

A Basic Course in Number Theory
Professor Shripad Garge
Department of Mathematics
Indian Institute of Technology, Bombay
Lecture 62
Brahmagupta-Pell Equations

Welcome to the penultimate lecture of our course, we have been discussing units in quadratic extensions of rational numbers. We saw the proof essentially of Dirichlet theorem in the case of the quadratic extensions in our last lecture, where we proved that the field $\mathbb{Q}(\sqrt{d})$ where d is positive will have infinitely many units, we are yet to ofcourse, prove the explicit structure of the group of units which is what we intend to do today.

And we also want to describe all these units using continued fractions for root d basically, we are going to look at convergents of root d and these convergents will give us the solutions to the famous Brahmagupta equation. And before going to the Brahmagupta equation, we want to go to what is known as the fundamental unit.

(Refer Slide Time: 01:19)

The fundamental unit η : Units in $\mathbb{Q}(\sqrt{d})$ is an infinite set. Let $A = \{\eta : \eta \text{ is a unit in } \mathbb{Q}(\sqrt{d}), \eta > 1\}$. Then $A \neq \emptyset$, in fact, $\text{Units} = \pm A^{\pm 1}$.
 If $\eta \in A$ is of the form $\eta = u + v\sqrt{d}$ then, $\eta^{-1} = \eta' = \underline{u - v\sqrt{d}}$, then $v > 0$. Also $u > 0$.
 Call the smallest element of A by η_0 .

So, we observe that units in $\mathbb{Q}(\sqrt{d})$ is an infinite set, this is something we have observed in our last lecture, let A be the set of units, we consider those units which are bigger than 1. So this is a set of units is it an empty set or is it a non-empty set. So, we observe that if you have units, the units will be either positive or negative. Since you have that 1 and minus 1 are always units, we call them the trivial units in $\mathbb{Q}(\sqrt{d})$.

So, whenever you start with any non-trivial unit, if that non-trivial unit is negative, you can multiply it by minus 1 and then you get a non-trivial unit which is positive. So, we have now

a non-trivial positive unit, the only trivial positive unit is 1. Since our unit η which is now a positive unit is non-trivial, η cannot be 1.

So, the possibilities are that η less than 1 or η is bigger than 1. If η is bigger than 1, then it is in the set A , so A is non-empty. If η is less than 1, we will take 1 upon η , 1 upon η has to be bigger than 1 η is positive. So, its multiplicative inverse is also a positive. Remember from the times of Brahmagupta we know that if you have a negative number and you multiply by that to a positive number you will get a negative number.

So, your η if that is positive, its inverse should also be positive. And therefore, whenever η is less than 1 the inverse is bigger than 1. So, in any case, we have that A is a non-empty subset. In fact, the whole set of units is expressed by elements in A by taking the plus or minus 1 power of elements in A and putting a plus minus sign outside.

So, then A is non-empty. And in fact, the units is equal to plus minus A to the power plus minus 1 this is a way to denote that any unit has to be plus or minus η or η inverse where η is in A this is what we mean. So, in some sense, A contains about one fourth of the units. Whenever you have any unit in A , you get three more units you will get. So, if you start with η an element in A then you will have 1 upon η , you will have negative η and negative 1 upon η .

So, you get four different units starting with 1 unit in A and then you have the two trivial units plus minus 1 which will give you the whole set of units in $\mathbb{Q}(\sqrt{d})$. We also noticed that the units are of the form $u + v\sqrt{d}$ where u and v can be integers or half the integers. So, let us see what are the conditions on u and v .

If this is of the form $\eta = u + v\sqrt{d}$ then η inverse is η conjugate because norm of a unit is 1, and the conjugate is $u - v\sqrt{d}$. Now, η is bigger than 1, so its inverse is less than 1. So, this u prime is less than 1, this implies then v has to be a positive number, v cannot be 0 because if $v = 0$ the only interior unit is going to be plus minus 1. But we have something which is bigger than 1. So, v is non-zero, we could be either positive or negative.

But here we have that $u - v\sqrt{d}$ is less than $u + v\sqrt{d}$. So, cancelling u , we get that $-v\sqrt{d}$ is less than $v\sqrt{d}$, so v has to be positive. Now, v is positive, what about u ? Is u positive or is u negative? If u is negative, then η prime will be a negative number because now our v is positive, so negative v is a negative number. And if your u is

also negative, then it tells you that you have η prime to be a negative number, which is also not possible, because if you have something bigger than 1, it is a positive number, its inverse should also be positive.

So, also, u is bigger than 0, can you have u equal to 0, what we could have here is that u is bigger than or equal to 0, if you have u equal to 0, your unit looks like v into root d and to have v into root d multiplied by some element again into the algebraic integers or you would have that the norm is equal to plus minus 1 that tells you that minus $d v$ square is plus minus 1 and these can happen if your d is positive, then minus $d v$ square can be negative.

And so, only for d equal to 1, you have a possibility of having the solution, but 1 is not considered a square for interior, we are not considering d equal to 1. So, therefore, u equal to 0 is not a possibility. So, what we have obtained is that if you take a unit η in A , then its integral part, so, if you write it as u plus v root d , then u is positive and v is also positive.

Moreover, we know that these u and v are integers or half the integers. So, once you start from 1 and u and v are both positive integers or half integers, you will start from 1 by 2 plus 1 by 2 root d , 1 by 2 plus 1 root d , 1 plus 1 by 2 root d , 1 plus root d . And then you will increase but you have these finitely many possibilities for the smallest possible possibilities for u and v .

Therefore, you have, therefore we can find the smallest element in capital A , it is important to note that just because you have a set of elements of the form u plus v root d where u and v are integers does not mean that you will always find the smallest set of smallest element in such a set. What we have is that the u and v are not just integers, not just half the integers, but they are both positive. So, since you have both of them positive, there is a smallest possible such unit call that η naught call the smallest element of A by η naught.

(Refer Slide Time: 10:07)

The fundamental unit η : $\forall \eta_1 \in A$ then $\exists n \in \mathbb{N}$
 such that $\eta_0^n \leq \eta_1 < \eta_0^{n+1}$. Here we get
 $1 \leq \frac{\eta_1}{\eta_0^n} < \eta_0$. Then $\eta_1 = \eta_0^n$.
 All units in $\mathbb{Q}[\sqrt{d}]$ are $\pm \eta_0^n, n \in \mathbb{Z}$.
 Thus this group is isom. to $\mathbb{Z}_2 \times \mathbb{Z}$.

Now, η_0 is a unit. So, all positive powers of η_0 are units and these powers will certainly go to infinity because η_0 is bigger than 1. So, the powers will go to infinity if η_1 is any unit in A then there is a natural number small n such that η_0^n is less than or equal to η_1 less than or equal to η_0^{n+1} . η_0^n and η_0^{n+1} are going to infinity and η_0 was the smallest element in A .

So, there will be an n such that the powers of η_0 up to that end are less than or equal to the η_1 that you have fixed but the $n+1$ power and also the $n+2$ and so on will go beyond η_1 . So, we take that largest such integer so that we call that integer is called n , okay. Now, here η_1 is a unit η_0^n is a unit, we can divide throughout by the η_0^n .

So, here we get $1 \leq \frac{\eta_1}{\eta_0^n} < \eta_0$ upon η_0^n less than η_0 , so our η_1 upon η_0^n , remember, η_1 is a unit η_0^n is a unit so all powers of η_0 are units, then this is definitely a unit. And this unit is now sandwiched between the number 1 and η_0 , if this number was not equal to 1, it would give you an element in A , because A is the set of all units bigger than 1.

So, if this number was not equal to 1, we would get that this would then be in A , but it then cannot be less than η_0 η_0 was chosen to be the smallest element in A . So, this contradiction says that whatever we have assumed here that it is not equal to 1 that cannot be true. So, therefore, we get that η_1 is η_0^n therefore, every element in A is a power of η_0 .

And then we can write down all units in A , all units in $\mathbb{Q}(\sqrt{d})$ are plus minus η raised to power plus minus n or you may just have it to be η^n where you let n vary over integers. This very special element is called the fundamental unit, it is the generator of the infinite cyclic group which with plus or minus will give you the set of all units.

So, this proves that the group of units is actually isomorphic to $\mathbb{Z} \times \mathbb{Z}$ by $2\mathbb{Z}$ the plus part and the negative part these correspond to the group \mathbb{Z} by $2\mathbb{Z}$ and then η is generating the infinite cyclic group. So thus the units, thus this group is isomorphic to \mathbb{Z} by $2\mathbb{Z}$ cross integers. So, we have proved Dirichlet theorem completely for the quadratic case and we have also obtained the fundamental unit η .

(Refer Slide Time: 14:29)

The fundamental unit η :

Example: $d = 2$. $u^2 - 2v^2 = \pm 1, u, v \in \mathbb{Z}$.

$u + v\sqrt{2}, \underline{u, v > 0}$.

$(1 + \sqrt{2})(1 - \sqrt{2}) = 1 - 2 = -1$.

The fundamental unit in $\mathbb{Q}[\sqrt{2}]$ is $1 + \sqrt{2}$.

$(1 + \sqrt{2})^2 = 3 + 2\sqrt{2}$ gives solution to $u^2 - 2v^2 = 1$.

Let us try to do an example, so we have d equal to 2 we are looking at remember we are looking at solutions to $u^2 - 2v^2 = \pm 1$. The u and v are integers because our d is not congruent to 1 modulo 4 when d is congruent to 1 modulo 4, you have that the u and v can be half the integers but here, u and v are integers. Integers, we have also noticed that when you look at the fundamental unit $u + v\sqrt{d}$, then both u and v are positive.

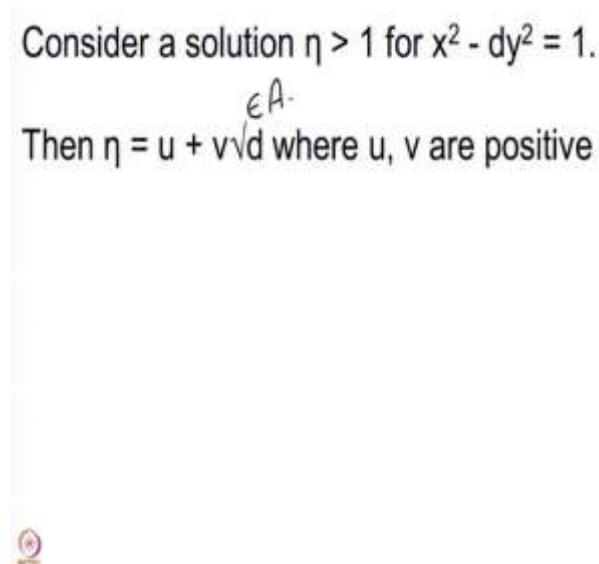
So, we should start with the first 1, which is 1 and 1. So, we will look at remember, our d is equal to 2. So, 1 plus (\sqrt{d}) root 2, root 2 alone is not a unit, we will look at 1 plus root 2 is this a unit, we multiply by its conjugate and we get this to be 1 minus 2 which is minus 1, (bravo) we obtained a unit and this is clearly the smallest unit if you have u and v to be integers which are positive, then u and v will be bigger than or equal to 1.

And clearly, the both u and v are positive, so, they will both be have to be equal to bigger than or equal to 1, so you get 1 plus root 2 to be the smallest element of the corresponding A . So, this is our fundamental unit, the fundamental unit here in $\mathbb{Q} \sqrt{2}$ is 1 plus root 2, its norm is minus 1. So, if you wanted to get something whose norm is plus 1, if you wanted to get a solution to the Brahmagupta equation, you have to now take the square of this 1 plus root 2.

So, if you take the square of this, it will be 1 square plus root 2 square, so you get 3 plus 2 times root 2 this gives solution to $u^2 - 2v^2 = 1$, here we had that this was a solution to $u^2 - 2v^2 = -1$. But now, we have a solution to $u^2 - 2v^2 = 1$, 3 square is 9, 2 square is 4, 2 times 2 square is 8 and 9 minus 8 is 1.

So, this is how for the simplest case, we have found the solution, but what now, we want to do is to find the solution in the general case. So, we are going to start with D to be a positive square free integer and we are going to write down the solutions to the Brahmagupta equation $u^2 - dv^2 = 1$.

(Refer Slide Time: 18:02)



So, we consider such a solution η bigger than 1 for $x^2 - dy^2 = 1$ then this η will be of the form $u + v\sqrt{d}$ where both u and v are positive this is something that we have already seen, such an η is going to be in the set capital A that we had defined earlier. So, here both u and v are clearly positive.

(Refer Slide Time: 18:29)

Consider a solution $\eta > 1$ for $x^2 - dy^2 = 1$.

Then $\eta = u + v\sqrt{d}$ where u, v are positive and u/v is a convergent to \sqrt{d} .

Here $0 < u - v\sqrt{d} = \frac{1}{u + v\sqrt{d}} < \frac{u + v\sqrt{d}}{2u}$, $u > v\sqrt{d}$
 $u + v\sqrt{d} > 2v\sqrt{d}$

$0 < \frac{u - v\sqrt{d}}{2v\sqrt{d}} < \frac{1}{2v\sqrt{d}} \Rightarrow \left| \sqrt{d} - \frac{u}{v} \right| = \frac{1}{v} |v\sqrt{d} - u| < \frac{1}{2v^2\sqrt{d}}$

Then u/v is a convergent to \sqrt{d} .

Moreover, u by v is going to be a convergent to root d . So, let us see how this comes about. So, here this u minus v root d is the inverse of u plus v root d , this is less than our u plus v root d because we have that this is less than u plus v root d because we have the number 1 sandwiched between these two numbers, this is less than 1 and this is bigger than 1.

So, we have that u minus v root d is less than u plus v root d . And ofcourse, we have that this is a positive number. So, that tells you that you that u has to be bigger than v root d and putting that here, we get that u minus v root d has to be less than 1 upon $2v$ root d . Since u is bigger than v root d ; u plus v root d is bigger than 2 times v root d and so the reciprocal is less than 1 upon $2v$ root d .

So, u minus v root d is these are both positive numbers we have u minus v root d less than 1 upon 2 root d and therefore, root d minus u by v which is really 1 upon v , v root d minus u which is simply the mod of this is less than 1 upon $2v$ square root d which is further less than 1 upon $2v$ square.

So, this u by V is a rational number which is trying to approximate root d in a way better than the convergence would do we know that the convergence would have approximate root d in a good way that means p_n by q_n are close to root d by distance at most 1 upon q_n square and in fact one of the two consecutives one of the each pair of consecutives convergents will have the property that one of them is less than 1 upon $2q_n$ square.

And then we saw the proof that if anything tries to do better than convergents then that has no other option but to be a convergent. So, here we see that this u upon v is trying to

approximate root d in a way better than the convergence and therefore, u by v is a convergent to root d . So, this is some nice situation, because we wanted to find a non-trivial solution to $x^2 - dy^2 = 1$ and any such non-trivial solution bigger than 1 has to be a convergent to $2\sqrt{d}$.

We are happy with solutions bigger than 1 because all other solutions can be obtained by taking the inverses of these solutions in $\mathbb{Q}\sqrt{d}$ and putting a plus minus sign. The plus minus sign will not change the value of the norm, norm will still be 1. So, we are looking at solutions which are bigger than 1 and satisfy $x^2 - dy^2 = 1$ any such solution should give you the x upon y to be a convergent. But we are going to get more and more conditions on this convergence.

(Refer Slide Time: 22:39)

The continued fraction expansion for \sqrt{d} is

$$\sqrt{d} = [a_0; \underbrace{a_1, \dots, a_m}_{m \text{ is period}}, a_1, \dots, a_m, \dots].$$

$\sqrt{d} + [\sqrt{d}]$ has purely periodic continued fraction expansion.

$$\sqrt{d} = [a_0; \overline{a_1, a_2, a_3, \dots, a_m}].$$

We first of all see that if you let root d be this particular continue the, if we consider the continued fraction expansion for root d we have seen that root d plus its integral part has purely periodic continued fraction expansion. This is a result that we have seen, which means that the continued fraction expansion for root d which will change from the continued fraction expansion of root d plus integral part of root d only in the first place because you are adding or subtracting an integer.

But from second place onwards the periodicity has to start. So, you have that the continued fraction expansion will look like $a_1 a_2 \dots a_m$, where m is your period of the expansion. And you can take m to be the smallest one where you have the repetitions. So, m is the period of the continued fraction expansion that you have the partial quotients getting repeated. So, from

first step onwards, we should have that these continued fraction expansion partial quotients start repeating.

So, you will have a_1, a_2, a_3, \dots , then again a_1 , and so on up to a_m , then again a_1 and so on up to a_m , so we have that \sqrt{d} turns out to be $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_m + \frac{1}{\ddots + \frac{1}{a_1 + \frac{1}{\ddots + \frac{1}{a_1}}}}}}}$. And then you have a_1, a_2, a_3 and so on up to a_m , this is the continued fraction expansion for any root d . And ofcourse, we know how to compute the partial quotients, the complete quotients and the convergents.

(Refer Slide Time: 24:50)

If $u/v = p_n/q_n$ then n is odd.

$$\sqrt{d} = \frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}}$$

$$(q_n \sqrt{d} - p_n) = \frac{(-1)^n}{q_n \theta_{n+1} + q_{n-1}}$$

If n is even, then $\rightarrow > 0$. $(p_n - q_n \sqrt{d}) < 0$

Therefore n is odd.

But we claim that our u/v which gives us a solution to the Brahmagupta equation so this u/v comes from the solution to the Brahmagupta equation if it is p_n/q_n for some n , then n is odd. Why is this? This is because, we will write \sqrt{d} to be $p_n \theta_{n+1} + p_{n-1} / q_n \theta_{n+1} + q_{n-1}$ this is a formula which we have already derived here θ 's are the complete quotients.

And now, we look at $q_n \sqrt{d} - p_n$ we simply multiply throughout this expression by $q_n \theta_{n+1} + q_{n-1}$ and subtract p_n and from this, this is also something that we have done in one of the last lectures, what we get here is that this is $(-1)^n / (q_n \theta_{n+1} + q_{n-1})$. So, this part turns out to be $1 / (q_n \theta_{n+1} + q_{n-1})$ if n is even then this quantity becomes positive because the numerator is positive and denominator here is anyway always positive.

So, this turns out to be positive and then we get that $p_n - q_n \sqrt{d}$ is negative, but that cannot happen because our $p_n/q_n = u/v$ remember p_n and q_n are u by v this is u by v

root a this is a positive number and its inverse then cannot be a negative number. So, if u/v is p_n/q_n for some n then n has to be odd.

So, this is the first condition that we obtained, we have proved that u/v where $u^2 - v^2d = 1$ if u/v is p_n/q_n , we consider the rational number u/v then it has to be a convergent to root D . Moreover, if it is p_n/q_n for some n being a convergent that n has to be odd.

(Refer Slide Time: 27:50)

If $u/v = p_n/q_n$ then $n = lm - 1$, for some $l \in \mathbb{N}$. Here m is the period.

$$\sqrt{d} = \frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}}$$

$$(p_n - q_n \sqrt{d}) \theta_{n+1} = q_{n-1} \sqrt{d} - p_{n-1}$$

$$\underbrace{(p_n^2 - q_n^2 d)}_{(-1)^{n-1}} \theta_{n+1} = (q_{n-1} \sqrt{d} - p_{n-1})(p_n + q_n \sqrt{d})$$

$$= (-1)^{n-1} \sqrt{d} + C$$

$$\theta_{n+1} = \sqrt{d} + C$$

Further, we see that it is not just odd, but it is of the form $lm - 1$ where l is some natural number and m is the period. So, here m is the period we will prove this also because, recall once again that we have root d to be $p_n \theta_{n+1} + p_{n-1} / q_n \theta_{n+1} + q_{n-1}$ and if we consider if we expand it out by taking this denominator multiplying it to this side and then writing it out explicitly, we get $p_n - q_n \sqrt{d}$ into θ_{n+1} to be $q_{n-1} \sqrt{d} - p_{n-1}$.

And therefore, if I multiply by $p_n + q_n \sqrt{d}$ to both the sides we get $p_n^2 - q_n^2 d$ into θ_{n+1} equals two on this side we get $q_{n-1} \sqrt{d} - p_{n-1}$ excuse me this is $(-1)^{n-1} \sqrt{d} + C$ which is again of the form some integer into root d plus another integer, but the integer that we get here is $p_n q_n - 1 - p_{n-1} q_n$.

So, this is $(-1)^{n-1}$, we have already seen that n is odd, so we get that this is root d plus C . Moreover, this is equal to 1, so we get that this is θ_{n+1} . So, θ_{n+1} is root d plus an integer.

(Refer Slide Time: 30:40)

If $u/v = p_n/q_n$ then $n = lm - 1$, for some $l \in \mathbb{N}$.

$$\theta_{n+1} = \sqrt{d} + c = a_0 + \frac{1}{\theta_1} + c = \underbrace{(a_0 + c)}_{a_{n+1}} + \frac{1}{\theta_1}$$

$$a_{n+1} + \frac{1}{\theta_{n+2}} \Rightarrow a_{n+1} = a_0 + c$$

$$\theta_1 = \theta_{n+2}$$

Then $n+1 = lm$ and $n = lm - 1$.

But we already have plus some integers C but root d already has this continued fraction expansion, this is how we begin getting the continued fraction expansion for root d . So, this is a naught plus C plus 1 upon theta 1. On the other hand, this would be a n plus 1 plus 1 upon theta n plus 2 because the complete quotient q theta n plus 1 its integral part is a n plus 1 and then you would have the next remaining fractional part you will write it as 1 upon theta n plus 2, but if you look at it from this point of view, the integral part has to be a naught plus c .

So, this expression gives us that a n plus 1 is a naught plus C and then you should have that theta 1 is theta n plus 2 which means that the theta 1 is obtained after the n plus 1 steps. So, n plus 1 has to be a multiple of your period m , you may remember m was chosen to be the smallest possible such number where you get periodicity. So, n minus 1 is a multiple of m call it $l m$ and therefore, we get n to be n plus 1, then $l n$ plus 1 is $l m$ minus 1 and so, we get n to be $l m$ minus 1 for some natural number multiple of m .


(Refer Slide Time: 32:40)

If $u/v = p_n/q_n$ then $n = lm - 1$, for some $l \in \mathbb{N}$.

In fact, $l = 1, 2, 3, \dots$ if m is even and $l = 2, 4, 6, \dots$ if m is odd.

n has to be odd, so if m is even then any lm is even and $lm-1$ is odd.

If m is odd, $lm-1$ is odd, the l has to be even.



Furthermore, these l s have to be $1, 2, 3$ when m is even and $2, 4, 6$ when m is odd, that is because we want our n to be odd, n has to be odd. So, if m is even then any lm is even and lm minus 1 is odd this is okay. If m is odd, we want lm minus 1 also to be odd the l has to be even because if you take l to be odd m to be odd lm will be odd into odd which is odd and odd minus 1 will be an even integer.

So, the only possibilities are these possibilities. So, what we have done is that we have completely written down all possibilities for the n s where u upon v is the n th convergent, it remains to see and it will not take more time now, to see that any such convergent indeed satisfies the Brahmagupta equation.

(Refer Slide Time: 34:10)

We next prove that all such convergents do indeed satisfy the Brahmagupta equation.

$$\frac{u}{v} = \frac{p_n}{q_n}, \quad n = l_m - 1, \quad n \text{ is odd.}$$

$$\theta_1 = \theta_{n+2}, \quad \sqrt{d} = \frac{p_{n+1}\theta_{n+2} + p_n}{q_{n+1}\theta_{n+2} + q_n} = \frac{p_{n+1}\theta_1 + p_n}{q_{n+1}\theta_1 + q_n}$$

But $\sqrt{d} = a_0 + \frac{1}{\theta_1}$, $\theta_1 = \frac{1}{\sqrt{d} - a_0}$.

$$p_n = q_{n+1} - a_0 q_n, \quad p_{n+1} - a_0 p_n = q_n d$$

Such a convergent satisfies the Brahmagupta equation.

we get

$$p_n^2 - q_n^2 d = p_{n+1} q_n - q_{n+1} p_n = (-1)^{n+1} = 1$$

So, we now have to see that all such convergents, what do we mean by such convergents? We are looking at u by v to be p_n by q_n , where n is of the form l_m minus 1 and n is odd. We will prove that all such convergents also satisfy the Brahmagupta equation that is a simple check. So, this is what we do. So, we have this n and ofcourse then θ_1 is θ_{n+2} because n is l_m minus 1 $n+1$ is l_m .

So, θ_{n+2} is θ_1 and we use once again the previous formula and use this to write it θ_1 but we have that \sqrt{d} is $a_0 + \frac{1}{\theta_1}$. So, treat θ_1 as $\frac{1}{\sqrt{d} - a_0}$ minus a_0 , we put this formula in this equation for the θ_1 once, we would get some equation for \sqrt{d} and separating out we get finally, that p_n is $q_{n+1} - a_0 q_n$ and $p_{n+1} - a_0 p_n$ is $q_n d$.

So, when you expand this out this particular equation by putting theta 1 equal to 1 upon root d minus a naught we get 2 sides where you have some multiple of root d plus an integer equal to some another multiple of root d plus another integer and then these multiples of root d will have to be same and the integers then also will have to be the same. So, therefore, we get these 2 particular equations, we try to eliminate the a0 from these equations.

So, you can eliminate a0 by multiplying this equation by p n and multiplying this equation by q n, but let us say with a negative sign. So, if you do that the we get here p n into p n we get p n square p n into p n and to this side we are going to multiply by minus q n, so minus q n square d this is we will have this q n plus 1 p n minus p n plus 1 q n, which we know is minus 1 to the power n plus 1, but n is odd and therefore, n plus 1 is even and so, we get that this is equal to 1, so indeed p n and q n does satisfy the Brahmagupta equation.

So, what we have proved is that any solution to Brahmagupta equation which is bigger than 1 is a particular type of convergent to root d and moreover, if you take a particular type of convergent to root D that does satisfy the Brahmagupta equation. So, we have explained in complete detail the solutions to Brahmagupta equations, which are bigger than 1.

And as we have discussed the set of units in the quadratic extensions, we see that all the solutions to the Brahmagupta equation can be now explained once you have these solutions with you.

(Refer Slide Time: 38:59)

Thus, we have described all possible solutions to the Brahmagupta equation.

Similarly the solutions to $x^2 - dy^2 = -1$ can be described.

There is no solution if m is even.

If m is odd then $u/v = \frac{p_n}{q_n}$ where $n = lm - 1$ with $l = 1, 3, 5, \dots$



There is also this $x^2 - dy^2 = -1$ we will simply mention the solutions to this, but we will not have time to prove this The answer is that when m the period

when that period is even there is no solution. So, remember for root 3, we had the continued fraction expansion which was $1, \overline{2}$.

So, there the period is even after 2 stages you get repetitions then you are not going to get any solution to $x^2 - 3y^2 = -1$ that can also be checked by using some simple arithmetic modulo 4. So, whenever m is even there are no solutions. Whenever m is odd the solutions are explicitly written down as follows that any such solution which is bigger than 1 is a convergent p_n/q_n where you are n is still $lm - 1$, but l is now an odd integer 1, 3, 5 and so on.

So here n has to be even that is quite clear because we want that minus 1 to the power odd has to come, and therefore your n has to be an even integer. This is where we complete our penultimate lecture. We are just going to tie up some loose ends in the next lecture. It is going to be a short lecture. I look forward to see you there. And thank you very much.