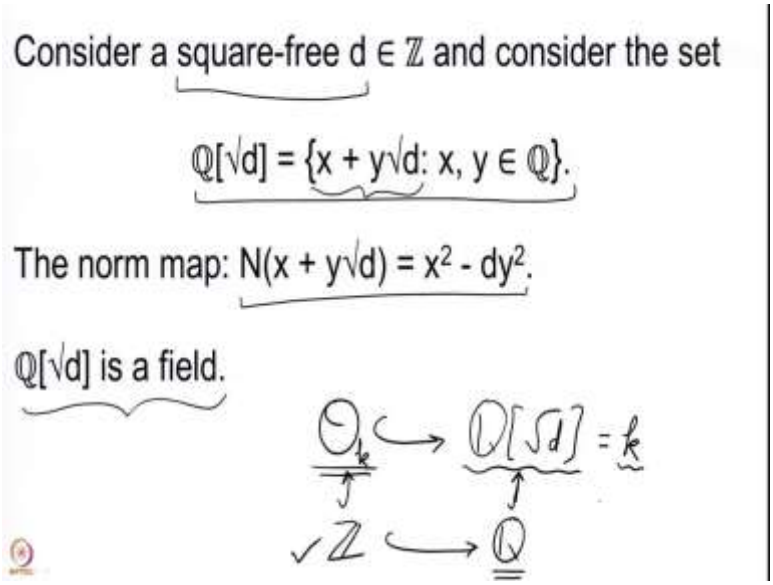
A Basic Course in Number Theory
Professor Shripad Garge
Department of mathematics
Indian Institute of Technology, Bombay
Lecture 61
Units in Quadratic Fields: The Real Case

(Refer Slide Time: 00:32)



Welcome back, we are studying the quadratic extensions of Q and what are called the units in Q, so the quadratic extensions of Q we defined them in the last lecture these are the sets Q root d where d is a non-square natural number, these are the sets Q root d where d is a non-square number, but we often take it to be a square free number because when we take the set Q root d in the sense that we take the elements x plus y root d then it is enough to take the ds which are square free, that means there is no square dividing the d.

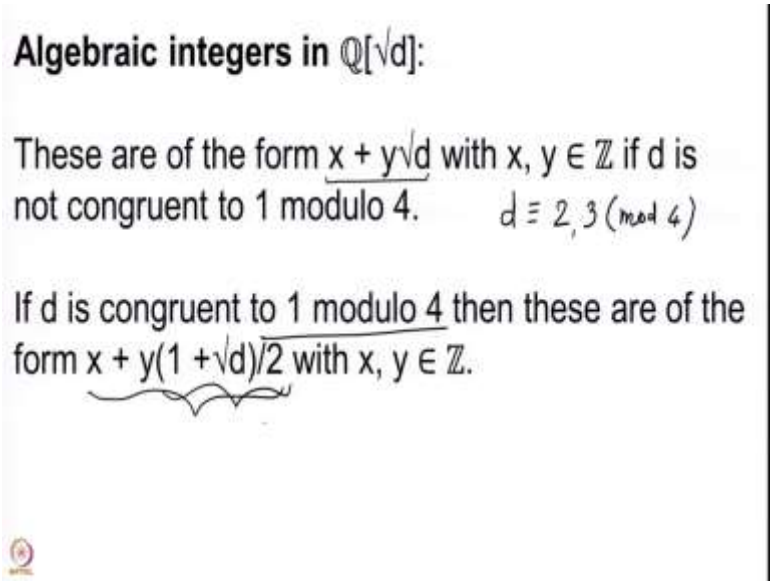
We saw that there is this norm map defined on any such ring, any such set this is the ring because we have addition defined on the set, we have multiplication defined on the set, the addition gives you a group structure and multiplication is associative, multiplication has identity and multiplication has distributivity property with the addition.

So, this is what is called a ring and moreover with the help of the norm we also see that this is actually a field that means any non-zero element in this set is invertible with respect to the multiplication. So, you can divide by any non-zero element in the set Q root d and you will still be in the set Q root d. So, in some sense the elements in Q root d behave like the rational

numbers. And then we saw that just like we have the integers sitting in rational numbers there are these algebraic integers sitting in Q root d.

So I may have told you that this is in fact a more general construction if you look at Q root d, this is something like Q and we have Z sitting here inside Q, then there is a ring called O k, which is sitting here where you call this field to be k and we have this kind of what is called a commutative diagram. It is also a nice diagram in the sense that the intersection of these two O k and Q is precisely Z, so this is a very nice diagram and it holds not just for Q root d but also for a general finite extension of Q.

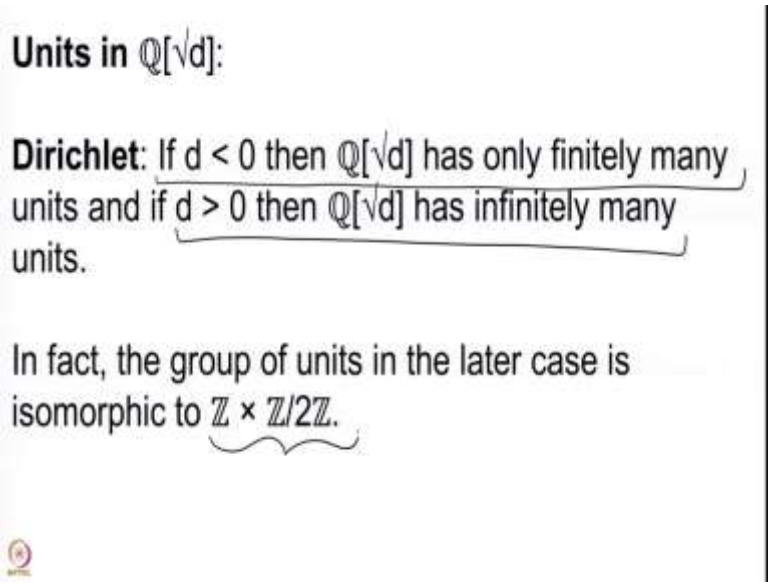
(Refer Slide Time: 03:05)



But when we look at Q root d, we saw that there is a nice description of algebraic integers in Q root d, the description is given by the elements have the form x plus y root d where x and y are integers provided that d is not congruent to 1 modulo 4, so here d is congruent to 2 or 3 modulo 4 and here we have that d is congruent to 1 modulo 4, then we have noticed that 1 plus root d by 2 is also an algebraic integer that also satisfies a monic polynomial over integers.

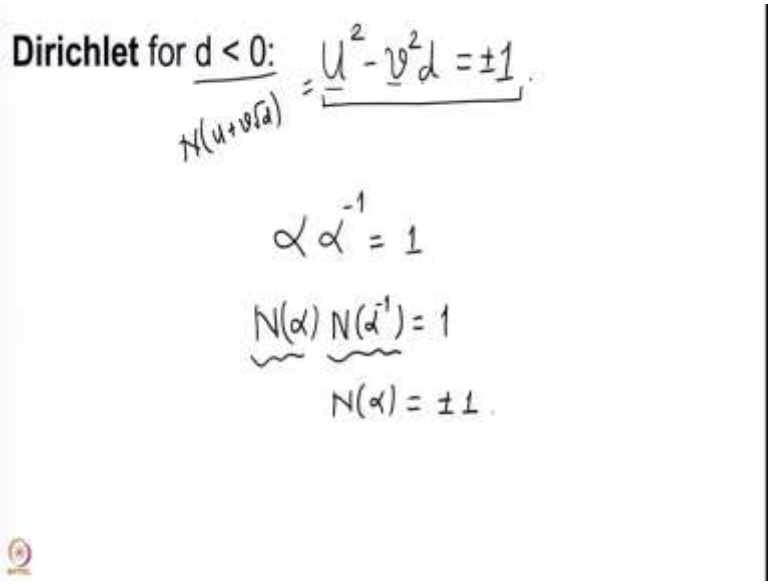
And therefore a general element is of the form x plus y into this 1 plus root d by 2, where now x and y are integers or you may call them as u plus v root d where u and v are integers or half integers. So, this is the description for algebraic integers and clearly here every element need not be invertible, you know we have 2 in the algebraic integers and you cannot divide by 2.

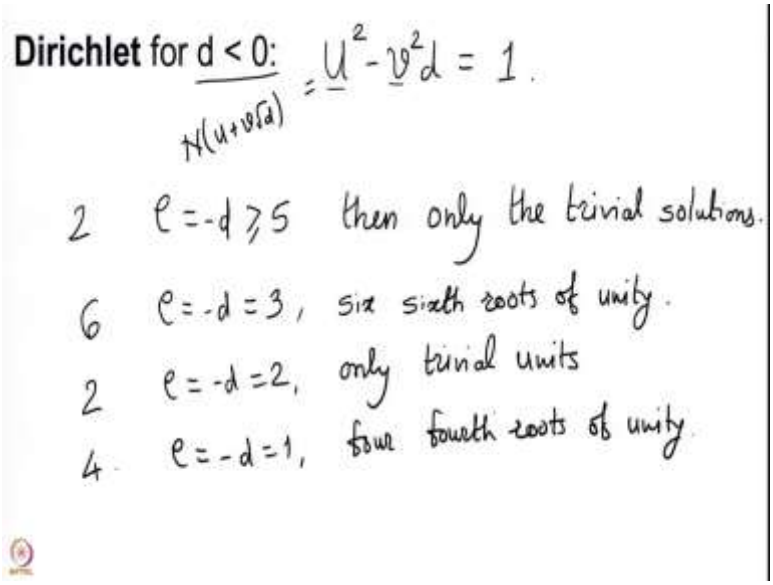
(Refer Slide Time: 04:25)



So, the question is what are the units in Q root d and there was this nice result of Dirichlet which we had in the last lecture which described units Dirichlet theorem once again describes units in all O k, it gives you some kind of description for the group of units, in particular when we are looking at quadratic extensions this has a very nice simple statement that for negative d there are only finitely many units and for positive d there are infinitely many units and in fact you have that the group is of the form Z cross Z by 2Z, so it is an infinite cyclic group direct product with the group of order 2.

(Refer Slide Time: 05:03)





We saw the proof for d less than 0 already there were the possibilities that we looked at, so we looked at the solutions to u square minus v square d equal to 1, this is the formula for norm of u plus v root d. Notice that in fact we could had this norm to be plus or minus 1, we have noticed that when u is a unit its norm is a unit in Z, because if alpha is a unit then there is an alpha inverse also in O k such that this product will give us 1 and therefore norm alpha into norm alpha inverse will give you norm 1 which is simply 1.

And these are both integers, so you have product of 2 integers equal to 1 then both the integers will have to be either plus 1 or both will have to be minus 1. So, therefore this u square minus v square d can be plus or minus 1. But if your d is negative, which is what we have assumed then u square plus v square into minus d are all positive numbers and their sum cannot be negative.

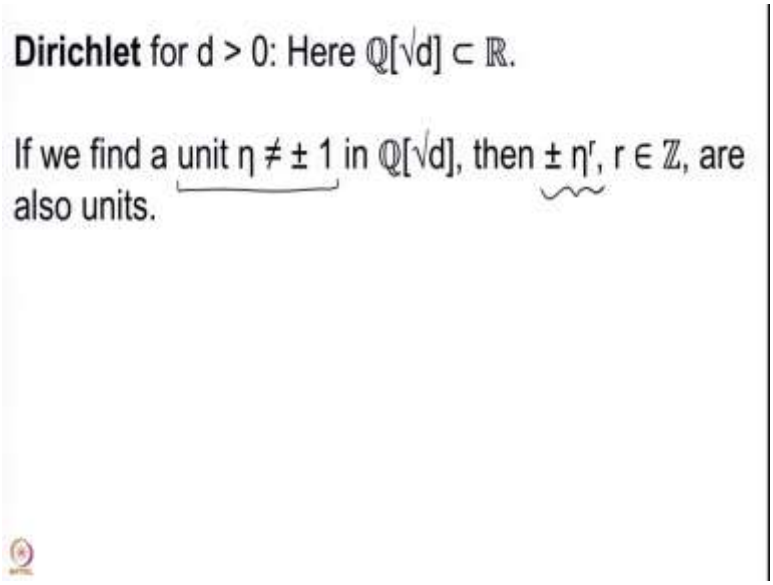
So, what we then get is that this was only going to be plus 1 and so we have to only solve the equation u square minus v square d equal to plus 1 where d is a negative number. We observed that e which is negative d if this is bigger than or equal to 5 then only the trivial solutions are the plus and minus 1, which are units inside they are the units in O k also always.

And in these cases e equal to minus d bigger equal 5, these are the only solutions, e equal to 4 will not happen, if you take e equal to 3 which is negative of d then there are six sixth roots of unity, which will come and these are the units, if you have e equal to 2 only trivial units and finally if you take e equal to 1 then the four fourth roots of unity.

So, in all these cases we see that the group is finite, here we have that the cardinality is 2, here it is 6, here it is 2 and here it is 4. In all these cases we can actually write down the explicit group of units and therefore we have a very easy proof for Dirichlet theorem in the case of the quadratic fields. Next we go to the positive d.

So, if d is positive square root of d is a real number, when d was negative the square root of d was an imaginary number, here the square root of d is a positive real number and therefore the field Q root d remember we are taking x plus y root d where x and y are rationals and now root d is a real number, so everything of the form x plus y root d is going to be a real number.

(Refer Slide Time: 09:01)



So, Q root d is going to be a subset of the real numbers. It is not something which is contained in the complex plane outside real numbers. It has no elements outside the real numbers. Q root d is completely contained in real numbers, it is a very nice thing to try and imagine how all these points are located, how these points are distributed in the real line, but I will leave it to you to think about it, but at least we start with this observation that Q root d is contained in R.

So, what does it mean? It means that if you are looking at roots of unity, if you are looking at complex numbers which are all finite order, which are say something like omega where omega power n is 1 for some n, then the only such elements which are contained in R the real line R plus and minus 1, so the only units of finite order, finite order means that the unit to the power a

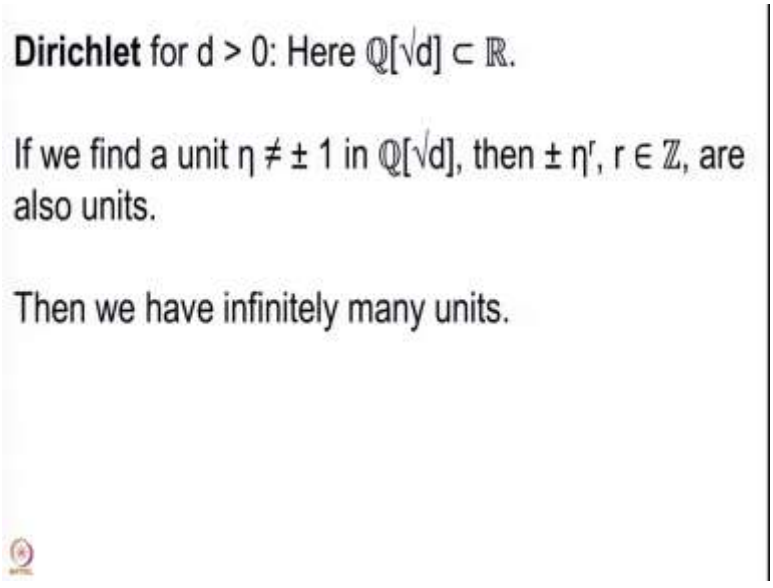
finite quantity finite number gives you 1, so the only units of finite order in such Q root d are plus and minus 1.

So, the only trivial units are the units of finite order. Now, if you show that there is a non-trivial unit, so if we find an eta a unit eta which is not equal to plus minus 1, then we will have a non-trivial unit, then this unit has the property that eta power R is never 1, for any R other than 0. So, you will have the eta power R, so you will take eta, eta square, eta cube up to the power 4 and so on these are all going to be distinct elements.

Because if you have say a and b which are not the same, but eta power a is eta power b, then you will look at the smallest among the a b and cancel that part out, you will get that eta power the difference of a and b is 1, that is a contradiction because eta is not equal to plus minus 1 and the only elements of finite order in Q root d are plus and minus 1, so you cannot be a finite order.

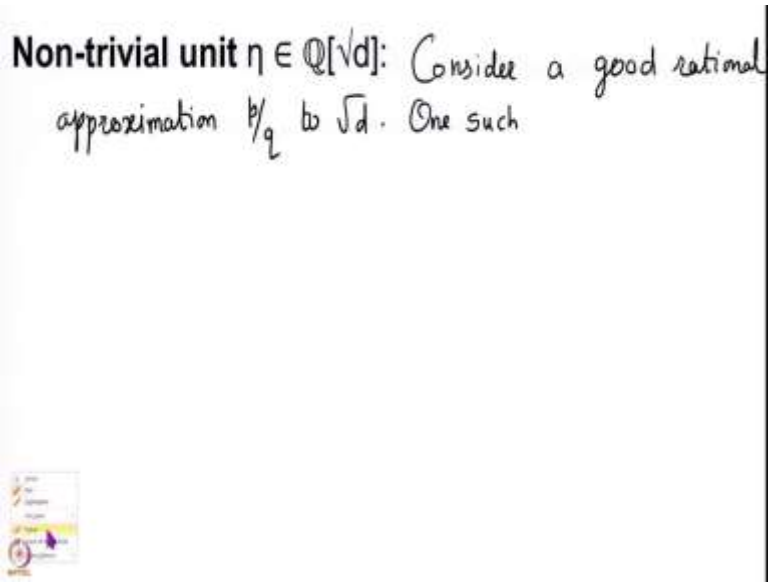
So, all these eta power are these are all distinct elements, their negatives will also be units, they will also be infinitely many, so in fact we have that the plus minus eta power R, these are all going to be units, so in a sense this is proving if you find a non-trivial unit, then we would have proved Dirichlet theorem for d bigger than 0, because Dirichlet theorem said that the set is finite if d is negative and its infinitive if d is positive.

(Refer Slide Time: 12:25)



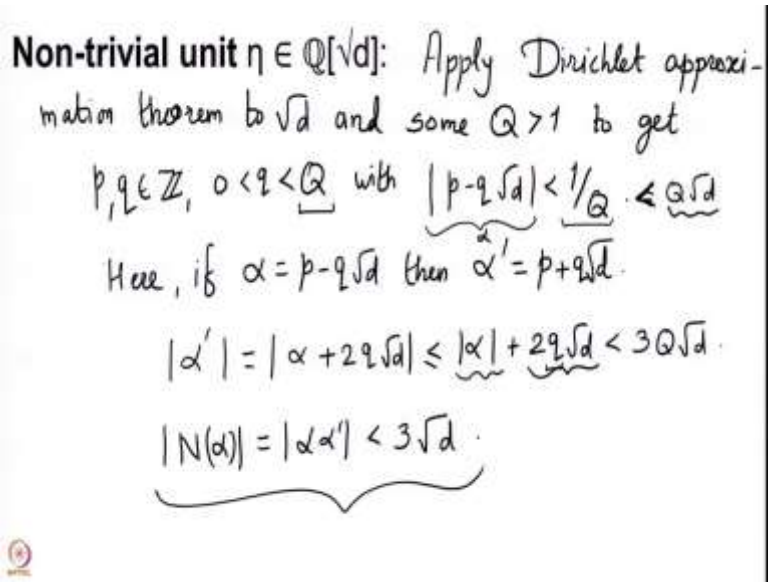
So, if you find the non-trivial unit you are going to get infinitely many units. So, our aim is now to find a non-trivial unit in Q root d, where d is positive, that is what we now plan to do.

(Refer Slide Time: 12:45)



So, consider a good rational approximation p by q to root d, remember we had the Dirichlet theorem which gave us one such approximation, so one such can be obtained or let us just applied Dirichlet theorem.

(Refer Slide Time: 13:54)



Apply Dirichlet theorem approximation theorem to root d and some Q bigger than 1 to get p q in integers the denominator is between 0 and capital Q with mod p minus q root d to be less than 1 upon Q. So, here if alpha is p minus q root d, then it's conjugate alpha prime has the form p plus Q root d. Now, we want to get some bound on the norm of alpha, but the norm of alpha is the

product of alpha and alpha prime, we have some bound on the modulus of alpha, the bound on alpha prime is going to be this is p plus q root d, so this is simply obtained as alpha plus 2q root d.

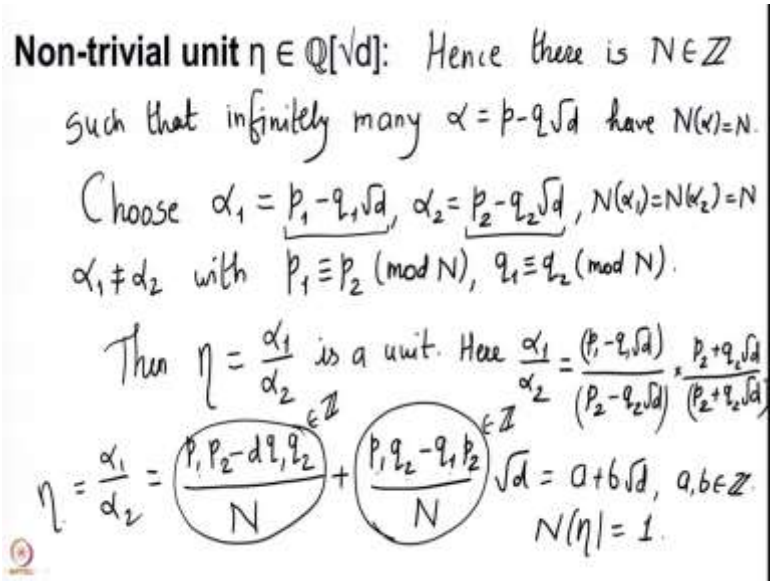
Therefore this modulus is less than or equal to mod alpha plus 2q root d, we do not have to put a mod for Q root d because root d is taken to be the positive root and Q is anyway a positive quantity, here we see that this is alpha its mod is less than 1 upon Q the small q has the property that it is less than capital Q, so we get that this whole thing is than 3 Q root d.

So, alpha prime mod of alpha prime is less equal mod alpha first of all plus 2 q root d now 2q root d is less equal to strictly less than 2 capital Q less d, root d, 2q root d is less than 2 capital Q root d and mod alpha which is less than 1 upon Q is certainly less than or equal to Q root d, because Q root is something which is bigger than 1 and this is something less than 1, so in fact you have a strict inequality here.

So, we get a strict inequality to be this mod alpha prime to be less than 3Q root d, so taking the product we get that norm alpha which is alpha-alpha prime, this is less than 3 root d. So, whenever we have any good approximation p by q to root d, the p minus q root d is going to have norm to be less than 3 times root d.

But we know that root d is an irrational number, so there are infinitely many p by q, which are going to give us good approximations to root d. And so there are infinitely many norms, but the norm is an integer and its modulus is bounded by 3 root D, so there are only finitely many possibilities for the norm, which means that there will have to be a one value of norm for which you will have many infinitely many p by q such that the corresponding p minus q root d gives you the value to be that particular norm.

(Refer Slide Time: 18:01)



So, hence there is an integer such that infinitely many alpha equal to p minus q root d have norm alpha equal to N, we have that there are infinitely many pairs p upon q giving you good approximations to root d and ofcourse p1 minus q1 root d equal to p2 minus q2 root d if and only if p1 is p2 and q1 is q2.

So, whenever you have infinitely many pairs p1 comma pi comma qi giving you the good approximation then the corresponding alphas will be all distinct. So, you have infinitely many alphas having norm among a finite set of possibilities, so there has to be one possibility among those finitely many which is achieved by infinitely many alphas.

Therefore you have infinitely many alpha achieving this possibility, further we can do the following, let me write this statement. So, choose alpha 1 to be p1 minus q1 root d, alpha 2 to be p2 minus q2 root d, norm alpha 1 equal to norm alpha 2 equal to N, ofcourse we have that alpha 1 is not alpha 2, so this can of course be done, we have infinitely many alpha having this norm equal to N, so we can certainly choose two distinct ones among that infinite set.

But we want to do something more with p1 congruent to p2 modulo N the same capital N and q1 congruent to q2 modulo the same capital n. Why can we do this? Because the congruence classes modulo capital N are again, finitely many. So although you may be taking pairs ultimately you have a finite set of possibilities for congruence classes and so once again there has to be one

particular pair of classes where you have infinitely many distinct elements achieving that particular class.

So, you can choose two distinct elements alpha 1 alpha 2 with the property that alpha 1 is not alpha 2 but the rational part the p's are same modulo N, the root d part the coefficient of root d are same modulo N and you also have that the norms are both equal to the same capital N, this is something that we can do then I claim that eta which is alpha 1 upon alpha 2 this is a unit.

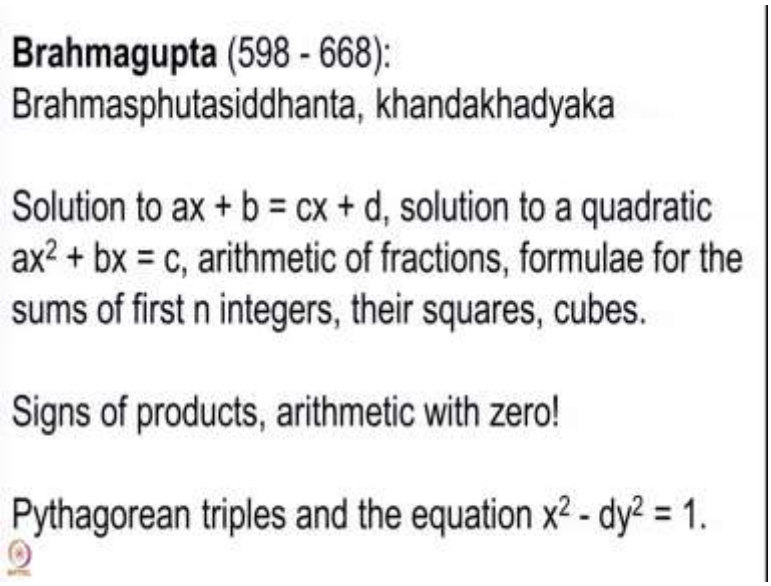
So, this is clearly a unit because it's norm is 1, norm alpha 1 upon norm alpha 2, which is N upon N this is 1, if you can prove that eta is again an element in the ring of integers, if we can prove that eta is in fact an integer plus integer times root d then we are done, anything in the ring of integers whose norm is 1 has to be a unit.

So, we simply compute alpha 1 upon alpha 2, so alpha 1 is p1 minus q1 root d, alpha 2 is p2 minus q2 root d, so this is alpha 1 which is this is p1 minus q1 root d upon p2 minus q2 root d, but we simplify this by multiplying by the conjugate of the denominator on both sides the numerator becomes p1 p2 minus d q1 q2 and we have the root d coefficient which is p1 q2 minus q1 p2 root d I will write the denominator separately for both and the denominator is p2 minus q2 will be into its conjugate, so I am going to get the norm.

Now, this norm so since p1 is congruent to ps2 mod N and q1 is congruent to q2 mod N we have that p1 q2 is congruent to q1 p2 modulo N and therefore this is an integer. Similarly, p1 p2 minus d q1 q2 modulo N this is same as p1 square minus dq 1 square, but p1 square minus dq 1 square is the norm of alpha 1 which is N, therefore the numerator is equal to N modulo N, so it is divisible by N.

So, we have that this member is also in Z, therefore we have that this has the form a plus b root d where a and b are integers and norm of this eta is 1. So, we have proved that there is a non-trivial unit in Q root d, so this non-trivial unit must give rise to infinitely many units in Q root d. So, we have proved the Dirichlet theorem in this particular case, let us just go to one bit of history.

(Refer Slide Time: 24:44)



So, we have Brahmagupta from the known accounts, he is from the 5^{th}, 6^{th} and 7^{th} century; CE, he was a very influential Indian mathematician, in fact he is main interest was in astronomy, but he did lot of work for arithmetic and algebra also, he is well known for having written these two books. So, the first book is called the Brahmasphutasiddhanta and second is called Khandakhadyaka.

So, it's two books are called Brahmasphutasiddhanta and Khandakhadyaka, Brahmasphutasiddhanta the literal meaning is that Brahma is the knowledge and sphuta is explained and siddhanta is the theory, so this is the theory that is explained in this book, but this book apparently turned out to be too tough for people to read and so on, so then later quite long time after he wrote this another book called Khandakhadyaka which basically means edible bytes.

So, this was this second book was of consisted of the material which people could easily follow and so on, Brahmagupta was well known for several things in mathematics. He is the first one who gave this solution to the general linear equation. So, he is the first one to solve ax plus b equal to cx plus d, he gave a method to solve this equation, he is the first one who described the solution to the quadratic equation ax square plus bx equal to c, he is also the first one who described the arithmetic of fractions, what would be the formula for say p by q plus a by b.

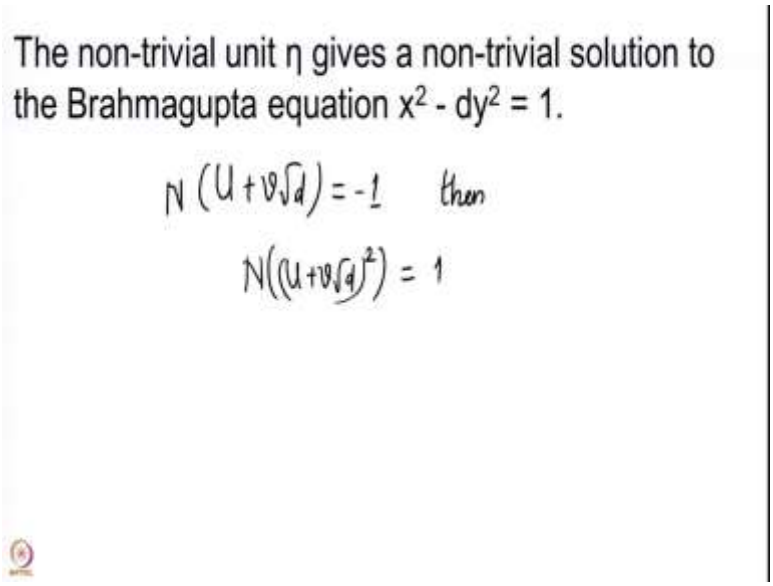
He is the first one to have explicitly written this formula in terms of the variable. So, he would treat p by q as p by q, a by b as a by b and then he wrote down the formula which you could apply to any general fraction. He was the first one who wrote down the product formula and so on so, so you know for us these things might seem very easy, but somebody had to note them and write them down for the first time and Brahmagupta has done that.

He is also the one who gave the sum of first n integers, the sum of squares of first n integers there the sum of their cubes and so on. He is also well known for describing the science of the products, he was the one who noticed that if you take two negative numbers and take their product you get a positive number, he is the one who noticed that positive into negative is negative.

He is the one who introduced the arithmetic with 0. And if you are still not impressed by his work, he is the one who also described Pythagorean triples, he is the first one to have described them and ultimately he also solved this x square minus dy square equal to 1. He was the one who wrote down solutions for this, he devised a method for describing this and his method was similar to what we have seen in the proof of Lagrange's theorem.

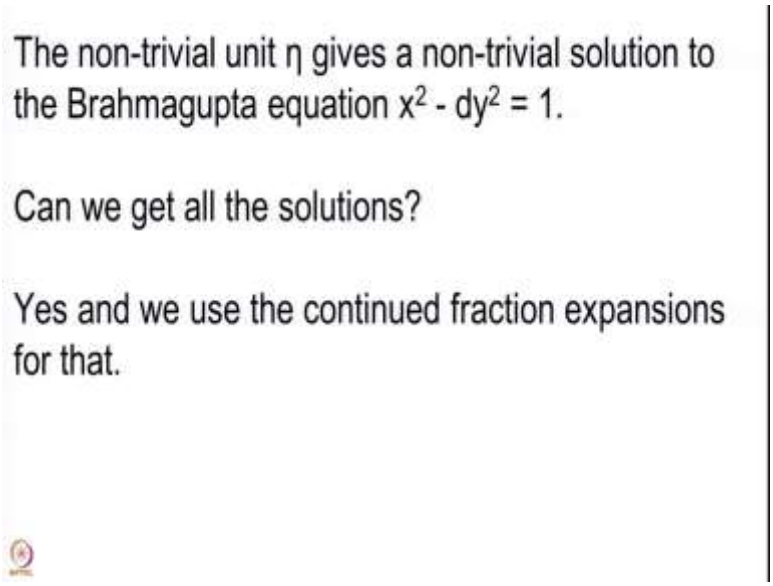
And also in the proof when we describe this numbers which sums of two squares. We observed that those binary quadratic forms are actually multiplicative that was observed by Brahmagupta for the norm form. He observed that this form x square minus dy square is multiplicative and he used that to write down the solutions. So, how is this relevant for us now?

(Refer Slide Time: 28:35)



A non-trivial unit eta will give you a non-trivial solution to x square minus dy square equal to 1, this is because your unit will have norm which is either plus 1 or minus 1, if your u plus v root d norm is if the norm is plus 1 then you have the solution to the Brahmagupta equation, if the norm is minus 1 then norm of the square is going to be plus 1, if eta which is u plus v root d is a non-trivial unit, its square is also non trivial that cannot be trivial now because then you eta will have finite hoarder. So, it has square will give you a non-trivial solution to the Brahmagupta equation.

(Refer Slide Time: 29:33)



So, the question is then can we get all solutions to Brahmagupta equation. Can we get all solutions to x square minus dy square equal to 1? And the answer is yes, we can get all the solutions, we are going to use the continued fraction expansion for obtaining these solutions, we will do this in our next lecture, which is going to be our penultimate lecture, we will give an explicit solution to the Brahmagupta equation the x square minus dy square equal to 1, there is a related form x square minus dy square equal to minus 1 we will also indicate the solution to that but we will not prove that solution in detail, so I hope to see you in that management lecture also. Thank you very much.