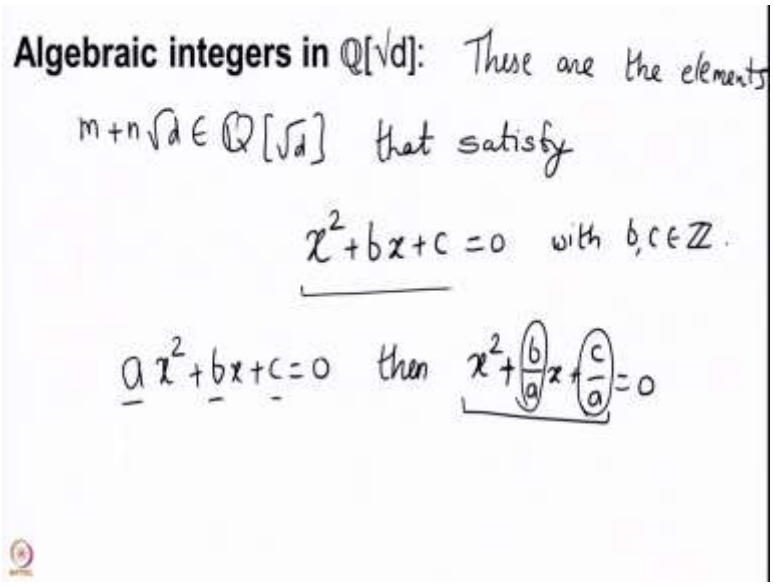
A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 60
Units in Quadratic Fields: The Imaginary Case

Welcome back, we are studying the algebraic integers in Q root d, Q root d is the set of all expressions of the form x plus y root d. So these are all the numbers where we are looking at d to be a natural number which is square free, so we have that Q root d is in fact contained in R, there is some theory which holds for d negative also. So we will mention when we come to that but mainly we will be considering the set Q root d where d is positive.

We observed in our last lecture that the set Q root d is actually a fade, you can add and subtract any two elements from each other and remain in the set Q root d, you can multiply any two elements and remain in Q root d, you can divide by a non-zero element and remain in Q root d, so some in some sense the elements of Q root d behave like the rational numbers.

We have the addition multiplication in rational numbers also and we can divide by any non-zero rational number to any other rational number and we are in the set Q. So, Q root d is a slightly bigger subset of complex numbers than Q and it has the same property that it remains a field, we then talked about what are called algebraic integers, so we have the normal integers Z sitting in Q and these algebraic integers, they are the analog of Z.

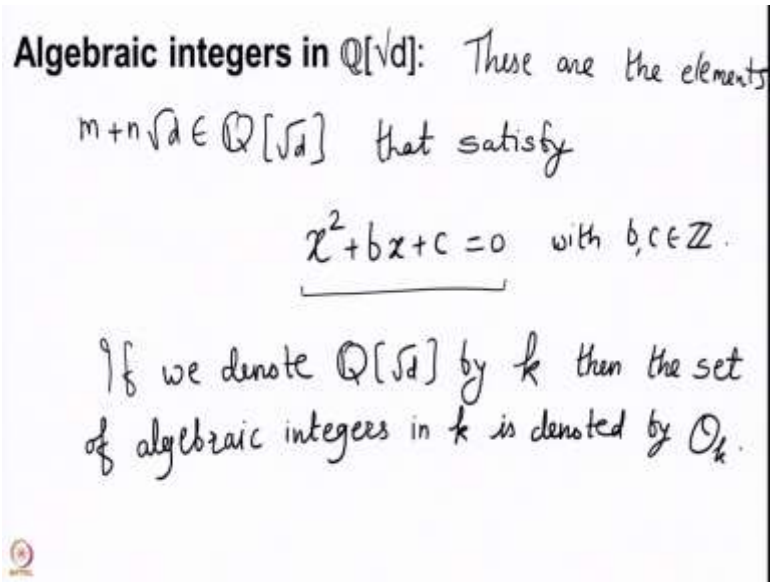
(Refer Slide Time: 01:58)



And we saw the definition in our last lecture, that these are the elements m plus n root d in Q root d that satisfy x square plus bx plus c equal to 0 with b and c integers. Now, we have observed that any element in Q root d is going to satisfy the equation of the form ax square plus bx plus c equal to 0 and here the a is clearly non-zero, then we can divide by a and we get that x square plus b by ax plus C by a this is also satisfied by the number m plus n root d.

But here because a is non-zero and a can be any integer the elements b by a and c by a then it not be integers. Here we started with a, b, c being integers, but if you divide by a then b by a and c by a need not always be integers, therefore any element in Q root d need not satisfy such an equation with b and c being integers, there are going to be some very specific such elements which will satisfy this particular equation.

(Refer Slide Time: 03:54)



The set of elements which satisfy these type of equations are inside some very special set and if we denote Q root d by this letter k then the set algebraic integers in k is denoted by this symbol. So, this is the set of all algebraic integers in Q root d, where k denotes Q root d, it turns out that this is a ring you can add and multiply by any two such elements and you will be in the same set and therefore the main question is what are the elements by which you can divide.

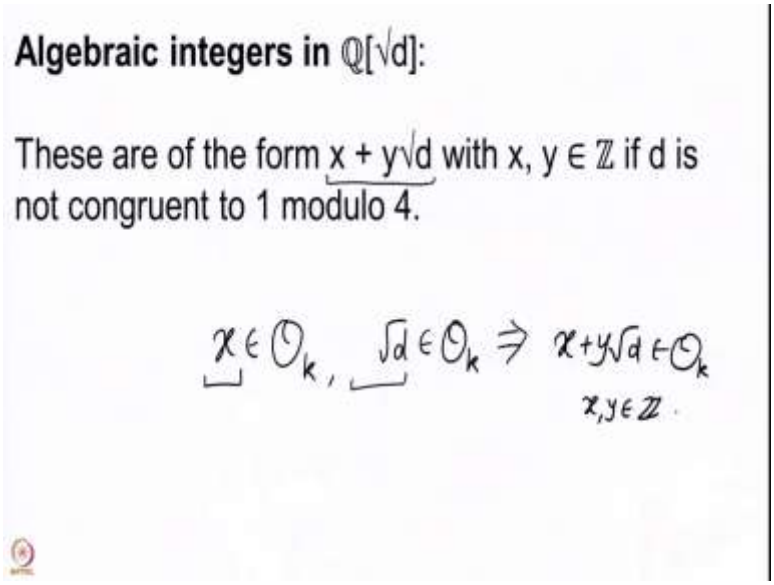
But even before we tackle that question, the main question that we want to know is whether there is a nice description for such set of elements for these elements, ofcourse the description is there given by the definition that any such element has to satisfy what is called a monic polynomial, monic meaning the leading term the coefficient of the highest degree monomial is 1.

So, the algebraic integers are the ones which satisfy monic polynomial over integers. This is one description, but is there a better description for instance for quadratic irrationals we gave the definition saying that these are the ones which satisfy some ax squared plus bx plus c equal to 0 where a, b, c are integers and something else, b square minus 4ac is a natural number and it is not a square and so on.

So, these are the things that we had by defining a quadratic irrational, but then we also said that these are nothing but x plus y root m where x and y are rational numbers and m is a natural number, which is non-square. So, this is some a simpler description for quadratic irrationals, is

there a simpler description for algebraic integers in Q root d? Yes, there is a nice very simple description.

(Refer Slide Time: 06:32)

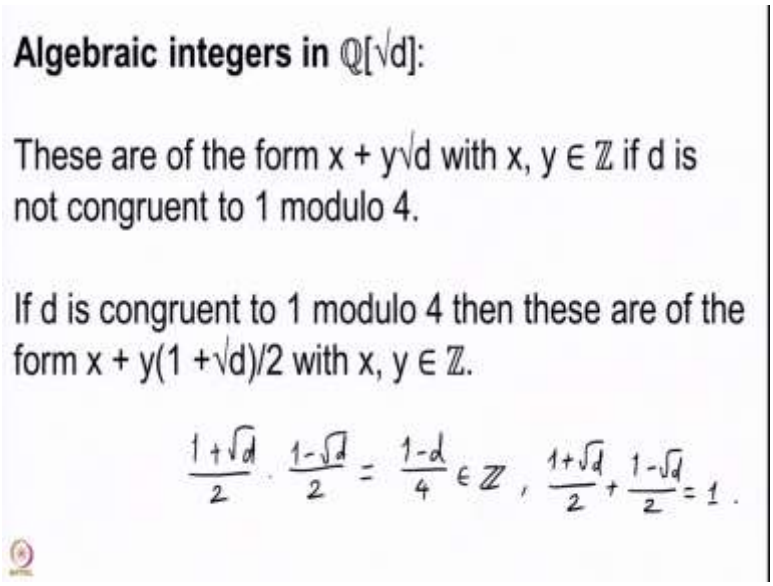


So, this description depends on whether d is congruent to 1 modulo 4 or not. When d is not congruent to 1 modulo 4 then the algebraic integers are of the form x plus y root d where x and y are integers. So, note first of all, this is one very simple observation that we make that x being an integer is in O k and y root d if y is an integer is also in O k, because any integer is going to satisfy a monic degree one polynomial, so you can construct a monic degree were two polynomial satisfied by the integer, you may just take the square of that polynomial.

Similarly, if I have y root d where y is an integer then we can again get a nice or you know even before we go to y root d you just consider that root d satisfies a degree to polynomial whose leading term is 1 namely x square minus d. So, root d is in O k, x is in O k and this would imply that x plus y root d is an algebraic integer whenever x and y are integers.

This is a very easy thing to see assuming that O k is closed under addition and products, but this is a converse to that it says that everything in O k is of the form x plus y root d where x and y are integers. This is when d is not congruent to 1 modulo 4, if you happened to have d to be congruent to 1 modulo 4 then this extra element 1 plus root d by 2 that is also an algebraic integer.

(Refer Slide Time: 08:32)



Because 1 plus root d by 2 into 1 minus root d by 2 this happens to be 1 minus d by 4, which is an integer, remember d is congruent to 1 modulo 4 and the sum of this element and its conjugate is also an integer. So, you can easily construct a degree to monic polynomial satisfied by the element 1 plus root d upon 2, when d is congruent to 1 modulo 4.

So, just like the previous analysis 1 is an algebraic integer, 1 plus root d by 2 is an algebraic integer, so there integral combinations will give you algebraic integers. In particular you can write it as x plus y root d where x and y are of some certain type of half integers, they are of the form m by 2 n by 2 where m and n should have same parity, both are odd or both are even.

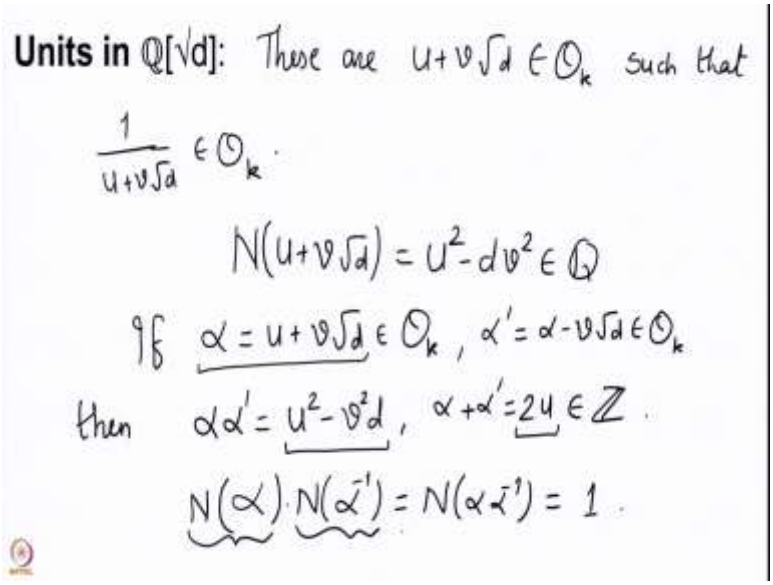
So, this is the description for algebraic integers in both the cases, to remember this what you should note is that d can never be 0 modulo 4 because we are taking d to be square free, d can never be 0 modulo 4, d should not be divisible by 4, any square-free integer cannot be divisible by 4, so the only possibility for d is 1 mod 4; 2 mod 4; 3 mod 4.

If it is 1 mod 4 then 1 plus root d by 2 is an algebraic integer by the calculation that we have done, so when it is 1 mod 4 it is an algebraic integer in and in all other cases it is not an algebraic integer. You should only remember when 1 plus root d by 2 is an algebraic integer or not, that will tell you whether you should look at the congruent to 1 mod 4 or 2 mod 4 or 3 mod 4.

So, this is the description that we have for the set of algebraic integers, this ring of algebraic integers. Now, we want to know which of these are units, so we want to know what are the

elements x plus y root d whose inverse is also in the same set O k, we want to know what are the elements which are divisible in the ring of algebraic integers which are invertible in the ring of algebraic in interiors, that is the question that we want to study, we call any such element to be a unit.

(Refer Slide Time: 11:21)



So, these are m let me not use it m n, these are u plus v root d in O k such that 1 upon u plus v root d is also in Ok. These are the elements that we want to compute. So, this will then form a group of elements because whenever you have a unit then multiplied by any other unit you are going to get suppose alpha 1 is a unit and alpha 2 is a unit then alpha 1 inverse which is 1 upon alpha 1 is in O k, 1 upon alpha 2 is also in O k.

So the product will give you that 1 upon alpha 1 into 1 upon alpha 2 is a product of two elements of Ok, which is also in O k, it would mean that whenever alpha 1 is a unit alpha 2 is a unit the product is also a unit. And ofcourse you have that the element 1 is there in the unit, 1 is always invertible and by the very construction a unit would mean that it is inverse is there in O k. So, if you collect the set of all units in Q root d, these are called units.

But these are invertible only within O k. We are not looking at unit in the elements which are invertible in Q root d, those will be all non-zero elements of Q root d, we are looking at numbers which are invertible in O k and as we have seen in the last slide these are of some very specific

type, these are of the type some x plus y root d where x and y are either integers or they are half integers.

So, in some sense we are looking at a discrete set when you have x and y you know the analogy you should keep in mind is that if you plot the set of integers on the real line then you have 0, 1, 2, 3 or on the negative side minus 1, minus 2, minus 3 and so on. The distance between any two successive such elements is 1 what you have is that there is an epsilon such that the distance between any two is at least epsilon, for the set of integers you can take it to be 1.

If you have half integers m by 2, n by 2 you allow m to be an integer, then you have 0 1 by 2, 1; 3 by 2, 2; 5 by 2, 3 and so on then you are epsilon is 2, then the epsilon is 1 by 2. So, there is whenever you have a set of real numbers with the property that any 2 are apart from each other by some minimum distance then the set is called discrete, it is discreetly divided, it is discreetly situated, discreetly located in the set of real numbers.

On the other hand there is a set called compact set. We will come to that later. So, what we have here is that our elements are discrete and these are also invertible, so we are putting two very strong conditions on these sets. And so as it turns out the units in Q root d can be explicitly described, there is a very important theorem by Dirichlet which will describe this.

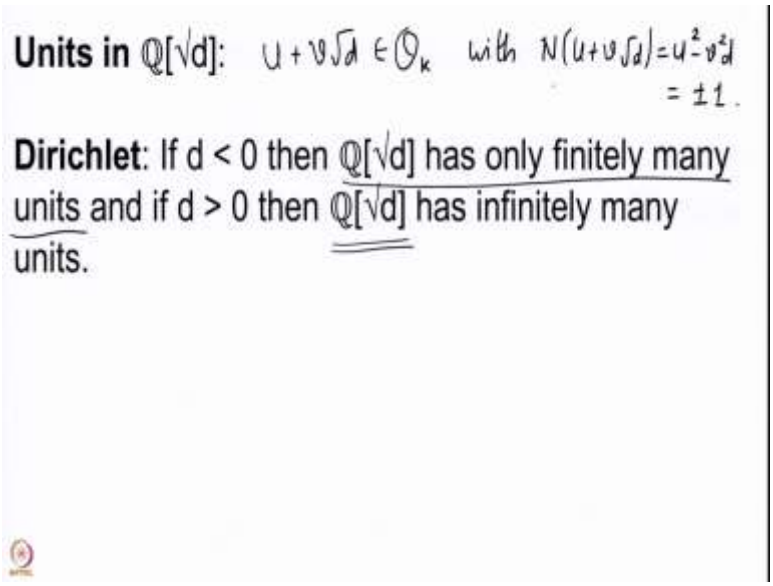
But before we go to that, let me observe one thing for you, that we have seen that the norm of u plus v root d is u square minus dv square which is always a rational number if alpha equal to u plus v root d is in O k if alpha equal to u plus v root d in O k and we take alpha prime which is alpha minus v root d, which is also in O k for the description that we have given of algebraic integers then the norm of alpha which is u square minus v square d and alpha plus alpha prime, which is 2u these are in fact integers.

There is a very nice and simple proof for this because given any such alpha u plus v root d we can construct a monic polynomial over integers satisfied by alpha, but if alpha is in O k, then the monic polynomial should have integer coefficients, the earlier was monic polynomial over rationals, so here the alpha should satisfy a monic polynomial over integers and then it turns out that u square minus v square d and 2 u must be integers.

In fact, this goes into the proof of the description that we have given in the last slide for writing down any algebraic integer in that particular form. So, this is what we use, so we have that alpha-

alpha prime is an integer, the norm is an integer and further we have that norm alpha into norm of its inverse is the norm of alpha-alpha inverse which is 1 both of these are integers, so you have an integer dividing 1 in the set of integers. And the only invertible integers are 1 and minus 1, if you have norm alpha to be anything other than 1 and minus 1 you cannot multiply to it by again an integer and get 1.

(Refer Slide Time: 17:38)



Let me recall for you that these are all the elements u plus v root d in O k with the norm equal to u square minus v square d to be 1 or minus 1, these are precisely all the elements which are the units in the field q root d and here we have a theorem due to Dirichlet which describes the set of units completely. In fact, the theorem of Dirichlet goes even higher it here we are looking at elements which are of the form a plus b root d.

And so you have what is called quadratic these are the elements which satisfy a quadratic polynomial. Dirichlet theorem is a general theorem it is a very well celebrated result, it describes units in the set of in the fade of algebraic numbers where you have a finite degree for the field. The fade of algebraic numbers precisely mean that you are looking at the elements which are of the form a plus a0 plus a1 alpha plus a2 alpha square plus dot dot dot plus ak alpha power k where that alpha satisfies a polynomial of degree n over rationals.

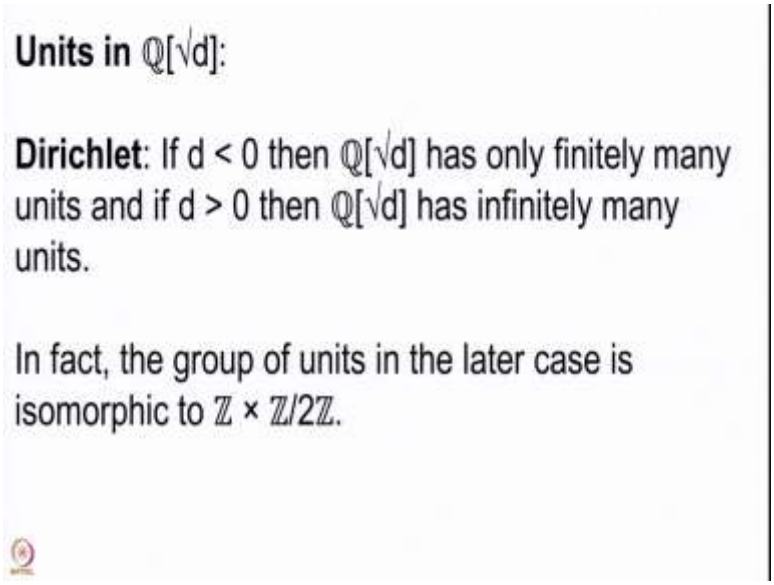
You are looking at the ring of algebraic integers in that field of algebraic numbers and there we describe the units that is the theorem of Dirichlet, but when applied to this particular specific

case, it gives a simpler description that whenever your d is negative then there are only finitely many units. So this is an instance that we will talk about d being negative, further if you are d is positive then Q root d has infinitely many units.

So, this is a very nice dichotomy that we have whenever d is negative, there are only finitely many units and whenever d is positive there are infinitely many units and we will see this in our now following part using only very basic theory, so Dirichlet theorem for quadratic fields can be proved by bare minimum.

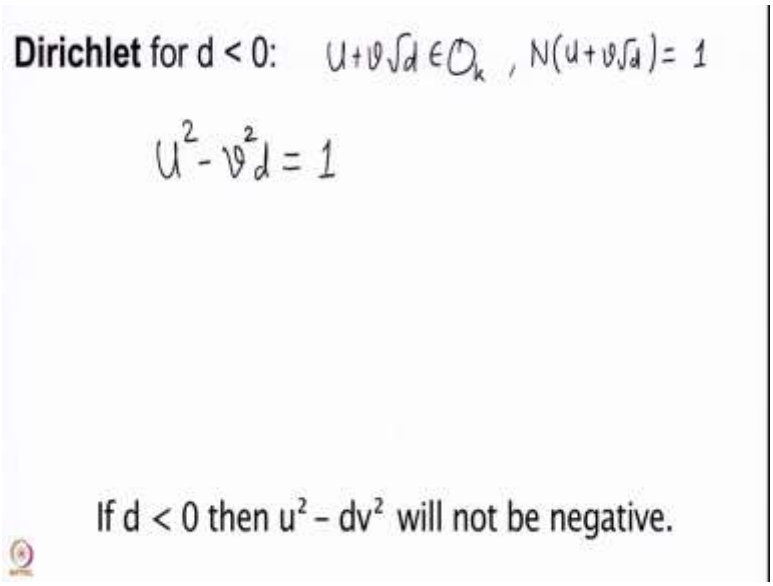
So, let us see what it involves note that the norm has to be 1 or minus 1, so we are looking at something which is of the form u plus v root d, where u and v are either integers or half the integers and then you are looking at u square minus v square d to be 1 or minus 1, this is the thing that we are looking at.

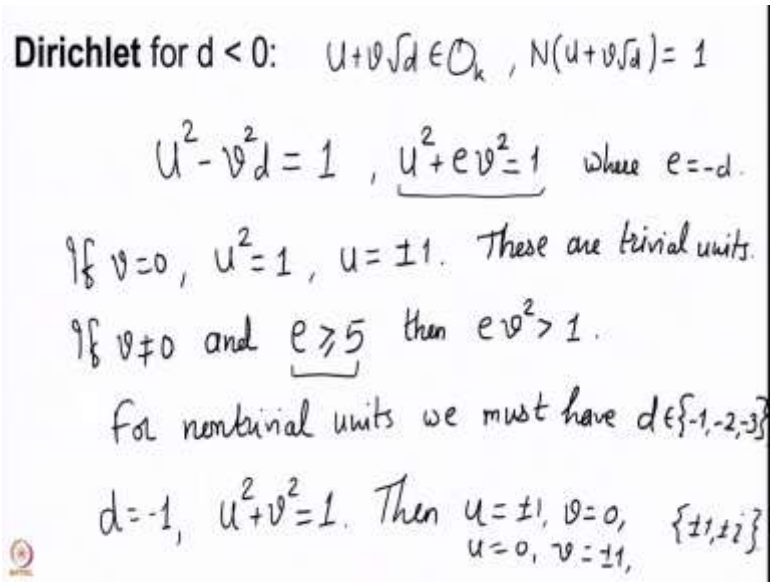
(Refer Slide Time: 20:35)



In particular when you have d to be positive then the group of units in fact can be explained and it is isomorphic to this group called Z cross Z by 2Z. So, this second statement is also something that we will see.

(Refer Slide Time: 20:50)





Let us, start with Dirichlet theorem for d less than 0, we are going to describe all elements of the form u plus v root d in O k, so there is the natural condition on u and v with the property that norm is equal to 1, so we are looking at solutions to u square minus v square d equal to 1 and remember d is negative, so we have u square plus e times v square equal to 1, we are looking at e equal to minus d.

So, these are the solutions that we want to describe. Now, notice that u and v are integers, so if you have that your v is 0 then we get that u square is 1 which gives that u has to be plus or minus 1, these are called the trivial units. After all 1 is always a unit and minus 1 is also a unit, so the

units 1 and minus 1 will always come in the group of units, whatever field you take and then the ring of algebraic integers in that field you take 1 and minus 1 will always show up, so they are called trivial units, we want to describe the non-trivial units.

So, we will not consider this case, therefore we are going to look at v not equal to 0, if v is not 0 and suppose that your e is bigger than or equal to 5, remember we are taking e to be an integer over d and e these are integers, d is negative, so e is positive and moreover e is square-free, therefore this is the same case as e bigger equal 4, but let us assume that e is now bigger equal 5, then ev square is bigger than or equal to 5.

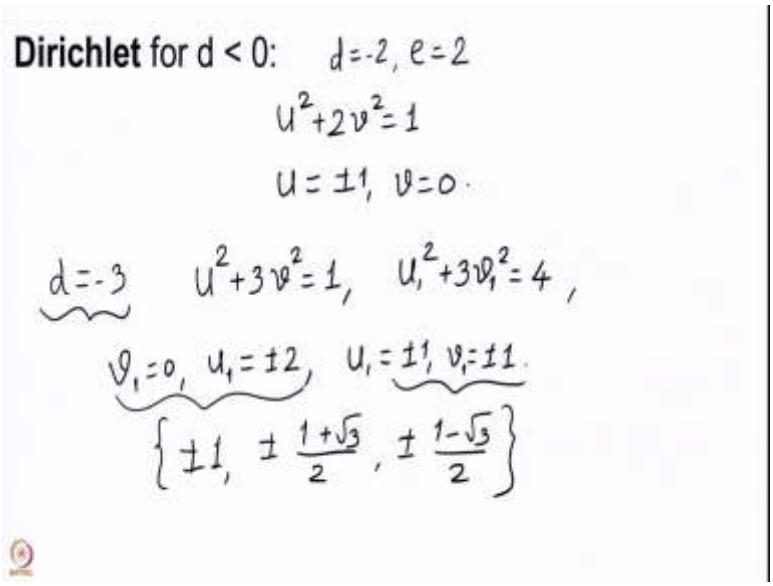
Because v is an integer, then ev square is strictly bigger than 1, because v is either an integer or it can be a half integer depending on what the discriminant does. So, v square will be simply possibly an integer or it can be a square of an integer divided by 4. So, you have if e is bigger equal 5 you are multiplying 2 a square of an integer by 5 by 4 and the v is non-zero, so v square is a non-zero square.

Therefore the product is strictly bigger than 1, in that case we will never have a solution to u square plus ev square equal to 1. So, if you want to have a non-trivial solution, so for non-trivial solutions for non-trivial units we must have d to be either minus 1, minus 2, or minus 3 these are the only possibilities for d to have a non-trivial unit, in all other possibilities for d the only possible solutions are plus minus 1 which is a finite set.

Remember what we want to prove is that whenever d is negative the group of units is finite that is what we want to prove. So, now let us take the case where d is minus 1, so we are looking at solutions to u square plus v square equal to 1, u and v are now integers because minus 1 is not congruent to 1 mod 4, so the algebraic integers for this d are of the form integer plus integer into root of minus 1.

So, u v are integers and therefore the only possible solutions are where u plus u is v plus minus 1 v is 0 or u is 0 and v is plus minus 1. So, these are the units which are plus minus 1 and plus minus I, we i is a chosen square root of negative 1. So, we have an explicit description of units when d is minus 1 which is plus minus 1 plus minus i.

(Refer Slide Time: 26:06)

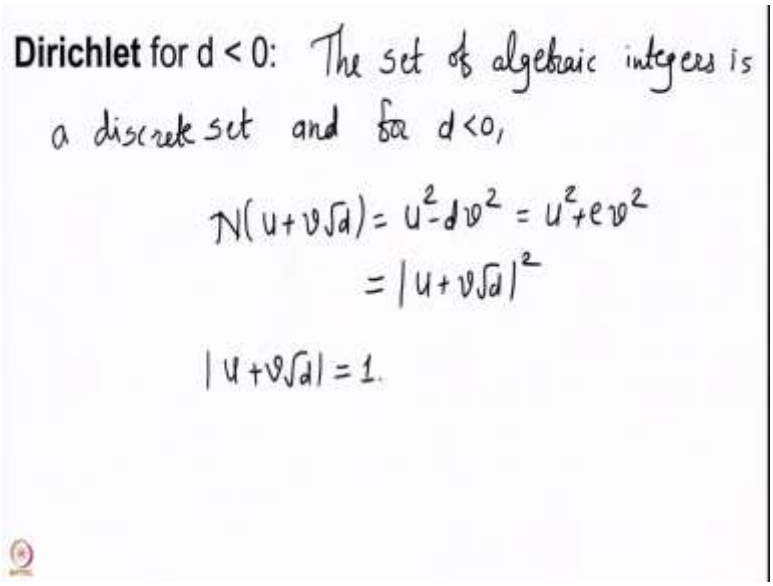


And now we go to d equal to minus 2, d equal to minus 2 or what is same as e equal to 2, then we are looking for solutions u square plus 2v square equal to 1, once again d is minus 2 it is not congruent to 1 mod 4, so u and v are integers and the only solutions are where u is plus minus 1 and v is 0. If your v is non-zero then 2 times v square will take you beyond, u square is also positive, so u square plus 2v square equal to 1 has no solutions.

Now, we come to an interesting situation where d is minus 3, now this is congruent to 1 modulo 4, so your u and v can be integers or they can be half of integers. So, when we are looking at solutions to u square plus 3v square equal to 1, we write u as u1 by 2, v as v1 by 2 and take the 4 and put it on the other side, so we are looking at solutions to u1 square plus 3v1 square equal to 4.

And u1 v1 are now integers and now you can easily see that this has solutions if your v1 is 0, u1 has to be plus or minus 2 or you can have u1 equal to plus minus 1 and v1 is also plus minus 1. But ofcourse this does not give you the solutions when you have too many u1s and too many v1s, so the set of solutions here is actually plus minus 1, plus minus 1 plus root 3 by 2 and plus minus 1 minus root 3 by 2, you get four solutions here and you get two solutions here. So, these are the 6 solutions and these are the only 6 solutions.

(Refer Slide Time: 28:22)



In fact, we should note the following thing that the set of algebraic integers is a discrete set and for d negative norm of u plus v root d, which is u square minus d v square, d is negative, so this becomes u square plus ev square this is actually the square of the modulus as a complex number, so when you are looking at a discrete set of the set of algebraic integers and you are looking at solutions to the usable mod to be 1, then you are looking at the unit circle in the complex plane.

So, you have on one hand the unit circle, which is a compact set in mathematical language and then you have a discrete close subset of this compact set and this is a slightly basic but on the advanced part of mathematics called topology that any discrete compact set has to be finite. So, this is the basic thinking behind this theorem that whenever you take such a field then the set of units in this has to be a finite set.

So we have described this set of units for d negative, we are going to describe this set of units for d positive in our next lecture and we will see how the continued fractions are used in giving the explicit description for these units. So, see you then. Thank you very much.