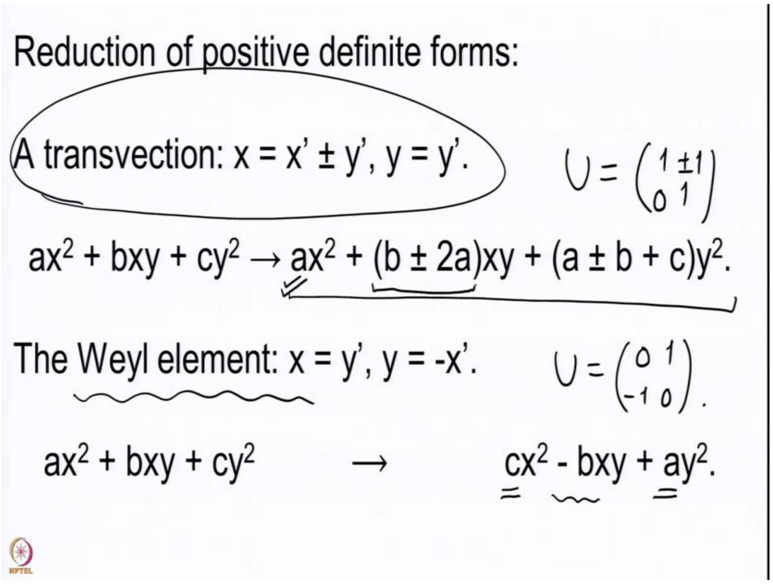
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 42
Reduced forms up to equivalence – I

Welcome back, we are studying positive definite forms and let me reiterate, our motivation is to study forms like x square plus y square and we want to understand all the numbers represented by this form that is we want to understand the whole value set of such forms. So, one way to do that, as we saw in the last lecture was to reduce this form a given positive definite form to a somewhat simpler form and therefore, we define this concept of a reduced form and then we also proved in the last lecture that every positive definite form is equivalent to a reduced form.

(Refer Slide Time: 01:09)

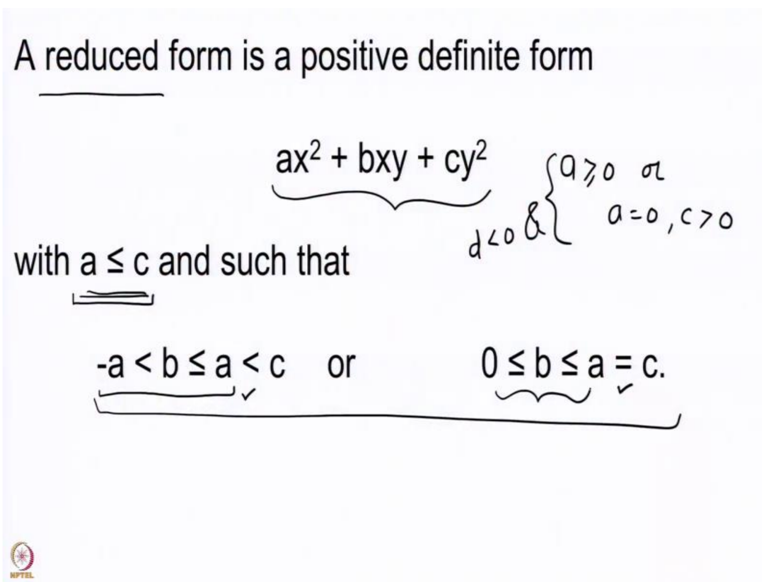


So, before we go to the main proof, let me just quickly recall these things for you that we have introduced these very important transformations. The first one is called a transvection. So, this is represented by the matrix whose diagonal entries are one upper tri diagonal entry can be plus or minus 1 and the lower diagonal entry is 0 and this element, this is the weyl element, this is represented by the matrix 0 1 minus 1 0. So, transvection because these are transvection is a very general term, if you study matrix groups and what is called geometric algebra, then you will see that these transvections are omnipresent there they come there in almost every search matrix group and they are very useful.

Weyl element is something which generates what is called the weyl group of the matrix group SL two. And therefore, I am using these notations to denote these two transformations. So, we have the transvection and we have the weyl element remember that weyl element is going to switch x and y, so, with a sign, so, that means that the coefficients a and c will be switched, but the coefficient b has a different sign.

So, when we have ax square plus bxy plus cy square, then we see that a goes to the place of c and c goes to the place of a, the only change is that b has a different sign. So, while the places of a and c are switched, the change in b is the change of a sign. The transformation given by the transvection has this description here, what is important to note is that a remains as it is and b can be made smaller or bigger by multiples of two a. So, this is the change that is happening for b and there is some change which is happening for c but that is something that we can take care of, okay.

(Refer Slide Time: 03:39)

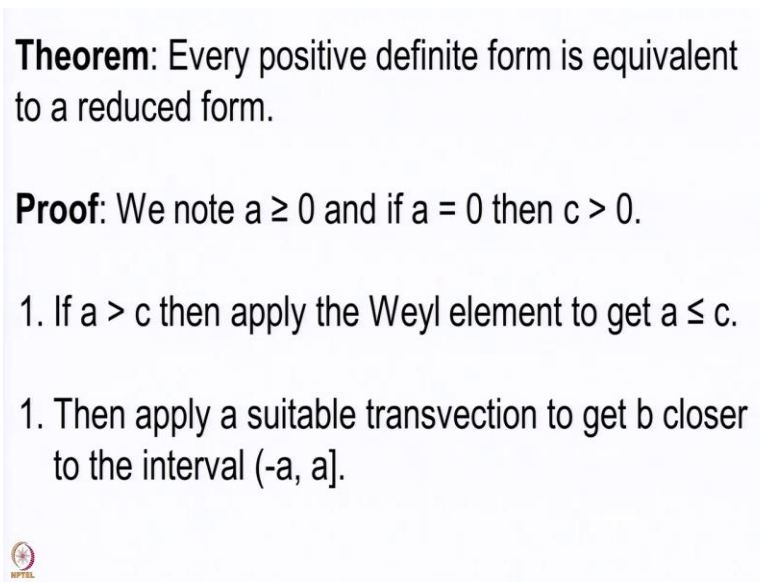


So, once we are done with this, we now go to the definition of what is a reduced form. This is slightly differently worded than the definition I gave in the last lecture. So, the only change is that we start with this binary form, which is positive definite and I say that you have first of all a to b less than or equal to c, which was evident in the conditions that we had later. But let me put it first. So, we have a positive definite form that means the a is positive or whenever a is 0, c is strictly positive. This is what we have and of course, that the discriminant is negative.

So, these are the two conditions which we have for the positive definiteness. So, we have these conditions, then for the form to be reduced, a has to be less than or equal to c and in that case, depending on whether a is equal to c or a is strictly less than c, we have the behavior of b, which is controlled by a.

If a is strictly less than c we allow b to go from minus a to a we allow it to be equal to a but not to minus a and if a and c are equal then we say that b has to be positive number non negative number it can be from 0 to a. So, this is the definition of a reduced binary form, which is by definition a positive definite quadratic form.

(Refer Slide Time: 05:35)



Now, we come to the theorem, which we proved in the last lecture that every positive definite form, every positive definite form is equivalent to a reduced form. So, you start with any positive definite form whatever coefficients it may have, you can always change it by using the allowed transformations, so, that in the end you get a reduced form and the proof was quite easy what we are going to do is that to show that any positive definite form is equivalent to a reduced form, we will have, we will start with a general positive definite form and show that there are transformations that can be applied to it, so, that the result is a reduced form.

So, we are only going to apply the transvection and the weyl element, these are the only two transformations that we are going to apply to our form and keep modifying the form suitably so, that after a finite stage we get a reduced form that is this simple idea of the proof let me give it to you once again.

We note once again that because the form is positive, the a has to be bigger than or equal to 0, a cannot be negative. Remember, the constants a and c are always represented by the form, if you have the form f of xy equal to ax square plus bxy plus cy square, you put x equal to 1 and y equal to 0, f of 1 comma 0 is a and F of 0 comma 1 is c.

So, a has to be bigger than or equal to 0 because the form is positive definite that means, the values are taken are either 0 or positive and if a happens to be 0, c which earlier was also bigger equals 0 now has to be strictly positive, because if a is 0, c is 0 your form simply becomes bxy, which is a indefinite form it cannot be positive definite. So, these are the two basic assumptions, these are the two basic observations that we make that a has to be bigger equals 0 and in the case when a is 0 c has to be bigger than 0, okay.

Now, we try to arrange so, that a becomes less than or equal to c, the problem may be that a may be bigger than c. So, if you are a is bigger than c, these are both non negative numbers, if a is bigger than c, then we apply the weyl element which will change b to minus b, but it will give you that now a is less than or equal to c, it will not be equal because we have a to b strictly bigger than c. So, a is less than c. Of course, what I have written is also true.

So, we apply the weyl element to switch the places of a and c, so that the new a the new coefficient of x square the new a is now less than or equal to the new c. So, the conditions on a and c are now satisfied, we now look at b your b might be a very wild integer, it may not be in the range that is prescribed.

So, what we do is that we apply a suitable transvection to get b closer to the interval minus a a. I have put here the sign for minus a as a round bracket and for the right hand side the closing bracket is taken to be a square bracket. So, the round bracket signifies that we are not taking minus a it is an open interval and the closed bracket signifies that that is a closed interval.

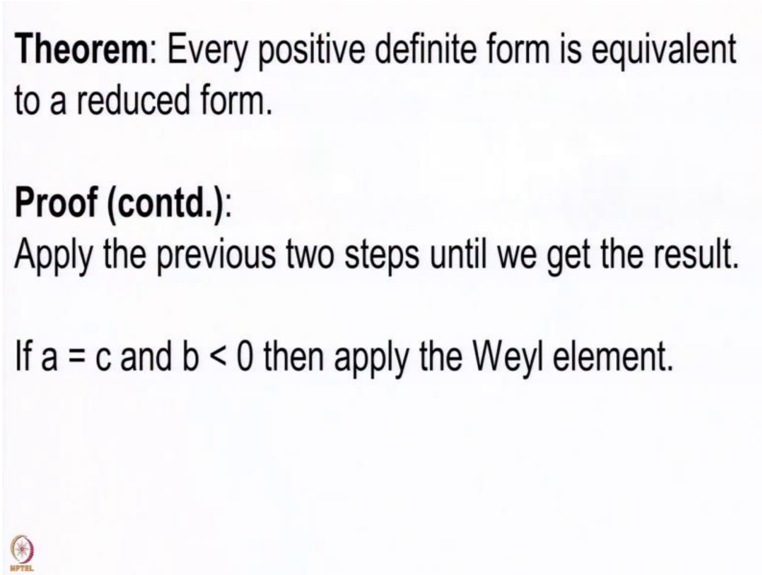
So, we are allowing a but we are not allowing minus a so we will actually start with minus of a minus 1 or minus a plus 1 towards a so these are all the integers that are allowed. So, wherever you have b remember you can apply transvections and b can be changed to b plus or minus 2 a so if b is positive and very large, you keep subtracting multiples of minus 2, keep subtracting multiples of 2 a to bring b less than or equal to a do not go to minus 2 a minus a or do not go beyond that stop when you have it within this interval, if you have it to be equal to minus a, you can add 2 a and bring it to a and while we are applying the transvections, the a, the coefficient of x square does not change, that is the most important thing.

So, we will still have the same a, the b coefficient has now come in the prescribed interval, what may happen is that the c might change, we had initially applied to the weyl element and we got that a is less than or equal to c, but by applying the transvection once c becomes a minus b plus c, so the c might become smaller than the a now.

Let me repeat we had a bigger equals bigger than c possibly. So, we applied the weyl element and made a smaller than or equal to c. So, a is a positive quantity which is now smaller, the coefficient of x square is now smaller than the coefficient of y square. Now, after applying the transvection, we are adjusting the coefficient of x y, but the coefficient of y square might become smaller further than the coefficient of x square and so, we may have a still smaller coefficient for y square, we apply once again, the weyl element to make the a and c to change places, b will acquire one a different sign but that is okay the interval does not change. And so, a is now further less than or equal to c, if your b was a you apply the transvection once again to get it within the range.

So, what is happening is that the coefficient of x square remains positive and by all these processes, we are either keeping it as it is or we are decreasing it. So, this process has to ultimately stop. So, ultimately, what we are going to get is that we will have a reduced form, which will have the property that first of all a the coefficient of x square is less than or equal to the coefficient of y square and further, the coefficient of x y satisfies the correct property.

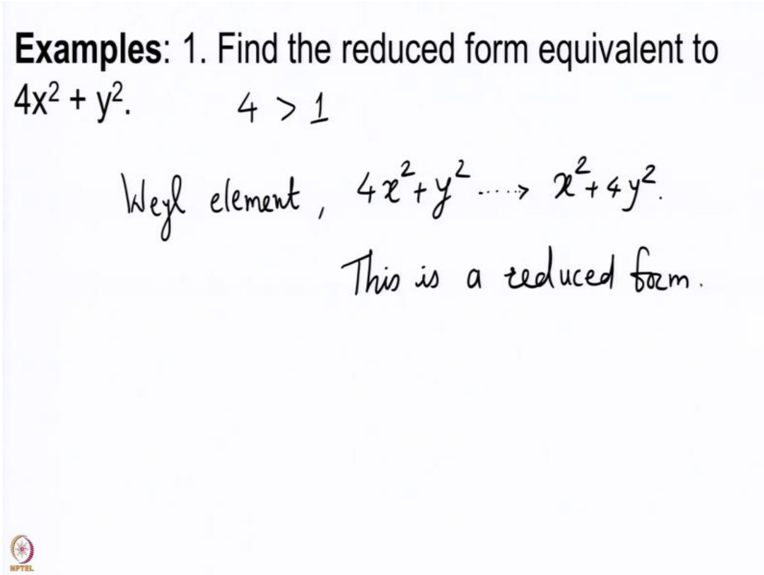
(Refer Slide Time: 12:35)



There is of course, this condition that whenever you have a equal to c, we want b to be positive. Now, if your a is equal to c and applying the transvection, and so on, you have got b to the negative, then you simply apply the weyl element once again, which is going to switch the coefficients of x square and y square, which are the same because you have a equal to c. So, those coefficients numerically, they do not change, but b changes its sign.

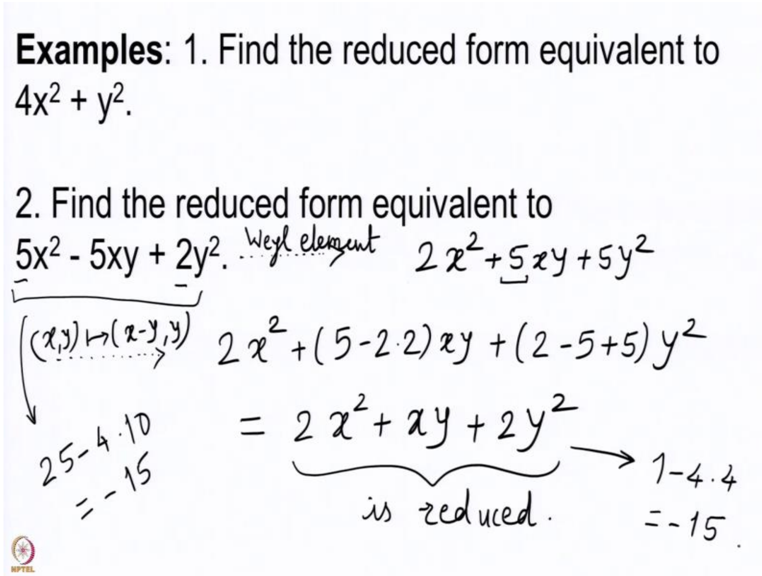
So earlier, the b which was negative has now become positive. So, by applying the weyl element in the end, if necessary, if a is equal to c, we have that b can also be made to be bigger than or equal to 0 and thus, every positive definite form is equivalent to a reduced form. So, to understand every theorem, it is good to work out some examples. So, let us go and let us do one or two examples and understand this theorem in proper way.

(Refer Slide Time: 13:40)



This is the first example, we are given the form 4 x square plus y square and we want to find the reduced form which is equivalent to this. So, we notice here that 4 is bigger than 1 the coefficient of x square is bigger than the coefficient of y square and therefore, we have to apply the weyl element first. So, we apply the weyl element which will then make 4 x square plus y square transforms to x square plus 4 y square here we do not have the b term there is no coefficient for x y the x y term is not there. So, that or in other words, the x y term is 0 and so it sign changes and it really still remains 0. This is a reduced form. So, 4x square plus y square is equivalent to the reduced form x square plus 4 y square.

(Refer Slide Time: 15:00)



Next example is slightly more complicated 5x square minus 5xy plus 2y square. So, even here 5 is bigger than 2. So, we apply the weyl element first to get it 2 x square the sign of b will change plus 5xy plus 5y square. So, we obtained a form where now the coefficient of x square which is 2 is less than the coefficient of y square which is 5.

Now, I apply the transvection which sends x comma y to x minus y comma y because I need to 5 is big the coefficient of x y is big, I want to bring it to the interval minus 2 minus 1 to 2. So, the new coefficient of xy is allowed to have values minus 1 0 1 and 2, these are the only quantities that we allow for the coefficient of xy to take.

So, I subtract y therefore, the effect will be that twice of 2 will be subtracted from 5 the coefficient of x square remains as it is here we get it to be 2 into 2 here we get this to be a which is here we get it to be a minus b plus c and which is then equal to 2x square plus xy plus 2y square. So, we have that the coefficient a of x square is 2 the coefficient of y square is 2 and the coefficient of xy which is 1 is bigger than 0 and is less than a. So, this is now a reduced form.

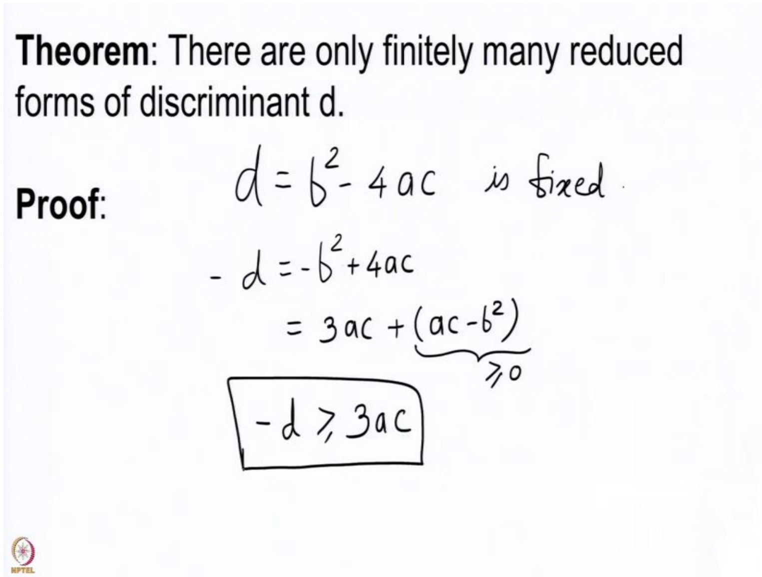
There is a small check which we can do to see whether we have not made any mistake in this calculation, which is that we can compute the discriminant of the original form and we can compute the discriminant of the form that we have obtained. So, the discriminant here is given by b square minus 4 ac. So, the discriminant here is b square which is 25 minus 4 into 5 into 2 so, that is 10 so, 25 minus 40 that will give you minus 15 and the discriminant here is b square which is 1 minus 4 a c, a c is also 4. So, you get 1 minus 16 which is also minus 15. So, it is likely that our calculations are correct and thus, we have computed two reduced forms for the two positive definite forms that we started with this is how one would do the calculation.

Now, there is one important thing, the important thing is the following that if one person starts transforming the given positive definite form to obtain a reduced form, that person may not use the method that we have used. So, the somebody else you know, I should perhaps tell you that this is all coming from Gauss, Gauss is the one who has studied the whole theory of reduction of binary quadratic forms. So, this is a very old study.

But recently a brilliant mathematician by name Don Zagier, he gave one more algorithm to obtain reduced form equivalent to a given positive definite form. We have one algorithm which is given described by Gauss using transvections and weyl element and there is this another algorithm given by Don Zagier and it is quite likely that the reduced form that Zagier obtains might be completely different from the form we have obtained.

So, then question that we should first of all ask is, how many forms can there be, if I give you one discriminant, the discriminant is not going to change when we have transformations. If I give you one discriminant can there be infinitely many forms with the given discriminant? Can there be infinitely many reduced forms of that discriminant and among the reduced forms of a given discriminant, how many of them can be in equivalent to each other?

(Refer Slide Time: 20:34)



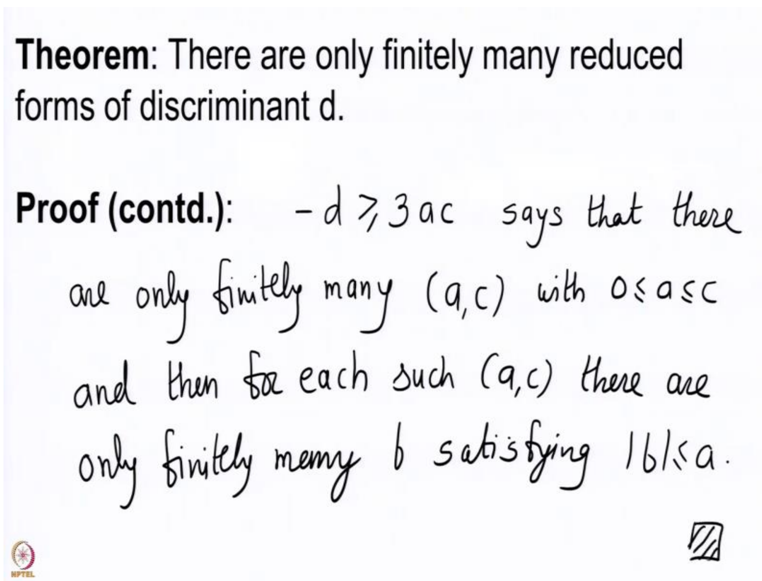
Perhaps, if any two equivalent reduced forms are same, then it would tell you that whether we apply Gauss method or Zagier's method, both of us we will reach the same answer. So, we will answer this question one by one we first want to see how many reduced forms can there be of a fixed discriminant. The theorem says that if you fix a discriminant d, then there are only finitely many reduced forms of that discriminant.

So, assuming that you may have two distinct reduced forms to be equivalent, it is likely that Gauss will give you one reduced form, Zagier will give you perhaps another reduced forms, but answers cannot be infinitely many different answers, the answers will be from a finite set, we will later see that the both the answers will have to be one and the same. But let us first show that reduce forms of a given discriminant is a finite set that is a very interesting proof and rather a simple proof.

So, what we have is d which is b square minus 4 a c is fixed. Now, we write it as. So, we have of course, minus b minus d which is minus b square plus 4 a c and here if I take 3 a c out then we have a minus b which is now a positive quantity we are starting with positive definite forms. So, d is negative minus d is positive minus d is 3ac plus ac minus b square this quantity is bigger than or equal to 0, b is not allowed to be bigger than a even the mod b is not allowed to be bigger than a, b is between minus a and a and a is less than or equal to c. So, a c always is going to be bigger than or equal to b square.

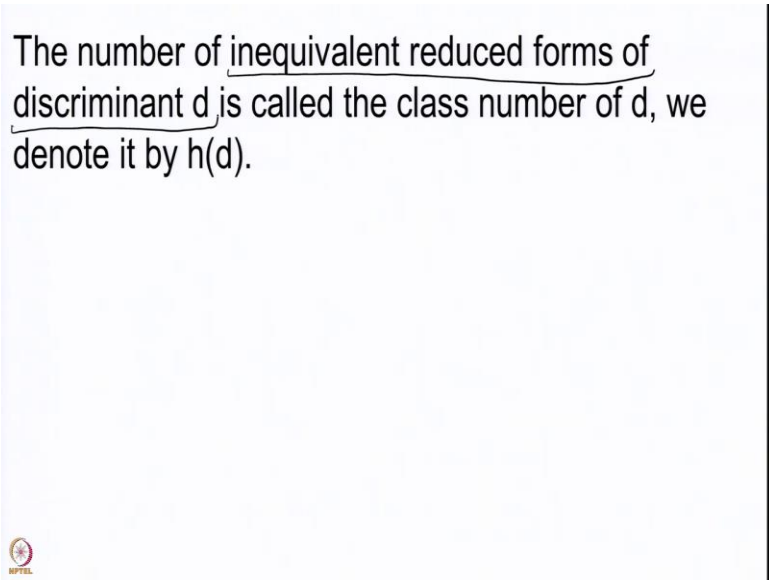
So, this quantity is bigger equals 0 and therefore, what we get is that minus d is bigger than or equal to 3 a c minus d is a fixed positive integer, the multiples of 3 the multiples which are positive, remember a and c are both bigger than or equal to 0. So, the possibilities for a and c are finitely many, because the multiple 3 a c is bounded above by minus d. So, we have that there are only finitely many choices for a and c even among them you will have to have that a is less than or equal to c. So, ultimately you have finitely many choices of the coefficients for x square and y square of reduced forms of discriminant d and further the choices of b are finitely many for a given a that will tell you that ultimately there are only finitely many reduced forms of discriminant d.

(Refer Slide Time: 24:11)



Let me write it down precisely, minus d bigger equal 3 a c says that there are only finitely many a comma c with 0 less equal a less equal c and then for each such a c there are only finitely many b satisfying mod b less than or equal to a. So, in the end we have only finitely many positive definite forms in fact, reduced forms of a given discriminant d, what we have used is that minus of the discriminant is always going to be an upper bound for 3 a c and once you have finitely many a c, then for each a, there are finitely limit choices for b. So, ultimately the pair's a comma b comma c satisfying the inequalities for the reduced forms are only finitely many the triples are only finitely many and therefore, there can only be finitely many reduced forms of a given discriminant d.

(Refer Slide Time: 26:11)



So, whenever we have a fixed number d, a discriminant d and we compute the number of inequivalent reduced forms of discriminant d, this number is called the class number of d. So, remember d is a negative number and we are looking at all reduced forms. So, all these reduced forms are now only finitely many and in principle, we should be able to tell how many of these are equivalent to each other.

In fact, we will prove that the equivalence is a redundant condition any to reduce forms are never equivalent, but that we will see later, right now, what we see is that if you are given a discriminant d, look at the reduced forms of that discriminant, look at the inequivalent ones among them, that number is called the class number of your given discriminant d and we will denote it by h of d.

In the next lecture, we will see that the number of reduced forms which are equivalent to each other it just one which means that any two forms which are reduced and equivalent will have to be the same forms. So, see you until then thank you very much.