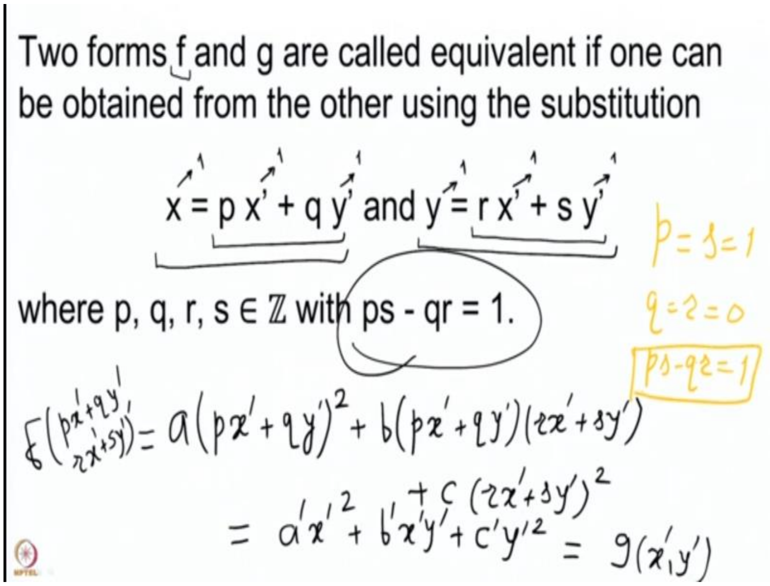
So, we will try to put some relation between these calling some of 2 of them to be related to each other or if you have all the properties, then the form, then the relation will be an equivalence relation. So one form will be equivalent to another form and we would also try to have this transformation, the relation so that the value sets turn out to be the same. So, what we will then do is that whenever we want to compute the value set of a given quadratic form, the given binary quadratic form, which may look difficult because a b and c might be big numbers, they might come from different signs and so it may happen that computing values by hand might be very different, very difficult.

So we would then transform it to a simpler looking form and once you transform it to a simpler looking form, then we may be able to compute the value set more easily and if you also have that this transformation keeps the same value sets, then you would have computed the value set of your earlier form. This is what we are going to do. We will also have some certain invariants associated to these quadratic forms. So what do you mean by invariant?

By invariant we mean that when you apply the transformations mentioned in the previous lines, these are the quantities which do not change. So these invariants which do not change and hence they are called invariants when we apply these transformations. So these are the things that we hope to do. Number one is that, we will say that one form is equivalent to another form or one form is obtained from another form by some way. So we will give these transformations.

We will go, we will give a method to go from one quadratic form to another quadratic form without changing the value set and there, we would also like to have this way to be invertible because I do not want, always know that I am going to go from a difficult form to a simpler form by this way. It may happen that you start with a simpler form, apply the transformation and you may get a difficult form. So the transformation should not be only one way. It should be both ways. It should be an invertible transformation. So we will see that there is a way to define this transformation. We will see that there is a relation that you can put on the set of binary quadratic forms which will also help you compute the value sets.

(Refer Slide Time: 20:46)



Two forms f and g are called equivalent if one can be obtained from the other using the substitution

$$\underbrace{\overset{1}{x} = \underbrace{p\,\overset{1}{x'} + q\,\overset{1}{y'}}}\ \text{and}\ \underbrace{\overset{1}{y} = \underbrace{r\,\overset{1}{x'} + s\,\overset{1}{y'}}}$$

where p, q, r, s ∈ ℤ with $\bigcirc\!\!\!\!\;ps - qr = 1$.

$p = s = 1$

$q = r = 0$

$\boxed{ps - qr = 1}$

$$f\left(\begin{smallmatrix} px' + qy', \\ rx' + sy' \end{smallmatrix}\right) = a(px' + qy')^2 + b(px' + qy')(rx' + sy') + c(rx' + sy')^2$$

$$= a'x'^2 + b'x'y' + c'y'^2 = g(x', y')$$

So this is what we are going to do. So here comes the definition. Let us start with 2 forms, 2 binary quadratic forms. So you have the form f and you have the form g. So suppose your form f is given by a, b, c and g is given by a prime, b prime and c prime. So we say that these 2 forms are equivalent if one of these can be obtained from the other using the substitution x equal to p x prime plus q y prime and y equal to r x prime plus s y prime. Here we have that these p, q, r, s they are integers but this is a very important condition that p s minus q r has to be one. So you may have your form f which is given in terms of x and y.

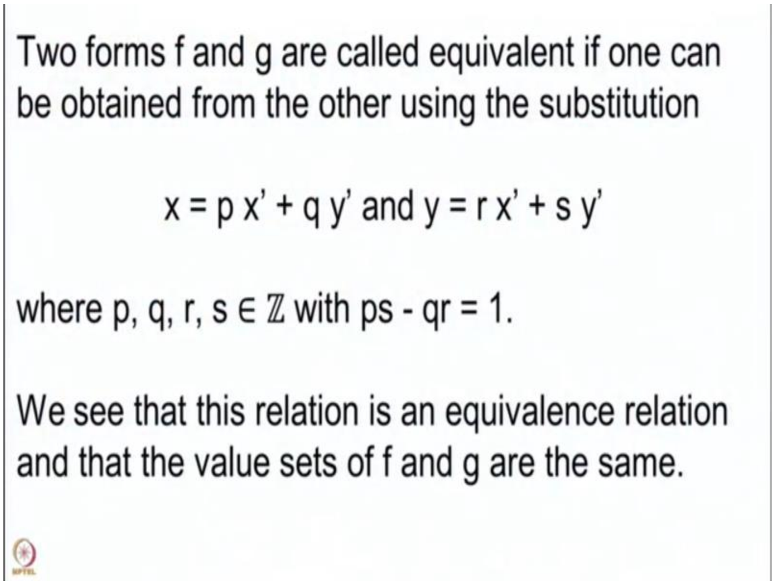
So you have f equal to a x square plus b x y plus c y square. Now, if you put instead of x, the value p x prime plus q y prime and instead of y, the value r x prime plus s y prime then you are going to get some expression in x prime and y prime which will remain to be homogeneous of degree 2 because our substitution is homogeneous of degree 1. Here we had degree of x to be 1, degree of x prime to be 1 and degree of y prime to be 1. So we are considering x prime and y prime to be new variables and we are writing x and y in terms of these new variables and the substitution is homogeneous of degree 1.

Therefore the ultimate expression that f will change to will continue to be homogeneous. It will continue to be of degree 2 because there is no change of degree. So you will get a different expression. So you started with a x square plus b x y plus c y square and when we had x, you would put a p x prime plus q y prime whole square plus b p x prime plus q y prime, r x prime plus s y prime plus c r x prime plus s y prime whole square. So this will be some a prime x prime square plus b prime x prime y prime plus c prime y prime square. This is our form g.

So when you started with f and instead of x and y, we put these substitutions in terms of x prime and y prime. If we get the form g in x prime and y prime, then we say that f and g are equivalent. Now notice that in this definition we did not say that you have to obtain g from f or that you have to obtain f from g. It can be that one is obtained from the other. So it is clearly this relation of f and g is clearly a reflexive relation. Whenever f is equivalent to g, g is equivalent to f. This is by definition. Further you will see that the form f is equivalent to itself because you can take p to be 1, q to be 0, r to be 0 and s to be 1.

So if you take p equal to s equal to 1, q equal to r equal to 0, you are going to get ps minus qr to be 1 and you are going to get same thing. You are going to get x equal to x prime, y equal to y prime. So the form f is equivalent to itself. The form f is equivalent to g. Then g is equivalent to f. That is a slightly non-trivial thing. We will see that in a moment, but more importantly whenever f is equivalent to g and suppose g is equivalent to a third form h, then f is equivalent to h. So all these 3 properties are put together in a box and we call them an equivalence relation.

(Refer Slide Time: 25:45)



Two forms f and g are called equivalent if one can be obtained from the other using the substitution

$$x = p x' + q y' \text{ and } y = r x' + s y'$$

where p, q, r, s $\in \mathbb{Z}$ with $ps - qr = 1$.

We see that this relation is an equivalence relation and that the value sets of f and g are the same.

So we see that this relation is an equivalence relation. That means the relation satisfies reflexivity, symmetry and transitivity. So this is of course an equivalence relation and further the value sets of f and g remain the same. So we will see this in our next lecture, which we will continue on the same theme. So, I hope to see you in that lecture also. Thank you.