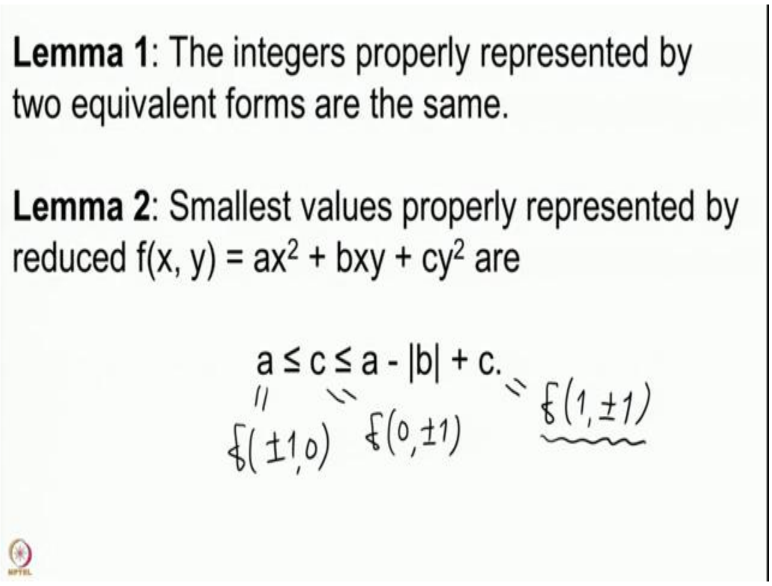
A Basic Course In Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture-44
Produced forms up to Equivalence - III

Welcome back, we are in the process of proving that whenever we have two reduced forms, which are equivalent, then they have to be the same. This is a long proof and while proving this we needed to acquire some intermediate statements, we had recorded them as lemmas in the previous lecture. So, let me recall those two lemmas for you and then we will go to prove this important theorem.

(Refer Slide Time: 0:49)



Lemma 1: The integers properly represented by two equivalent forms are the same.

Lemma 2: Smallest values properly represented by reduced $f(x, y) = ax^2 + bxy + cy^2$ are

$$\underset{f(\pm 1,0)}{\overset{}{a}} \le \underset{f(0,\pm 1)}{c} \le \underset{\underset{\sim\sim\sim}{f(1,\pm 1)}}{a - |b| + c}.$$

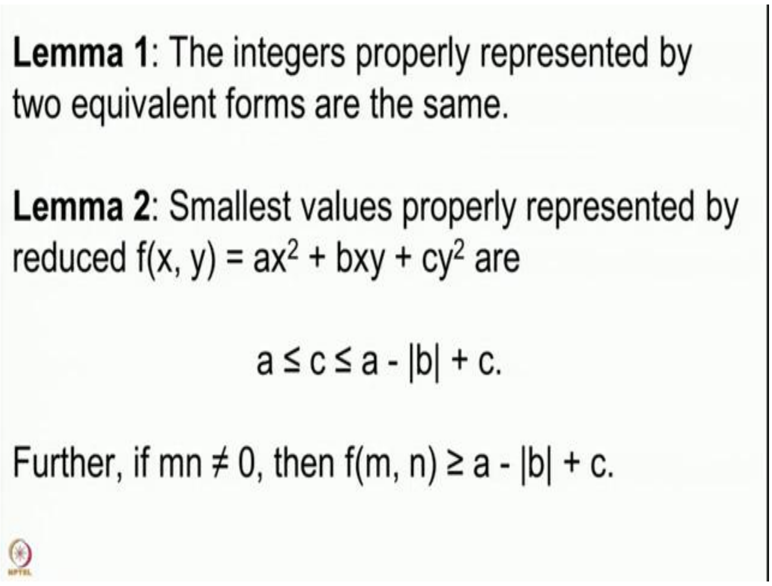
This is the first lemma that two integers the, this is the first lemma that the integers properly represented by two equivalent forms are the same. So, if you have two equivalent binary quadratic forms say f and f prime and some integer is represented properly by one of them, then it has to be represented properly by the other also represented properly means, first of all some integer being represented by a binary form means that there is a pair m comma n such that f of m comma n is that integer.

And when we say that this integer is properly represented by the form f, we need that the integers m and n be co prime, their GcD be equal to 1. We saw in the last lecture that the change of variables that we allow, takes co prime pairs of integers to co prime pairs and therefore, the proper represented set, the set of integers properly represented by equivalent forms will be the same. The second statement that we had was the following. This is also very important, here we start with our form being a reduced form.

remember, reduced form means that a is less than or equal to c and further b is between minus a and e. So, in some sense this is the simplest one among the equivalence class of the forms of f. So, if you take all binary forms equivalent to a reduced form, f will be the simplest in some sense, because its coefficients are the smallest possible. So, this is a reduced form and then we say that the integers which are represented properly, the smallest three among them are listed in front of you in the slides.

So, you have a equal less than or equal to c, which is less than or equal to a minus mod b plus c. Here we see that our integer a has the value which is attained at plus minus 1 comma 0, c is attained at 0 comma plus minus 1 and this is attained at f of plus or minus 1, 1 comma plus minus 1. So here is the sign for the last 1, this 1 will depend on whether b is positive or not. and, actually, we had proven a stronger statement, where we proved that if you take m comma n, such that both are not 0, that means, the product is not 0, then the value f of m n is at least the last of these three.

(Refer Slide Time: 3:56)



Lemma 1: The integers properly represented by two equivalent forms are the same.

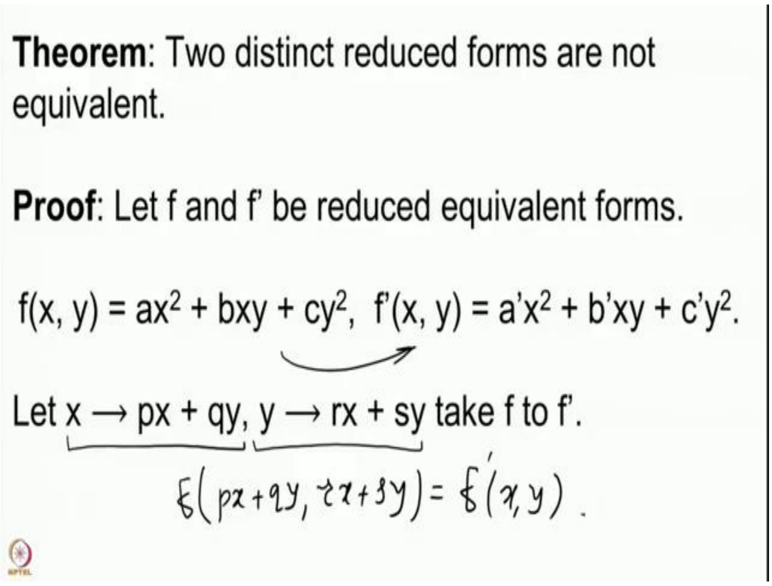
Lemma 2: Smallest values properly represented by reduced $f(x, y) = ax^2 + bxy + cy^2$ are

$$a \leq c \leq a - |b| + c.$$

Further, if $mn \neq 0$, then $f(m, n) \geq a - |b| + c$.

Which means that if you further have that m comma n, m into n is not a 0 integer which means that none of them is a 0 integer, then f m comma n is at least a minus mod b plus c. So these are the two lemmas, we are armed with these two lemmas and now we are going to prove the main theorem that we want to prove in this lecture, which is that two distinct reduced forms are not equivalent.

(Refer Slide Time: 4:27)



Theorem: Two distinct reduced forms are not equivalent.

Proof: Let f and f' be reduced equivalent forms.

$f(x, y) = ax^2 + bxy + cy^2$, $f'(x, y) = a'x^2 + b'xy + c'y^2$.

Let $\underbrace{x \to px + qy}$, $\underbrace{y \to rx + sy}$ take f to f'.

$$f(px+qy, rx+sy) = f'(x,y).$$

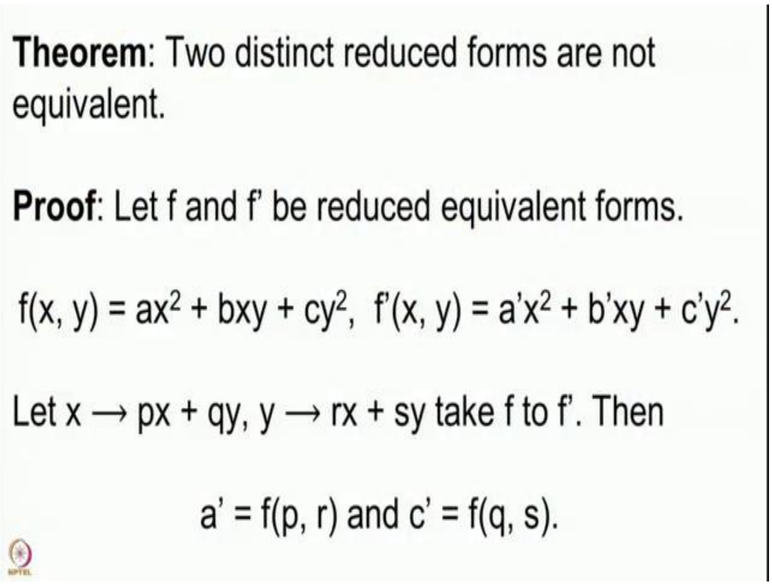
And our method of the proof is that we will start with two reduced forms, assume that they are equivalent and we will prove that they are one and the same. We will have to prove that their a's are same, c's are same and b's are same. This is what we are going to prove. So, suppose we have 2 reduced equivalent forms, we call them f and f prime. Let us say that f of x comma y has these coefficients a, b and c, and let us also assume that f prime is given by a prime b prime and c prime.

We are assuming that these two are reduced form. So, there are some standard inequalities that these coefficients a, b, c and a prime b prime c prime are going to satisfy. We further are shown that these are equivalent, so there is this change of variables x going to p x plus q y and y going into r x plus s y, which will take the form f to f prime. So, this form f goes to f prime when we apply this change of variables.

That means, if I write instead of x, if I write p x plus q y and instead of y, I write r x plus s y, then I should get the form f prime x comma y. Note that while defining the change of variables, we had identified the changed variable with x prime and y prime. We are not doing that, because we want to ease the notation.

So, we are going to keep the same x and y as variables for both the forms f and f prime, but note that we are keeping track of the change of variables, which is x going to p x plus q y and y going to r x plus s y, this is the change that we are assuming which takes place while taking the form f to the form f prime. We are going to prove the result by looking at these various inequalities for a prime b prime and c prime.

(Refer Slide Time: 6:48)



Theorem: Two distinct reduced forms are not equivalent.

Proof: Let f and f' be reduced equivalent forms.

$f(x, y) = ax^2 + bxy + cy^2$, $f'(x, y) = a'x^2 + b'xy + c'y^2$.

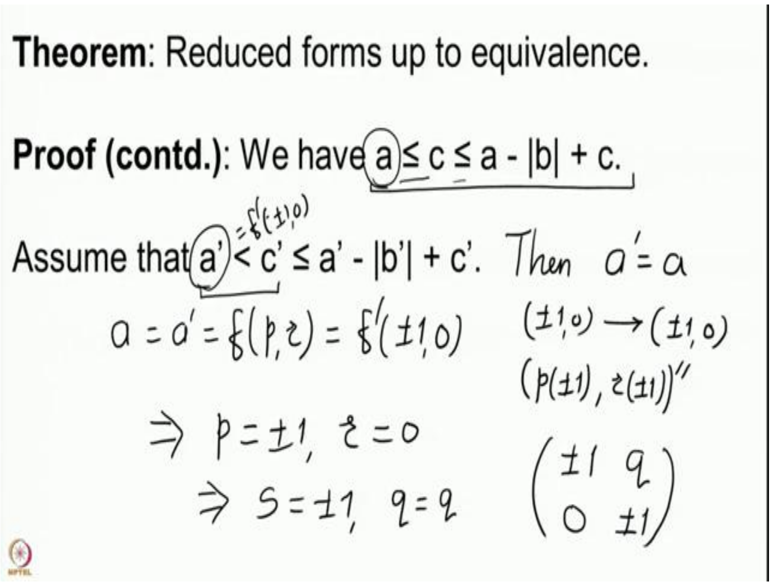
Let $x \to px + qy$, $y \to rx + sy$ take f to f'. Then

$$a' = f(p, r) \text{ and } c' = f(q, s).$$

Further, we also note that when we have this change of variables, then a prime is given by f of p comma r and c prime is given by f of q comma s. There is also a formula for b prime which we have in terms of a, b, c and p, q, r, s, all of them and we will actually need that formula sometime later, but we will come to right when we need it.

So, these are the things which we are going to remember for now, the forms that a prime and c prime take depending on ,p r and q, s and similarly, px plus q y and rx plus s y, this is the change of variable you can remember this by considering the matrix p, q r, s the 2 by 2 matrix with integer entries, whose determinant is plus 1, that is the most important thing.

(Refer Slide Time: 7:44)



Theorem: Reduced forms up to equivalence.

Proof (contd.): We have $\underbrace{\boxed{a} \le c \le a - |b| + c}$.

Assume that $\underbrace{\boxed{\overset{= f'(\pm 1, 0)}{a'}} < c'} \le a' - |b'| + c'$. Then $a' = a$

$a = a' = f(p, r) = f'(\pm 1, 0)$ $\quad (\pm 1, 0) \to (\pm 1, 0)$

$(p(\pm 1), r(\pm 1))''$

$\Rightarrow p = \pm 1, \; r = 0$

$\Rightarrow s = \pm 1, \; q = q$ $\quad \begin{pmatrix} \pm 1 & q \\ 0 & \pm 1 \end{pmatrix}$

Now, we have a less than or equal to c less than or equal to a minus mod b plus c, this is because our form is reduced. We also have similar inequalities for the coefficients of f prime. So we have a prime less than or equal to c prime less than or equal to a prime minus mod b prime plus c prime. We are assuming that the first inequality is a strict inequality. We start with the first one being the strict inequality. So among the three smallest values taken by the form f prime, a prime is the smallest and therefore, we must have that a prime is equal to a.

Here we have the three values taken by f, the values taken by f and f prime at co prime pairs are the same. The sets represented properly, the set of integers represented properly by f and f prime are the same. Here a prime is the smallest integer represented properly by f prime because this is nothing but f prime at plus minus 1 comma 0. And here a is the smallest integer represented by f, it may happen that a is equal to c and so you will have that a and c are the smallest being the same and you may have equality here also.

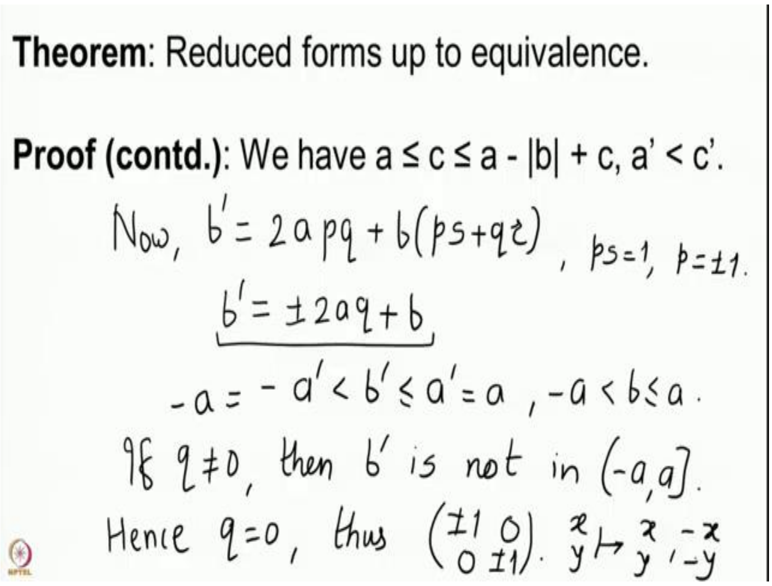
But in any case, a is the smallest integer represented by f, if a prime is the smallest integer represented by f prime, we must have that a equal to a prime because the two sets are same, so the smallest elements in both the sets will have to be the same. a prime is equal to a you also further have that a prime which is equal to a is f of p comma r and this is nothing but f prime at plus minus 1 comma 0.

So. what we get further is that when I have the integers plus minus 1 comma 0, you apply the change of variables and you still get plus minus 1 comma 0, we should have that p times x, which is plus minus 1 plus q times y, y is 0. So, we just get b into plus minus 1, r times x, r times plus minus 1 plus s times y, but s is y is 0, so you just get that this has to be equal to this pair.

What we have done is that we note that when you have x comma y being sent to p x plus q y comma r x plus s y, then the form f becomes the form f prime. And now we have the values plus minus 1 comma 0 for x and y, the value that you get is a, by applying the change of variables, you are going to get the same value. So, f prime at plus minus 1 comma 0 has to be f of p x plus q y comma r x plus s y, where x is plus minus 1 and y is 0.

So, we get from this computation that p is plus minus 1 and r is 0. But we also have that the determinant p, q, r, s has to be 1. So if p is plus minus 1, then s has to be plus minus 1. And let us say that at the moment, q is equal to q. So, we have that our matrix looks like plus minus 1, q, 0, plus minus 1. This is the change of variables matrix that we get. And after we get this matrix, we now look at the value change that happens to b prime.

(Refer Slide Time: 12:10)



Theorem: Reduced forms up to equivalence.

Proof (contd.): We have a ≤ c ≤ a - |b| + c, a' < c'.

Now, $b' = 2apq + b(ps+qr)$, $ps=1$, $p=\pm 1$.

$\underbrace{b' = \pm 2aq + b}$

$-a = -a' < b' \leq a' = a$, $-a < b \leq a$.

If $q \neq 0$, then b' is not in $(-a,a]$.

Hence $q=0$, thus $\begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$. $\begin{matrix} x \\ y \end{matrix} \mapsto \begin{matrix} x \\ y \end{matrix}, \begin{matrix} -x \\ -y \end{matrix}$

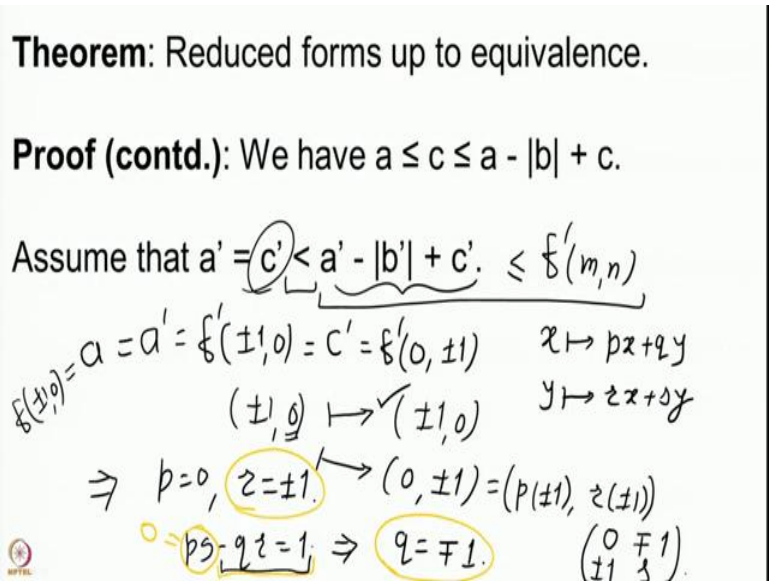
Now, b prime, if you remember is 2 a b q, plus b times p s plus q r and that is it. So, we note that since s is plus minus 1, r is 0, we get that this value is plus minus 2 a q plus b, ps is 1 and p is plus minus 1. So, we see that b prime is b plus minus 2 aq. Since f prime is a reduced form, we have that minus a prime is less than b prime is less than or equal to a prime, but we also have that a prime is a.

So, the values for b prime are between minus a and a and b prime also has this equality that b prime is b plus minus to a q. If q is not equal to 0, then b prime is not in the set minus a, a because b is already there, for b we already have this inequality. So, if I multiply 2 a by a non negative nonzero number and add or subtract it from b, we are no longer in the interval minus a, a. And therefore, to remain in the interval we must have q equal to 0.

Thus, our form becomes plus minus 1, 0, 0, plus minus 1, these so the allowed changes are x comma y can go to x comma y or to minus x minus y and then we check easily that after applying any of these 2 changes, the coefficients a, b, c are sent to the same coefficients a, b, c. That means you change x comma y to x comma y, of course, a, b, c remained going to remain as they are.

If you change x comma y to minus x comma minus y you are changing minus, you are changing sign of both x and y, then x square will change to x square x y will change to x y and y square changes to y square. Again, all the three coefficients abc remain the same. So, f is equal f is equal to f prime. In the very beginning case when a prime is strictly less than c prime, we have proved that a equal to a prime and therefore, using the allowed transformations, we see that b is b prime and c is c prime. Therefore, the forms are the same. Now, next case, we will assume that a prime is equal to c prime, but you have a strict inequality at the next level.

(Refer Slide Time: 15:45)



Theorem: Reduced forms up to equivalence.

Proof (contd.): We have a ≤ c ≤ a - |b| + c.

Assume that a' = c' < a' - |b'| + c'. $\le f'(m,n)$

$f(\pm1,0) = a = a' = f'(\pm1,0) = c' = f'(0,\pm1)$ $\quad x \mapsto px+qy$

$(\pm1,0) \mapsto (\pm1,0)$ $\quad y \mapsto rx+sy$

$\Rightarrow p=0,\ r=\pm1 \quad \mapsto (0,\pm1) = (p(\pm1), r(\pm1))$

$0 = ps - qr = 1 \Rightarrow q = \mp1$. $\quad \begin{pmatrix} 0 & \mp1 \\ \pm1 & s \end{pmatrix}$

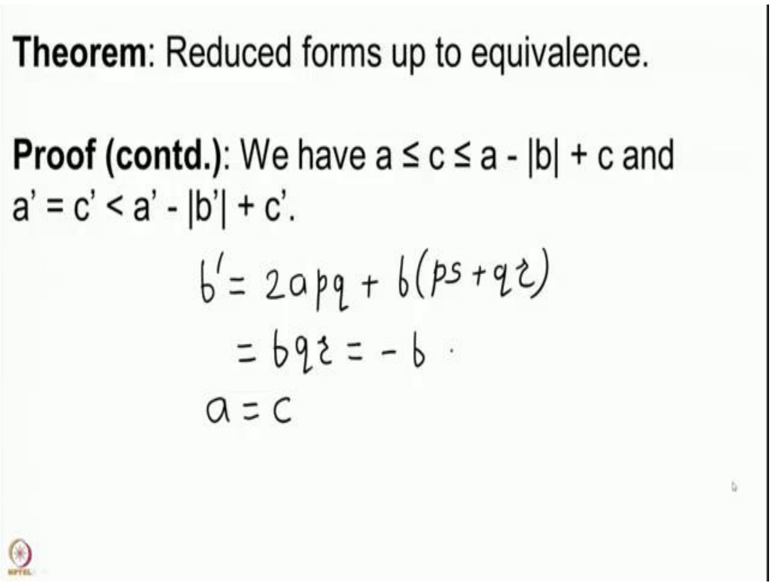
So, this is anyway there in force, a is less equal c less equal a minus mod b plus c, but we now allow a prime equal to c prime, but this is less than a prime minus mod b prime plus c prime. The reason for having the strict inequality here at the moment is that we know that whenever we have any 2 integers m comma n such that none of them is 0, then the values taken by f prime at m, n is at least this. So, if we are looking at the value taken to be c prime, it will have to be taken when one of the 2 is 0.

One of the 2 places m is 0 or n is 0, and these are the only possibilities for a prime and c prime. So, we of course, now have that a prime, which is f prime of plus minus 1, 0 this is equal to c prime which is f prime of 0 comma plus minus 1 and now we have that our, this is equal to a prime, a because c prime and a prime are still the smallest values represented by f prime properly. So, we now have that our a which was taken at plus minus 1 comma 0.

Therefore, the pair plus minus 1 comma 0 is sent to plus minus 1 comma 0 or it can also be sent to 0 comma plus minus 1. By the change of variables, which we have allowed remember x goes to p x plus q y and y goes to r x plus s y. So, this change of variables takes the pair plus minus 1 comma 0 to any of these 2 possibilities. Now, this is a change of variables which we have already studied in the last case. So, we will now come to this pair and here the change that happens, remember y is still 0.

So, we get this to be p into plus minus 1 and r into plus minus 1. So now, we get that p is 0, r is plus minus 1, you also have p s minus q r equal to 1, which implies that q is minus or plus 1. Minus or plus 1 means that whenever r is plus 1 q has to be minus 1. remember minus of qr is 1, p is 0. So, this quantity p s is equal to 0, we get minus qr is 1. So, r equal to plus 1 implies q has to be minus 1 if you take r to be minus 1 q has to be plus 1. So, the allowed transformation therefore reads, for p we have 0 for q we have minus or plus 1 for r we have plus or minus 1 and for s we have s. This is the form that we are allowing.

(Refer Slide Time: 19:26)



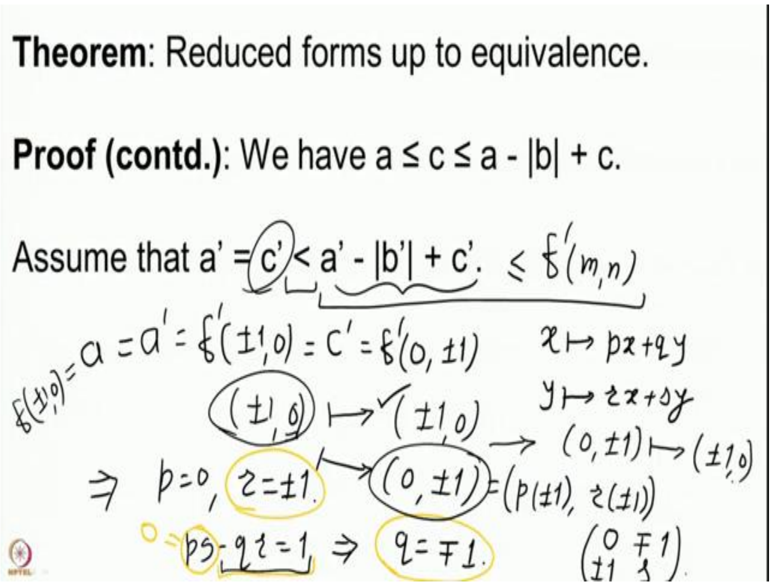
Theorem: Reduced forms up to equivalence.

Proof (contd.): We have $a \leq c \leq a - |b| + c$ and $a' = c' < a' - |b'| + c'$.

$$b' = 2apq + b(ps + qr)$$
$$= bqr = -b$$
$$a = c$$

Now, we look at the change that happens in b prime. So, b prime remember is 2 a p q plus b into p s plus q r, p is 0, so we simply get it to be b into q into r, q into r is negative of 1, that we have already observed here. So, we get it to be minus b. However, we have that a also has to be equal to c.

(Refer Slide Time: 20:23)



Theorem: Reduced forms up to equivalence.

Proof (contd.): We have a ≤ c ≤ a - |b| + c.

Assume that a' = c' < a' - |b'| + c'. $\leq f'(m,n)$

$f(\pm1,0) = a = a' = f'(\pm1,0) = c' = f'(0,\pm1)$

$x \mapsto px + qy$

$y \mapsto rx + sy$

$(\pm1,0) \mapsto (\pm1,0)$

$(0,\pm1) \mapsto (\pm1,0)$

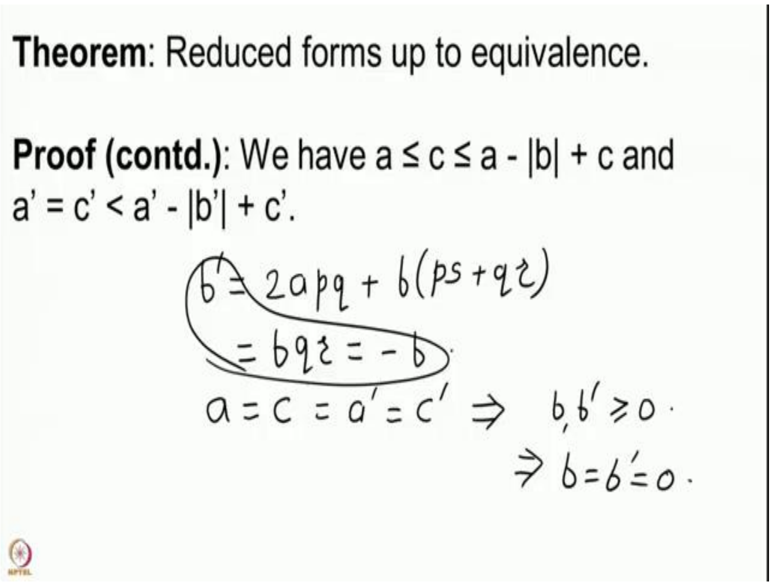
$\Rightarrow p = 0, \; r = \pm1. \quad (\pm1,0) \mapsto (0,\pm1) = (p(\pm1), r(\pm1))$

$ps - qr = 1 \Rightarrow q = \mp1.$

$\begin{pmatrix} 0 & \mp1 \\ \pm1 & s \end{pmatrix}$

Because we are allowing the transformation which takes minus 1 comma 0 to 0 comma plus minus 1 this is going to take also see this is also going to take the pair 0 comma plus minus 1 to plus minus 1 comma 0.

(Refer Slide Time: 20:41)



Theorem: Reduced forms up to equivalence.

Proof (contd.): We have a ≤ c ≤ a - |b| + c and a' = c' < a' - |b'| + c'.

$b' = 2apq + b(ps + qr)$

$= bqr = -b$

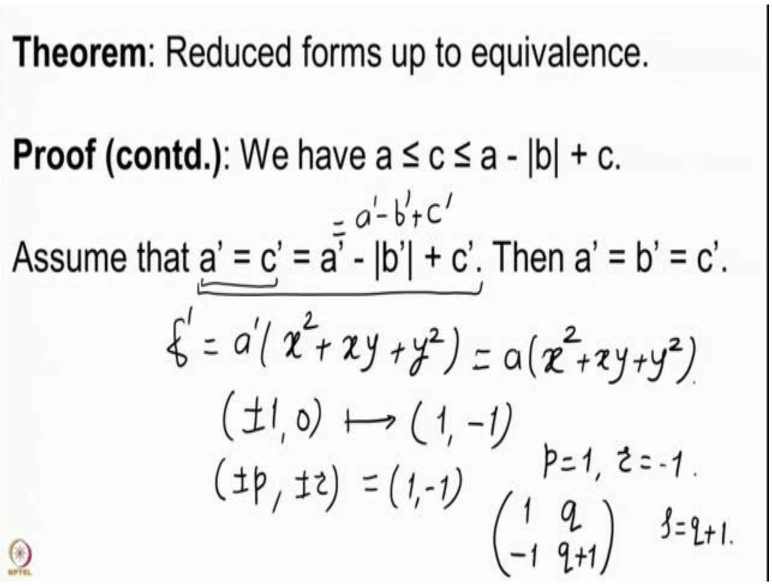
$a = c = a' = c' \Rightarrow b, b' \geq 0.$

$\Rightarrow b = b' = 0.$

So, this transformation will take a to c prime and a prime to c. So, we get that all these four are the same, which implies that both b and b prime has to be bigger than or equal to 0. But if b is equal to negative of b prime, then so this equality will force that both b and b prime are 0. And our form simply reads a into x square plus a into y square and f prime also reads a prime into x square plus c prime into y square, which is same as a into x square plus c into y square.

So, we are done with the second case, where we had assumed that a prime is equal to c prime, but we have a strict inequality at the next level. Now, we are going to start assuming that all these three are one and the same.

(Refer Slide Time: 21:45)



Theorem: Reduced forms up to equivalence.

Proof (contd.): We have a ≤ c ≤ a - |b| + c.

Assume that $\underbrace{a' = c'}$ $= \underbrace{\overset{= a'-b'+c'}{a' - |b'| + c'}}$. Then a' = b' = c'.

$$f' = a'(x^2+xy+y^2) = a(x^2+xy+y^2)$$

$$(\pm 1, 0) \longmapsto (1,-1)$$

$$(\pm p, \pm r) = (1,-1) \qquad p=1,\ r=-1.$$

$$\begin{pmatrix} 1 & q \\ -1 & q+1 \end{pmatrix} \qquad s=q+1.$$

So, this is the last case, where we have that a prime is equal to c prime, which is also equal to a prime minus mod b prime plus c prime. And of course, to have this possibility, because a prime is equal to c prime, b prime is positive and therefore, this minus of mod reads a prime minus b prime plus c prime. And so we get that b prime also has to be equal to a prime and c prime. Now, we come to the form where our form f prime reads a prime into x square plus x y plus y square.

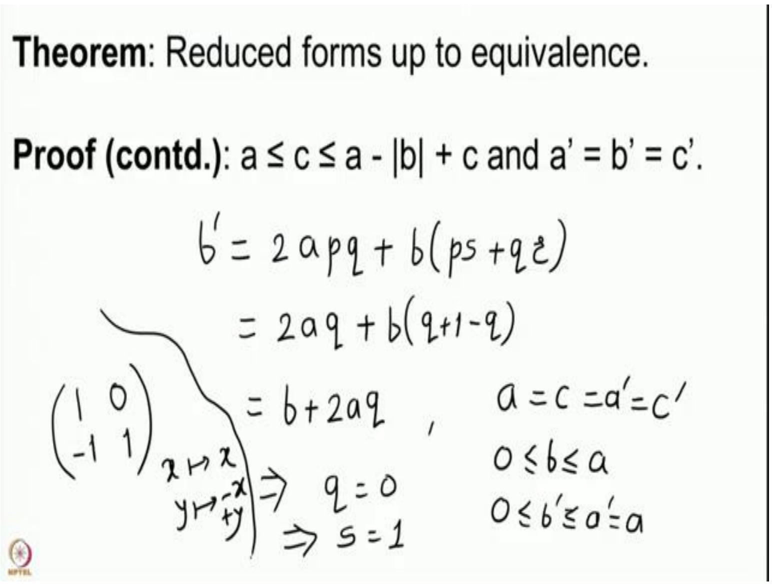
We know that these three values, a prime is equal to a, so the values taken at f prime at the integers plus minus 1 comma 0 is equal to a, a prime is a. a prime is a because we are taking the value the smallest value represented by f prime has to agree with the smallest value represented by f and that value is a. So, you get that a prime is a and the form reads x squared plus x y plus y square whole thing multiplied by a prime. Now, when are what are the integers m comma n, such that this form x square plus x y plus y square gives you the value equal to 1.

So, those are the integers which will give the value to f prime equal to a. So, we are looking at all possible pairs m comma n such that f prime of m comma n is a. We have seen the cases plus minus 1 comma 0, 0 plus minus 1. By looking at this form x square plus x y plus y square, it is an easy exercise and it will be in the corresponding assignment to you that 1 comma minus 1 is the only other possibility, except of course, you have minus 1 comma 1.

So this is the final third possibility that plus minus 1 comma 0 being sent to 1 comma minus 1. So we apply p x plus q y to this pair plus minus 1 comma 0 to get minus 1 plus minus 1 p plus q times 0 plus minus 1 times r plus y, s times 0 equal to 1 or minus 1. And we consider the case p equal to 1, r equal to minus 1 and we leave the other case as an exercise. So the matrix now reads p, q, r is minus 1, p is 1, r is minus 1 here you have q and here we have q plus 1 because we want the determinant to be equal to plus 1.

So these are the matrices that we are allowing, s is q plus 1. To have the determinant to be 1, we should have that s is q plus 1. So let us see what change happens for the element b prime.

(Refer Slide Time: 25:28)



Theorem: Reduced forms up to equivalence.

Proof (contd.): a ≤ c ≤ a - |b| + c and a' = b' = c'.

$$b' = 2apq + b(ps+qr)$$
$$= 2aq + b(q+1-q)$$
$$= b+2aq \, , \quad a = c = a' = c'$$
$$0 \leq b \leq a$$
$$0 \leq b' \leq a' = a$$

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \quad x \mapsto x, \quad y \mapsto -x+y$$
$$\Rightarrow q = 0$$
$$\Rightarrow s = 1$$

So b prime now becomes 2 a p q, let me write the formula for b prime, p is taken to be 1. So we have this to be to a q plus b into s, p is 1, s is q plus 1, r is minus 1. So we get it again to be b plus to a q. Remember, you have b prime equal to b plus to a q, but a is equal to c equal to a prime equal to c prime and then we should have that 0 less equal b less than or equal to a and b prime is also between the same range.

So this again forces q to be 0, s is 1 and our allowed matrix then becomes 1, 0, minus 1, 1 and then once again, so this change of variables is x going to x, y going to minus x plus y. So it is a simple exercise to you, to check that when you apply this change of variables, a is going to be signed to a, c is going to be sent to c and the coefficient b is also sent to the same coefficient b. So by looking at all these three possibilities, we prove that there are only these many transformations which are allowed to take a reduced form to a reduced form.

And all these transformations keep the integers a, b and c invariant. Therefore, the form f is sent to the form f prime. What we have actually done is that we have not just proved that any two reduced forms which are equivalent are equal, we have also computed all possible transformations, which send a reduced form to itself. We will see more of this in the assignment, but for the lecture we stop here and in the next lecture onwards, we will study the integers which are written as sums of squares. See you soon. Thank you.