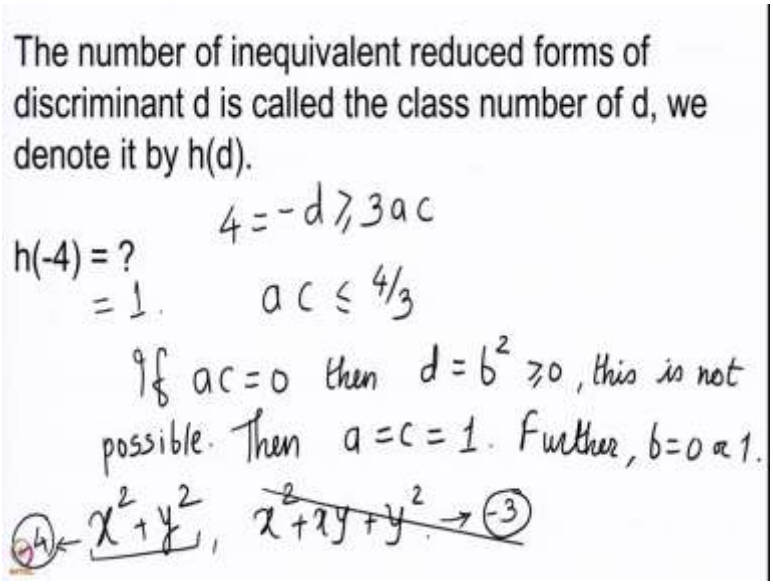
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 43
Reduced forms up to equivalence - II

Welcome back in the last lecture, we reproved the result that every positive definite form is equivalent to a reduced form and we also saw that given any discriminant d, which is a negative number there are only finitely many reduced forms of the discriminant equal to d. So, we would like to compute this number and the number of inequivalent reduced forms of the negative discriminant d is called the class number of d. This is a very important quantity.

In fact, given any such negative number, there is a certain field extension of the rationals associated to the number and then there is a quantity called class group associated to this field extension, this class number that we are going to compute actually happens to be the cardinality of the class group. So, the class group and so on, which is defined in a slightly non-trivial way, its order can be computed very easily simply by looking at the number of inequivalent reduced forms of the discriminant d.

(Refer Slide Time: 01:33)



So, this is a very important number, we denote it by h d, let us do one computation for this number, we know that this number has to be negative, and it is allowed to be 1 or 0 mod 4. So,

let us look at the first negative number which is non-zero and is 0 mod 4. So, that number is minus 4, let us compute h of minus 4. We have the following bound that minus d is bigger than or equal to 3 ac, but minus d here is 4. So, we get immediately the bound on ac to be less than or equal to 4 by 3.

Now, it is possible that your a and c might be 0 if a and c are if any of these, so, which means that if the product is 0, then d is b square because actual definition of d is b square minus 4 ac but ac is 0. So, d is b square and b square is always bigger than or equal to 0. So, this is not possible which means that ac the product ac is not allowed to be 0 that will have to be a positive number and the only integer which is not 0 and is yet less than 4 by 3 is equal to 1.

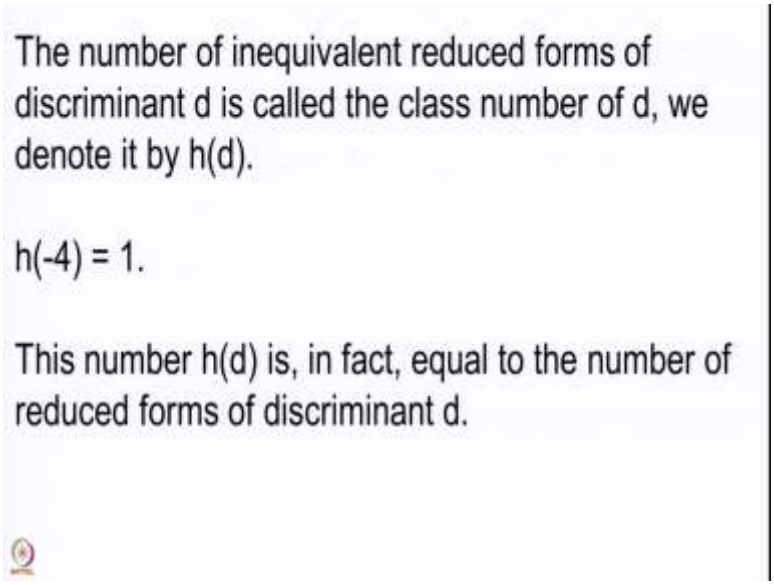
So, what we then have is that a equal to c equal to 1, a and c are both non-negative. So, they are both either 0 or positive and their product is equal to 1. So, they better be both equal to 1. So, now a is 1, b is therefore allowed to be 0 or 1 because a and c are equal. So, the possibilities for b go from 0 to a which is 0 and 1.

So, further b can be 0 or 1. So, the two forms that we get are x square plus y square, where a is 1, b is 0 and c is 1 and the other form is x square plus x y plus y square and so, these are the two possible forms satisfying the bound which was given by the discriminant being equal to minus 4 and now we need to see whether these two forms have the required discriminant.

So, this I think we had checked last time the discriminant of this is minus 4. So, this form is okay for us here if you check the discriminant it is 1 minus 4 and therefore, this is minus 3. So, this is not the form that we are going to take, we will take only this form which is the only reduced form of discriminant minus 4. So, the answer to our question is h minus 4 h is equal to 1. That is a very good thing.

In fact, this is something that we are also going to use later in remaining further lectures. But, therefore, you should remember this, but the proof is also very easy that h of minus 4 is equal to 1.

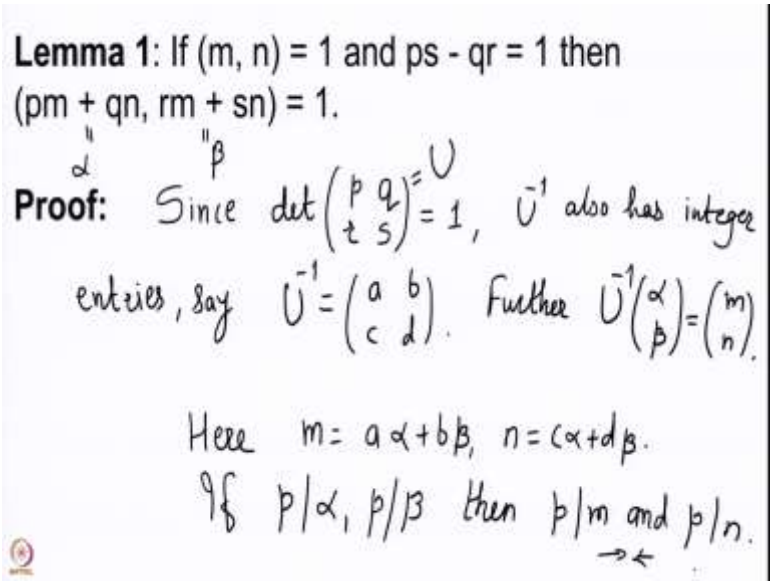
(Refer Slide Time: 05:25)



And now, we come to this next observation that this number h d is in fact equal to only the number of reduced forms of discriminant d, which means that we are doing away with the phrase inequivalent that is redundant, if there are two reduced forms which are equivalent then they have to be the same different reduced forms cannot be equivalent to each other. This is the next theorem that we are going to prove.

But before we go to this proof, there are some intermediate lemmas that we will have to do some basic statements which need to be observed and they need to be proved. So, we will state and prove these lemmas and then, we go to proving the statement, that two reduced forms which are equivalent have to be the same.

(Refer Slide Time: 06:21)



So, here is the first statement, which is quite a simple statement, if you have two integers, which are co prime and we look at our allowed transformation. So, we have ps minus qr equal to 1 and we transform the m and n by the allowed transformation which is that m is going to pm plus qn and n is going to rm plus sn. Then the GCD of these two numbers remains equal to 1, this GCD does not become bigger. So, how do we prove this? This proof is actually very easy.

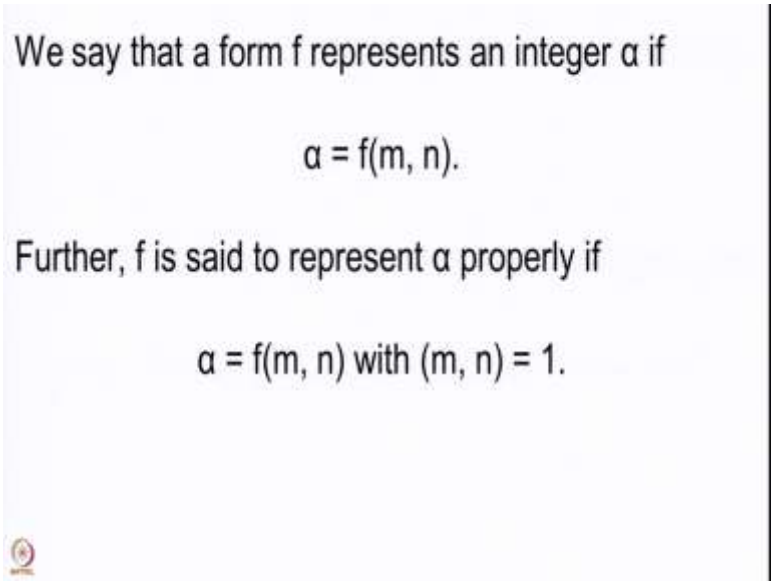
So, since determinant of our matrix, which is p q, r s is 1 we call this matrix to be u, we have that U inverse also has integer entries. Say, U inverse is a b c d. So, we have U inverse which also has integer entries and if we have we call these numbers as alpha and beta, then U inverse into alpha beta gives us our numbers m and n. So, m is a linear combination integral linear combination of alpha and beta, n is an integral linear combination of alpha and beta given by ab and cd.

Now, if alpha beta had a GCD, which was not equal to 1 that would mean that there is a prime which divides the GCD of alpha beta. Whether the GCD is positive or negative that we do not worry about right now, the GCD can be always taken to be positive, since we are looking at the number which is dividing both these quantities, so, if some negative number divides it, its negative, will also divide it.

So, we are taking the GCD to be positive therefore, we will assume that whenever this GCD alpha beta is not 1, then there is a prime p which divides both alpha and beta. But if p divides

alpha p divides beta then p will divide this combination of alpha and beta. If there is a p which divides alpha and beta then the p will divide m and p divides n. This is clearly a contradiction because we had assumed that the numbers m and n are co-prime. So, if m and n are co-prime and you have a GCD of alpha and beta to be not equal to 1 we get a contradiction. So, the GCD of m and n have to be equal to 1. This is a very important statement. Let us see the importance of this statement in the next slide.

(Refer Slide Time: 10:13)



First of all, let us recall that whenever we are given any form f, we say that an integer alpha is represented by f, if you have that alpha equal to f of mn for some integers m and n, okay. Further, this is a new definition, we say that f represent alpha properly the integer alpha is represented properly by f, if you have alpha equal to f of m comma n, where the m and n are co-prime, the GCD of m and n is equal to 1.

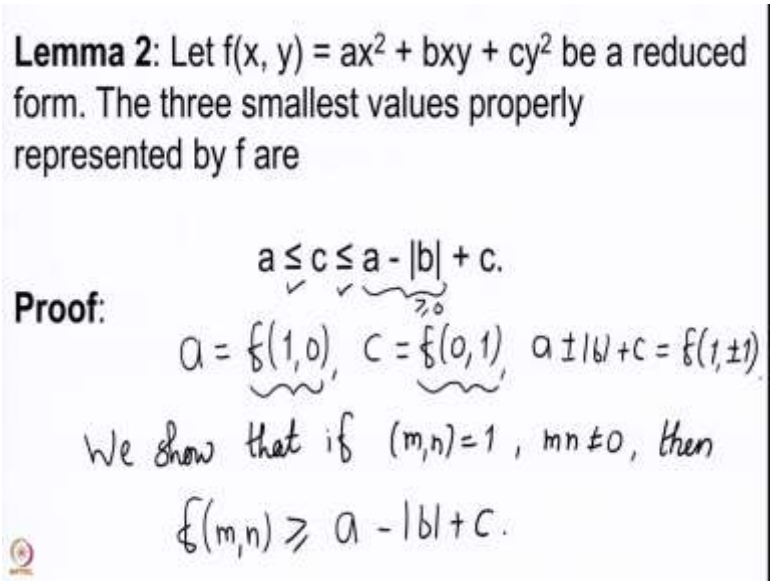
So, we have numbers which are represented by the given positive definite or in general a binary quadratic form, if you have alpha equal to f of mn. Now, these m and n might have a nontrivial GCD but if the GCD is 1, the corresponding integers which are represented by such pair of elements are called to be properly represented by the given form f. What does the lemma say?

Remember lemma said that whenever you had mn to have GCD 1, the transformation the change of variables will give you another pair, which will continue to have GCD 1. So, lemma 1 says that the integers properly represented by two equivalent forms are the same. We had earlier seen

that the value sets of two equivalent forms is the same set, if you have an integer which is represented by 1 form, it is also represented by its equivalent form and therefore, the values represented by two equivalent forms are the same sets of integers.

Here we have this is a somewhat restricted subset that the number of integers, the actual integers which are represented properly by these two forms which are equivalent are same. So, if I have alpha represented properly by f, and f is equivalent to g then alpha is represented by g but it is also represented properly that means, there will have to be some co-prime integers which will give you the value alpha. This is a very important statement. We now go to another very-very important lemma.

(Refer Slide Time: 12:52)



This lemma says that if you start with a reduced form given by ax square plus bxy plus cy square, then the three smallest values represented by f are the ones which are given in the screen. So, we are looking at reduced forms. Remember, the reduced form is always a positive definite form, it will take only positive values, so, we can talk about smallest values represented by the form and what we say here is that any small value represented properly by the form f will either be equal to a or c or a minus mod b plus c or bigger than this. So, this is a very important statement.

So, let u go about proving this statement. There are two parts, first of all, we will have to prove that these 3 values are represented by the form and then we will say that any value represented

properly by our form will have to be bigger than or equal to these 3. So, that will tell you that these are the 3 smallest values represented by our form; a is first of all equal to f of 1 comma 0, c is equal to f of 0 comma 1 and a plus or minus mod b plus c is f of 1 comma plus minus 1.

So, we then have that these values ac and a plus minus mod b plus c are represented properly by our form f. Now, note here that here although we have the integers 1 comma 0 and the GCD of 1 comma 0 is 1. Similarly, here we have 0 comma 1 and clearly GCD of 0 comma 1 is also 1. If you had anything where one of the two integers if you had any pair of integers where one of the two integers is 0.

Then the other will have to be a multiple of 1 clearly, and then the value represented will be a multiple of a or c by a square. This is what we have. And now, what we are going to see further is that if you have any two integers which are co-prime, then clearly whenever 1 of them is 0, the other is 1. So, if you are looking at integers, which are represented properly by our form f, and if the none of those integers is 0, then we have to only show that those values are bigger than or equal to a minus mod b plus c.

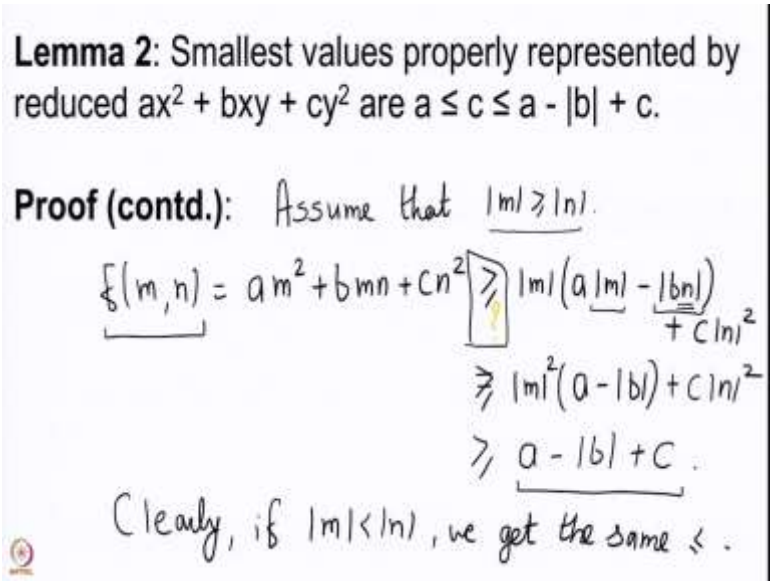
So, let me write down this statement, we show that if m n is 1, the product is non-zero, then f m comma n is bigger than or equal to a minus mod b plus c, this will complete the proof because the proper representation requires a pair of integers which are co-prime, if any of the m or n is 0, the other integer has to be 1. So, 1 0 and 0 1 these are the two possible pairs of integers which are co-prime and one of the two integers is equal to 0, but there are no other such elements.

So, once we are done with these two, the other numbers that are going to be properly represented will be given by m comma n where the product m n is non-zero and then we show that any such value f of m n has to be bigger than or equal to this third number a minus mod b plus c. Before we go further, let us also quickly observe that the inequalities that we have written here are true. We clearly have that c is bigger than or equal to a because our form is reduced.

So, this inequality is okay this inequality is there, because a minus mod b, this is always bigger than or equal to 0, remember, b can take values only from minus a to a so mod b can never be bigger than a. So, a minus mod b this is either a positive number or a 0 and therefore, the second inequality also holds.

So, we have these three numbers in these in this order which are represented properly by the form f and these are the three smallest values represented by f properly. So, now, we need to show this last statement that whenever you have a pair of integers m n of non-zero integers which are co-prime, then the value f of m n is bigger than or equal to a minus mod b plus c.

(Refer Slide Time: 18:28)



So, assume first of all, that our mod m is bigger than or equal to mod n, this is one thing that we are shown 1 inequality we will then also see the other proof; f of m comma n is am square plus bmn plus cn square. We observe one basic inequality here. We will prove this inequality later, but let us assume this inequality to begin with, okay.

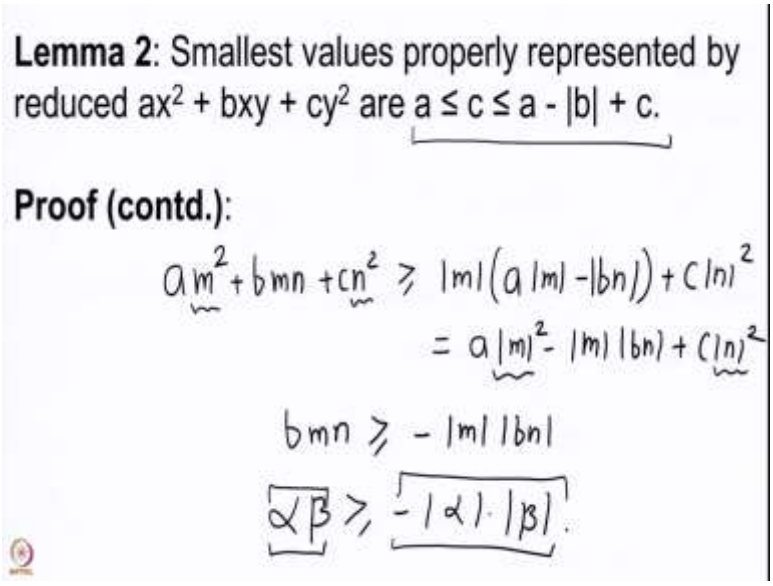
So, now, here we have that this is further bigger than or equal to mod m into a minus mod b. This is because here we are taking this mod m common, this would be mod b into mod n, and we are assuming that mod of m is bigger than or equal to mod of n. So, when we put a negative sign to it, it will mean that minus of mod m is less than or equal to minus of mod n.

Therefore, I can replace this n here by m and I will get a smaller quantity and therefore, we have this smaller quantity mod of n square a minus mod b and finally, I just have mod of n square, but we have observed that m and n are both non-zero. Therefore, mod of m is 1 or more mod of n is 1 or more, and therefore, this quantity is bigger than or equal to a minus mod b plus c.

So, barring the inequality that we have here which is not proved yet, we have the result that with mod m bigger than or equal to mod n, f of m n is always bigger than or equal to a minus mod b plus c. Now, m is the coefficient of a, n is the coefficient of c. Let us look at the inequality that we have obtained the inequality is symmetric as far as a and c are concerned, if you switch a and c the inequality that you obtain remains the same.

So, therefore, we will have the same method clearly if mod m is less than mod n, we get the same inequality. So, modulo this inequality that we have not yet proved, we are done with the proof because we would have proved that whenever m n are non-zero and are co-prime the values taken by m and n on the form f is bigger than or equal to a minus mod b plus c and let us just see what is happening. So, let me write down this inequality once again on the next slide and we will prove this.

(Refer Slide Time: 22:11)



This is the inequality that we want to prove. Now, notice that this thing is simply a times mod m square minus mod m into mod bn plus c times mod n square. Now, whether m is positive or negative, whether n is positive or negative mod m square is the same as m square mod n square is the same as n square. So, to prove this inequality, we have to only prove bmn is bigger than or equal to minus of m into mod minus of mod m into mod bn which is actually equivalent to showing that product alpha beta of any two integers is always bigger than or equal to the product minus of mod alpha mod beta. This is the only inequality that we have to observe.

But this is true, we can just look at all possibilities for the signs of alpha and beta. If both alpha beta are positive, here we get something which is bigger than or equal to 0, this is positive, and this quantity is clearly negative, because mod alpha is alpha, mod beta is beta. So, you have a positive quantity bigger than a negative quantity, which is clearly true. If both alpha and beta are negative, their product is positive.

So, this quantity is again bigger equals 0. If both are negative, whereas this is again going to be negative, this quantity on the RHS is always negative. So, what you may have is that the quantity on the LHS is either positive or it is negative and equals the quantity on the RHS. So, LHS is positive and therefore, it is bigger than the RHS which is negative or 0 or LHS is negative and equals the RHS.

So, how can LHS be negative; you may have different signs for alpha and beta, alpha is positive and beta is negative say, then you have that beta is equal to minus of mod beta. If beta is negative mod beta is its negative, if beta is minus 5 mod beta is 5 and then minus of mod beta is equal to beta. So, you then have equality here whenever any of these two have different signs. So, the worst thing that you have for inequality is that you get equality.

Whenever alpha and beta have distinct signs alpha beta is equal to minus of mod alpha minus mod beta and whenever alpha beta have the same signs be positive or negative, then we get that alpha beta which is now a positive quantity is strictly bigger than minus of mod alpha times mod beta. So, this proves our statement that whenever we have any reduced form the smallest three values which are represented by the positive definite reduced forms are a less equal c, less equal a, minus mod b plus c.

Armed with these two lemmas, we are going to prove that any reduced form is not equivalent to another reduced form unless they are the same. So, we will start with two reduced binary forms which are equivalent to each other and we will show that they are both are just the same forms, but we will have to wait for the next lecture for this. So, I will see you then thank you very much.