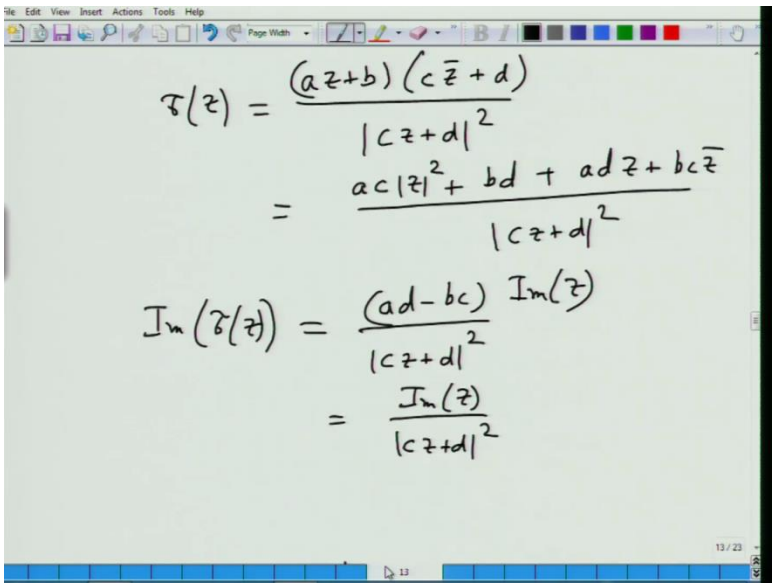
Riemann Hypothesis and its Applications
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

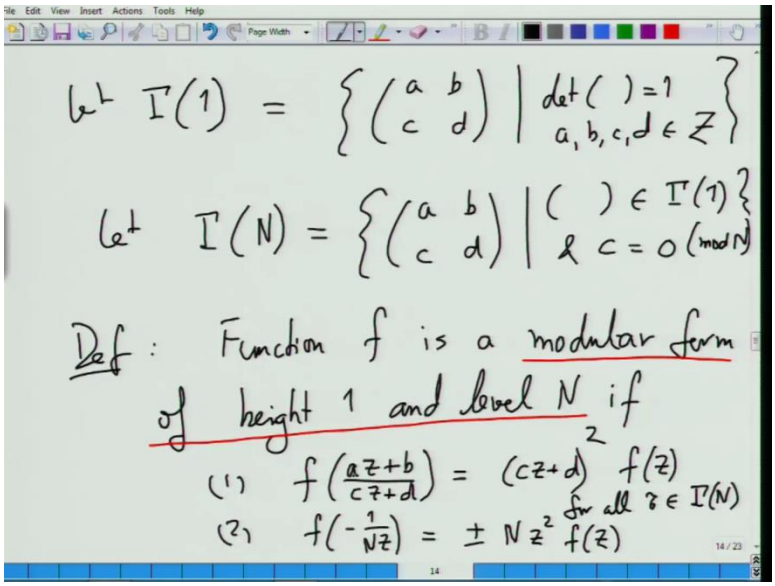
Lecture – 26

(Refer Slide Time: 00:20)



Let us finish this half ah yesterday I we saw that the mobius transform (( )) half of complex structure. And I also mentioned that this is ah the characterization of the transform that preserve angles between two cones. Now however these guys related to what how the thing that we are doing.

(Refer Slide Time: 00:57)



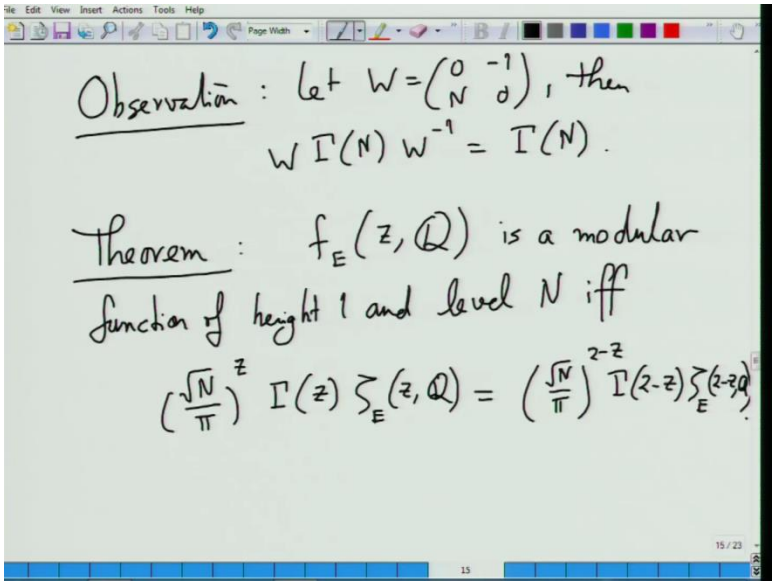
Well that is define of selected define the particular tau start with this gamma one what to be consider into gamma function. This is essentially consider the set of all matrices, so these are precisely be this is we are this investigations transforms given by them.

I am now going to define ah subgroups, total subgroups of this, by this is the group and multiplication, because ((Refer Time: 02:01)) So, I am going to define certain subgroups say the condition the additional condition is take all the matrices in gamma one, and c should be contour zero mod n. So c should be define by the number n which is supplied separately. The number n defines the appropriate subgroups over there. ok, Why this is subgroups, (( )) the only the additional condition is with the bottom left entry should divisible by n. So if we take two such elements, two set matrices and take the bottom left multiplication that would be c one times something plus d one times c two. Now c one, c two both are divisible by n, so therefore we (( )).

And now we define equals ok. So the function f is a modular form of height one and level N if the following two conditions solve. One is the primary condition, two is just slight twist on the one. The condition is that you apply this any of this transforms in gamma n on z and apply f on it. What you get the value is f z times c z plus d whole square for the new denominator of the transforms comes up as the multiplier and the (( )). And earlier what about height, we can define higher height when this degree is instead of two or its more [vocalized-noise], but we will not be

interested in that. And second is that f of minus one over N z, this is what quite, it doesn't quite fall into this, because this determinant of this transform is N. Z goes to minus one over N z, so here a is zero, b is minus one, c is N, d is zero. So it is zero minus one N zero, so that determinant is N, so it is not given belong to this. But it is very closely related to this group.

(Refer Slide Time: 06:33)

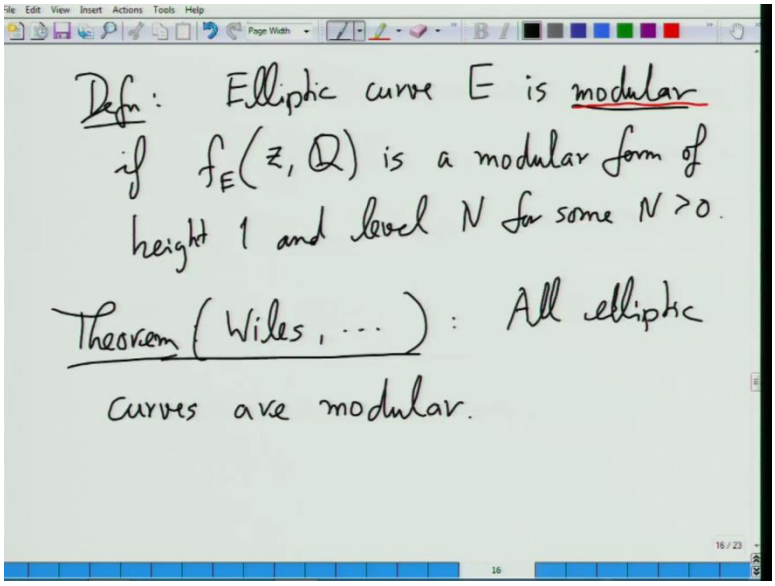


In fact ah this is the simple observation if we let matrix W is zero, minus one, N, zero then W gamma N W inverse, so essentially the matrix W commutes with the group gamma N. Commutes in the sense not with the individual elements, but with the whole groups. So this is very closely related to this group and what we are saying is that in fact what one can show is if this condition is true, when f of minus one over N z must be a linear combination of plus N z square f z and minus N z square f z. And what this condition is saying that there should just one these two, it is the plus or minus, so that's make the function f which is remember that the function of that kind we the Fourier series kind that we are looking at that is the function we started right. This is the function associated with electrical rational number Fourier series periodic with period of one. And then we are looking at at least that set we are look at the transformation on upper half plane, and see how the function behaves that and that should be available function not all of them, but (( )) areas of function we are interested in it and these function is called (( )). For this may seems like a very strange condition why could such transform equal to a very high to believe that there should be a case. And even if something like

this what you will arrival, interesting theorem which says that f E, this is the Fourier series associated with the electric curve E, who all the rational numbers is a if and only if that if I can get this expression right. So this relates this Fourier series representation with the Dirichlet series representation that the Fourier series being modular is equivalent to the corresponding the Dirichlet series functional equation.

And the if I fix the height to be one, but this more general theorem holds actually. If the height is, whatever is the height, so the height is k and this number two, which is occurring here and here becomes two K. So the symmetry becomes no longer series are equal k. Level of course occurs say this places that level really represent the multiplicative factor at this point, and this is the central connection with with the things that we have studied so far and the thing that I will new thing that I will introduce that. If you recall, go back, so I give the started this proof sketch right, so you looked at this curve then the point of order and it does not have a point if F is modular. F is the that is specifically Frey curve, and the (( )) theorem say if F is modular, then it does not have a point of order greater than equal to six.

(Refer Slide Time: 11:55)



And then we jump into modular curves. What are modular curves really are, so we say curve is modular. Ok let me just define it also. So elliptic curve E is modular elliptic curve, is a corresponding modular series is modular form of height one and some level. So now everything

connects of that what Frey (( )) shows that if the elliptic curve specific elliptic curve F was modular, then ah it doesn't have a point of order greater than equal to six, which means that the discriminant of it that cannot be greater than equal to six, which in term means that the solutions to that (( )) equation doesn't hold.

And finally, the last piece in the puzzle was (( )) by Wiles then other later on that which showed that all elliptic curves are modular. If Andrew Wiles showed it not for all elliptic curve, but only a sub classability, which was good enough because that particular elliptic curve f did fall in the sub class, call semi-stable whether it is not important. And then later on, ah other ah mathematician worked on that prove and generalized it which includes all it. Now we know that all elliptic curves are modular which means the corresponding Fourier series have are modular form, which is equivalent to saying the corresponding zeta function associated with those elliptic curves (( )) by the those. But this required huge amount of effort, you may that Andrew Wisel proof is originally of course, more than hundred pages long, It was later on (( )), but still is fifty pages.

Whereas if you remember, we derived functional equation for all zeta function pretty easily, because (( )) required some derive function. If you remember we have to do this ah going to the Fourier analysis, like we did some e to the minus i n square (( )), still it was not too difficult. And in fact, this if you now go back and look at that proof and keep in mind that what you are, keep in mind this equivalent between the zeta function, functional equations and corresponding Fourier series, modularity. Respect with to our zeta function, the original Riemann zeta function also we can associate the corresponding Fourier series. And if you run through the proof of the functional part which equation of the Riemann zeta function, the functional structure is zero that proof is actually showing also that the corresponding modular function not modular function, the corresponding Fourier form, is modular.

Not exactly this much more or less so let me see, so there is the corresponding Fourier series is modular of height half. Half because you see this is two z whatever is the height multiply by two n then that is line along with the symmetry, so it is half here. And level is two, because (( )), what?

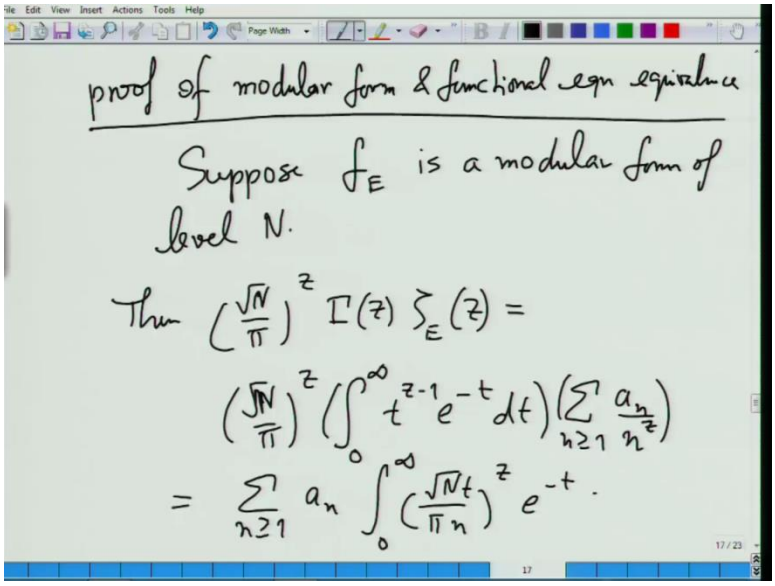
Student: (( ))

Professor: U ten by two, what (( )) pi to the minus z.

Student: (( ))

Professor: (( )) z by two zeta, so that gamma z by two actually comes to plays the role that is where it is (( )) flips. Here we are sticking with gamma z, so there is some transformation that happen which brings in that level two very easy to work in terms of (( )). And this two actually straightforward (( )). The equivalence between modular forms, because write down the condition verified (( )). For example, if you say which direction do you want, let us start with this.

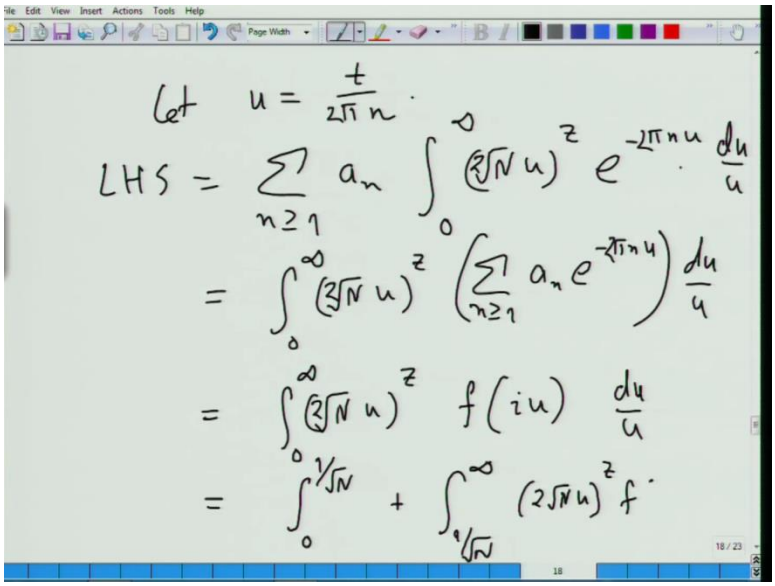
(Refer Slide Time: 18:42)



Let say suppose f is a modular and then we want to show this functional equation. So let us start with the left hand side.

What is this equal to, let just write down everything. What is gamma z, (( )) integral which is t to the z minus one e to the minus t dt. And zeta z is n greater than equal to one, a n divide by n to the z. And I will be using that uniform convergence, so this mapping the infinity integral infinite sum freely. So then this become sum n greater than equal to one, a n divide by n to the z. And I will be using that uniform convergence, so this mapping the infinity integral infinite sum freely. So then this become sum n greater than equal to one a n zero to infinity square root N by pi n to the z, (( )) t also, e to the minus t d t by t.

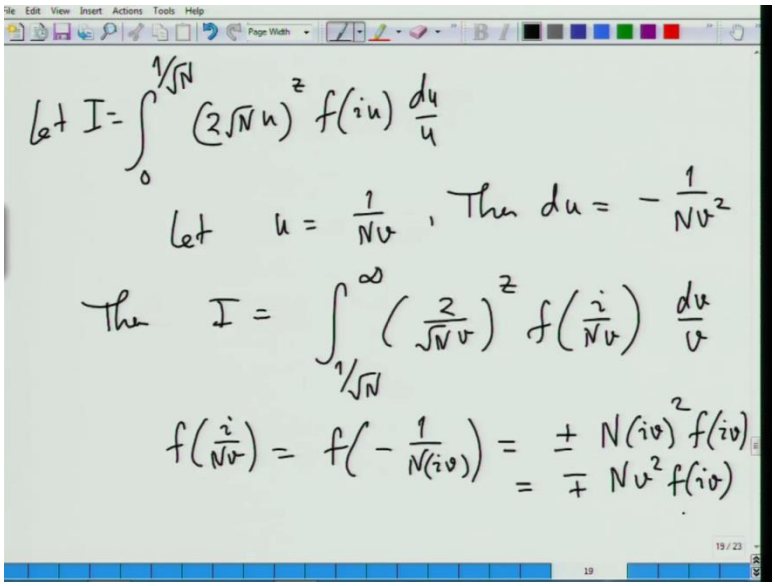
(Refer Slide Time: 20:59)



And we will do a value substitution, u is then what do you get, t is e to the minus pi n u and then dt over t d t is du by u. Now take the integral summation n side of n, and what is this sum. What was f of E, what was the f of E recall them, sum over n a n e to the two pi (( )) two pi i n z. So this is going to be equal to f of stick to somewhere, I want to do this, to use t over two pi n. So if you t over two pi n, then t over pi n is two, but I will take care of the (( )) and du by u that's ok, the two cancels out. So this is going to be equal to f of i u…

Now split this integral into two parts, going from zero to one over root N, then one over root N to infinity. Then we look at the first part, this is actually may be picking this the functional form for the zeta function proof. There also we did this, we did this exponential sum, we replace it with there was function W that we defined and then we split that integral zero to infinity to zero to one and one to infinity. Zero to one, we work with n use that property of W function to write it in terms of one to infinity integral that is exactly we are going to do.

(Refer Slide Time: 24:37)



Let's look at the zero to one over root N, this integral [noise], what is the F of i, we call f as modular, we should something not right, so you will use this one the second condition, f of minus one over N z use this. For i u we should use directly the other conditions may be you should f of i u is going to be (( )), ok two things. F only makes sense when it is augmented on the upper half of complex plane and that certainly the case; f of i u, u is positive, so it is upper half of complex plane, so that it does make sense to work with this properties of f.

What is f of i u, use that mapping of this, let's use this and see how we write f. So z is i u.

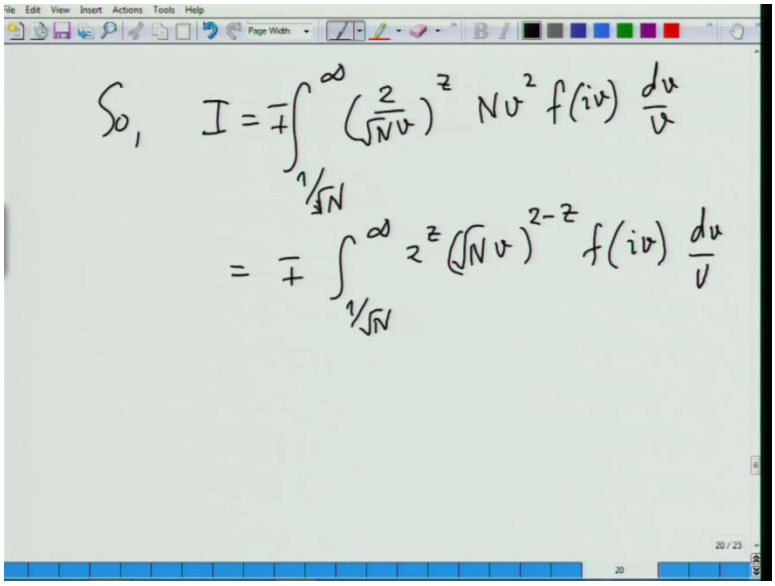
Student: (( ))

Professor: We can actually easier to use the second form, so let's to tend that let me first do a (( )) substitution here. Let u be ah one over N then du is minus one over N v square. Then I equals what happens to I, when u is zero v is infinite; when u is one over square root N then v is one over square root N. So the I is negative of the integral going from one over square root N to infinity. And then what is square root N u, two by square root N u to the z f of i by N v, du is minus one by, so minus minus goes away, one by N v square. And u is one over N v, so that is dv by v.

Now we going to flip this, f of i over N v, z to be ok… So f of i over N v is f of minus one over N i v; i v is in the upper half of complex plane, v is real which is upper half of complex plane. So I can use the other form to write it as plus minus N v square which is i v square times f of i v. So we (( )) that in.

I equal to one over square root N to infinity, two by square root N v to the z, and what happens to this, this is minus plus N v square f of i v dv by v. So what comes out this that is (( )) power of two that is taking out, (( )) which is goes somewhere.

(Refer Slide Time: 28:22)



If (( )) power of two, if you see this integral two power that is forgot about square root N u to the z f i u du by u. The other integral is square root N v to the two minus z f i v dv v. The same integral if you looking at changes in exponential from z to two minus z, which in zeta function that is so basically what we saying is total entire integral is square root N u to the z plus square root N u to the two minus z times something which you independent of z. When you flip z to two minus z, which becomes in stage in valid, except for the sign, because the plus minus sign can change the sign, flipping z to two minus z can change the sign that is what is occurring here, (( )) so there is flip of sign.

I think there is the two is to be absorbed by here. If you take two here, then we start with this, this and use (( )). With that today the takeover from this course apart from whatever I have

described is that for zeta function, rational for elliptic curve we have not as much knowledge as we have from other zeta function, even the functional form we just (( )). And we not even close to doing the corresponding Riemann hypothesis. Say this, we can say the same thing, because of the functional form, one thing that immediately follow with zeta function is (( )) it define over the entire complex. And now the middle line, the symmetric around lines real that is equal to one. So you want to the conjecture would be that all the zero lie (( )). In fact there is I can talk about in next time, there is another very famous conjecture which is (( )) conjecture which touch about specifically about the zeta function, elliptic curve, and its properties. So this is very famous conjecture…

Student: (( ))

Professor: (( )) And this with very we are known idea of this, but it remains one of the major open questions.