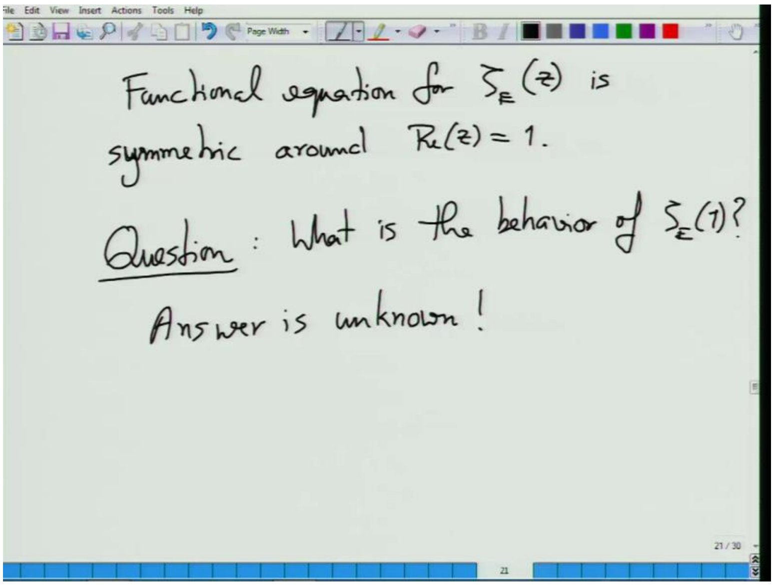
Riemann Hypothesis and it is Applications
Prof. Manindra Agrawal
Department of Computer Science and Engineering
Indian Institute of Technology, Kanpur

Lecture - 28

Welcome to the last lecture. Now, it is a kind of a course where you always feel that, even you one can do a little more. Not a much more. But, anyway one has to put at a stop at some points. So, here is what I am going to do today. I think, I said that last time. I will very quickly describe the bridge, when you written tier conjunction. And then finally, wind up by showing you, how elliptic course or complex some course are equivalent to torus.

So, let us start to with that recalling our discussion earlier. That over elliptic curves, the zero functions that we define and there is a analog corresponding power series. So, that power series being modular in essentially equivalent to zeta function, having a functional equation.

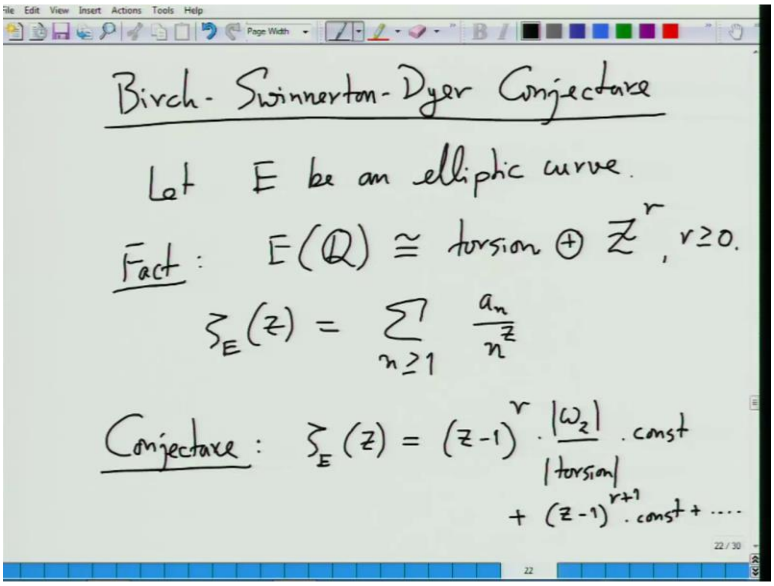
(Refer Slide Time: 01:25)



And that functional equation was, symmetric along the line. Symmetric around real z equals 1. So, the corresponding version of Riemann hypothesis for this would be that, all the zeroes of this zeta function lie on this line real z equals 1. Already I said, very little is known about this fact. In fact, something very simple, something that you might expect. That something much simpler is also completely unknown, which is....

So, we just ask the following question. How does zeta 1 behave? Is it zero, is it nonzero and if it is zero, what is the order of that zero? So, answer is completely unknown. And that conjecture which I refer to actually refers to this behavior.

(Refer Slide Time: 03:33)



So, what Birch Swinnerton Dyer conjecture says as the following? It is actually describe the behavior of zeta 1. ((Refer Time: 04:03)) So, what is known is, this is the fact. That if you look at this group of points on the elliptic curve, group of rational point on this elliptic curve. And this group has a fairly simple structure. And the structure is like this, that this group of points is isomorphic to the following structure.

There is a set of points which is called a torsion points, which are points of finite order. So, which means that if you had the point to itself, a finite number of times you get the zero, which is the infinity element here called the elliptic curve. Then there is, this image of integer z and z to the r means, the disjoint sum of r's copies of z. So, this group essentially is disjoint sum of r plus 1 subgroups. First one of them is torsions of group, which is a group of all points of finite order.

And, then there are r copies of z. This number r is not fixed. It can be zero, it can be 1, 2 but, it is fine. So, this is known about the group of rational points on the elliptic. So, now we come back to this conjecture. Now, if you recall the, what is the zeta function of the corresponding curve defined. This is equal to summation and greater than equal to 1 a n divided by n to the z, where a n in the sense, measures the number of a, n is prime.

Then, a n is number of points on this curve modulo p. And for other non composite numbers, there is somewhere that you can define. So, a n this numbers a sub n's are in a loose sense, counting the points on this curve. However, feels of finite characteristics or infinite characteristic. Now, let us come to this conjecture. So, this conjecture says not one. But, if you look at the zeta z, as a power series around z equals 1.

Then, how would be the behavior of, this is the following. It is says, that power series of zeta e at z equals 1 was like z minus 1 to the r times of constant. And this constant also the conjecture describes you, very precisely. I am only going to describe two numbers in this constant, overall constant that occur. One is simple, that is the number of the size of this torsion subgroup. So, that stays in the denominator.

In the numerator, there is this number. This absolute value of omega 2 and this number will, this value will come to any moment this time. When, we talk about elliptic curve or complex number, then this number will be define. And then there is another some other numbers here, which are related to certain other quantities, associated with this elliptic curve plus the higher power ((Refer Time: 09:15)).

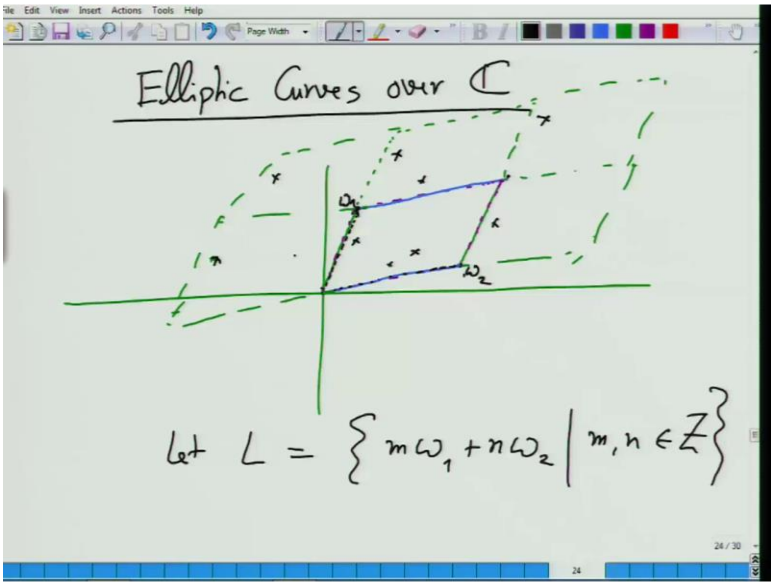
So, forgetting the constants is the main point here, is that zeta 1 has a zero of order r, where r is precisely the number of copies of z in the group of rational points, which of curves means that if r is zero, then zeta e 1 is nonzero. So, if zero if and only if r is greater than zero and the order is exactly. Now, this is conjecture has again is a fairly recent origin, I think. It was done in 70’s, 1970’s.

Not very old conjunction, where interesting thing is that, at the point this conjecture the time this conjecture was defined. Nothing was known about elliptic curve and this... For example, the fact that the zeta function that is phi the functional equation is a shelf of recent vintage, at 1990’s. So, at that point not even clear with there, that is the functional equation here. And there was no reason to believe, really why they?

Why it should have a zero and the order should be precisely r. So, what these guys did was, they did extensive computer experiments. That is calculating, specifically curves the zeroes and the order of zeroes. And then trying to look at the corresponding rational groups and order of the number of copies and that solve this. This is how they using some more intuition plus this, they formulated the conjecture.

It remains completely open. And in addition to Riemann hypothesis, this is also identified as one of the 7 million problems. So, that is all I will say about this conjecture. Now, let us come to the other topic.

(Refer Slide Time: 11:32)



Elliptic curves over complex inverse. Now, one thing that should become immediately clear is that, the geometric picture we have in mind for elliptic curves. That there is this two independent curves, one is a close curve and the other is infinite curve. That belong a ((Refer Time: 12:02)). Because, that reason there was two independent curves which precisely that. There also some imaginary solutions in the in-between region.

So, what real said that do not exist. But, the moment you go complex and with all the solutions do exist. In fact, for every value of y there will be precisely three values of x. So, that geometric picture will go away. And the interestingly, one way under what is the geometric picture that comes out of... Once, you look at over complex number and interesting part is that, is actually a torus.

But, one has to do a litter bit of work in making this correspondence. So, exactly what I am going, correspondence would be is the following. So, let us first look at a torus. A torus is a set of circular thing, which has actually two cycles in it. One is big cycle and one is the small cycle. Now, as a geometric figure is simple enough and we can view it, as forms. If you make it, take the complex plane. And you identify some parallelogram in the complex thing.

One end of which line is at zero, that is all is not important. It is a parallelogram. Now, what you do is, you cut out this parallelogram from the plane, fold this. So, let us think of it is the paper and fold this. This side folding on to this side and joining here. So, it makes a cylinder. And then you take the cylinder and fold it on the along that x axis. And join the two circles together, that becomes a torus.

So, the effect here on this piece here, is as if we are identified this line with this line, by folding. And this line with this line, is that clear. That is a geometric curve. That is a one way of forming a torus. And it is a nice way in for our purpose because, it gives an understanding of how do we start from a complex plane. We already know some way of twisting and turning complex in this various ((Refer Time: 15:08)).

So, this actually is another Riemann surface. Another way of forming a Riemann surface complex plane. Now, what I promised you was that, I will show the elliptic curves over complex numbers to be equivalent to torus. In order to do that, what I willing to do is, to give a homomorphism. I clear, it is isomorphism. From the points on a torus to the points on a elliptic curve. And this isomorphism should preserve the group operation.

What is the group operation? It is a good point. We know the group operation on elliptic curves. What is the group operation on torus? Well, the group operation on torus is again, can be easily defined if you use this picture. So, the points on torus will be the points inside this. The one thing that we have to be careful about is, when we look at this piece, we should the points in the torus are counted by taking these two edges in and the other two edges out.

So, given any two points on this torus or on this piece, what is the natural addition operation that you can define? Well, these are two complex numbers. That we add the two complex numbers, that gives you two another complex numbers and very natural addition. But, then it also needs to be inside the same piece. But, this addition of these two may fall out of this process. So, say addition of these two is somewhere here.

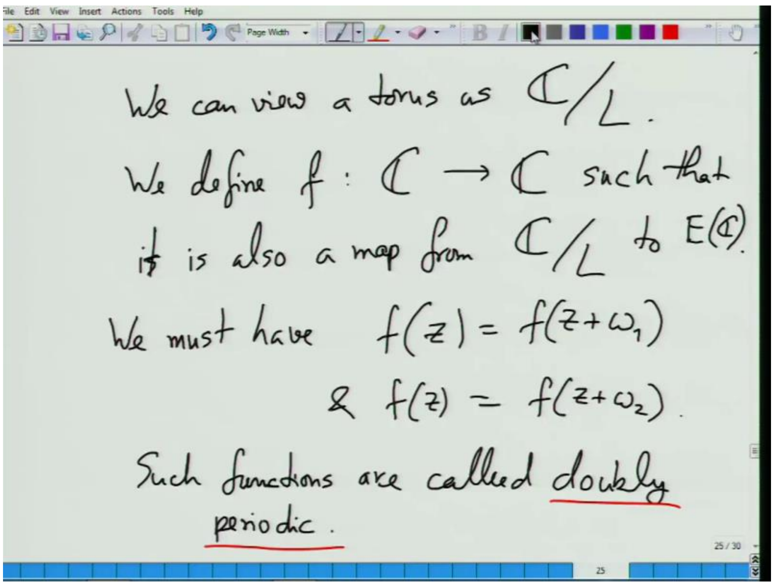
Then rack it back. So, just think of this. Take the another copy or the same piece, stick it there and wherever that, this location is just to pull it back here. So, in sense you are going double modular, modular in this direction as well as modular in this direction. So, whichever way you go and then you come back to the same place. So, that is a natural way of defining an addition and that it. So, this is see that the points on this piece or a strip, not strip this here.

These are closed under or form a group under such an addition operation, with the identity being zero. That is why, I said we will start. We will in one end, we will keep zero. And will show that the mapping, there is a isomorphism from the torus to the elliptic curve with preserve this group option.

Student: ((Refer Time: 18:19))

Exactly. So, that is that perfectly observation. So, essentially when you look at this structure, you can think of rather in lattice, on the complex plane. So, if you look at consider this. Let say this as omega 1 and this as omega 2. Then, you can define a lattice to be m omega 1 plus n omega 2, m n in z, which all integers. So, set of all points that come out of such linear combinations, from the lattice. So, every point at the corners of such pieces, will be an lattice.

(Refer Slide Time: 19:17)



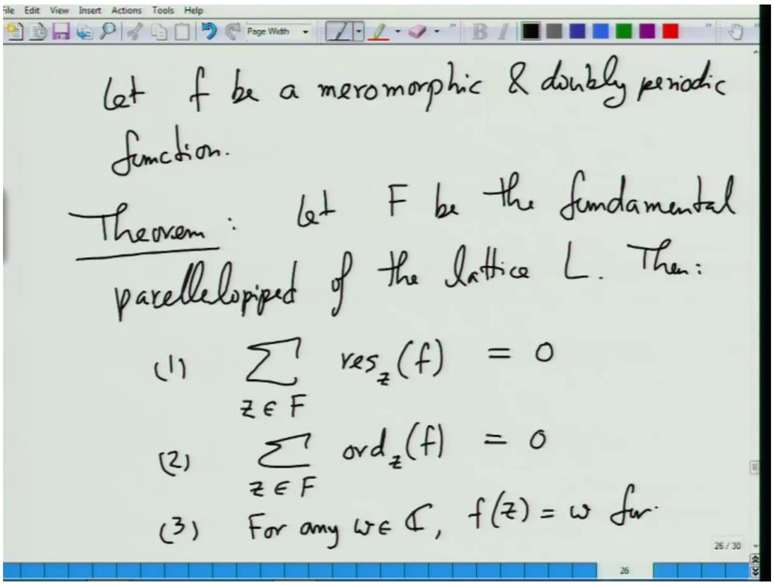
And then the torus can just been viewed as complex numbers, quotient at this lattice. So, L is a group, which is 0. See, L is a group. It is a commutative group. So, it can be just quotient with a set of group of complex numbers and addition with this lattice. That group that you get, that is group operations define on this. And now, I want to give a mapping from this structure, which is a torus to an elliptic curve.

Now, interesting though in mapping the algorithm, we will not only be isomorphism of groups structure but, it will also be a meromorphic. So, with all possible nice properties, you can imagine. And in order to define that, what I will do that, I will go back to this structure here. And define a function on the over the entire complex plane. And the one thing that becomes very obvious is, if this function which is from complex plane to complex number, it has to make sense over this, as a function from c slash L ((Refer Time: 21:06)).

Then, it has to be periodic. In there, whatever value takes at this point, it must take the same value at all point corresponding points and all the pieces here. So, this will have. There is a two dimensional grid here. Each one has a corresponding point to this here. And at each one of those points, function value will have to be this end. So, this function there is obviously a periodic function. In fact, it is more than periodic because, it is a periodic is just typically along one.

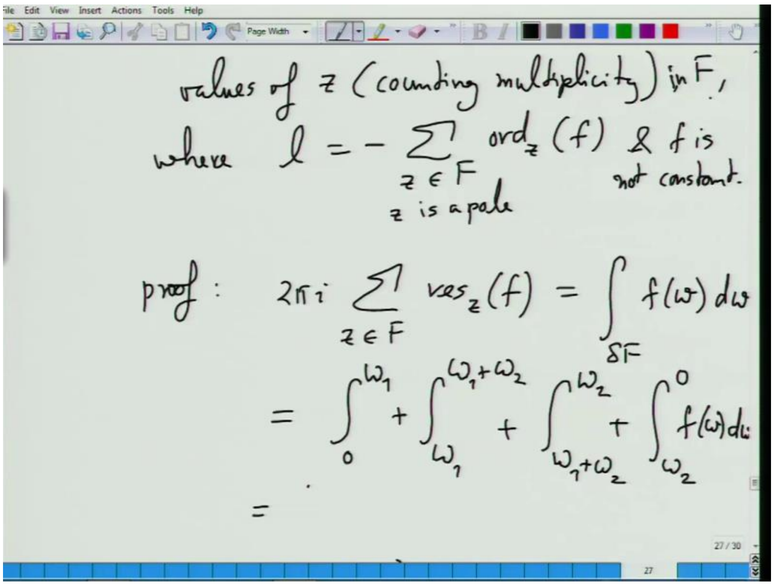
So, that is f of z is f of equal to f of k plus z and its periodic period k. But, this function actually has two periods. So, if this is omega 1 omega 2, then we must have f of z equals f of z plus omega 1 and f of z f of plus omega 2 for all set. Such functions are called doubly periodic. So, that is a minimum we will need. But, as I said we will do more, we will actually make this f metamorphic function. But, the moment you put the condition of meromorphism on such function, which is doubly periodic, a number of interesting things happened.

(Refer Slide Time: 23:11)



So, let me quickly summarize that. So, there is an associated lattice L with this doubly periodic function, which is essentially all integer linear combination of the two periods. And F is the fundamental parallelepiped associated with the lattice, which is essentially that defining which one point at zero, one edge at zero, that is it.

(Refer Slide Time: 25:18)



This theorem says that, if you sum over all points z in F. Look at the residues of these sum of these points, residues of f at each one of those point, when sum is zero. Call, what is the residue of f at a point. It is the, if you look at the power series expansion or Lorentz series expansion of f at that point, there is a coefficient of power of 1 over z, coefficient of 1 over z. Sum over all the residues is zero.

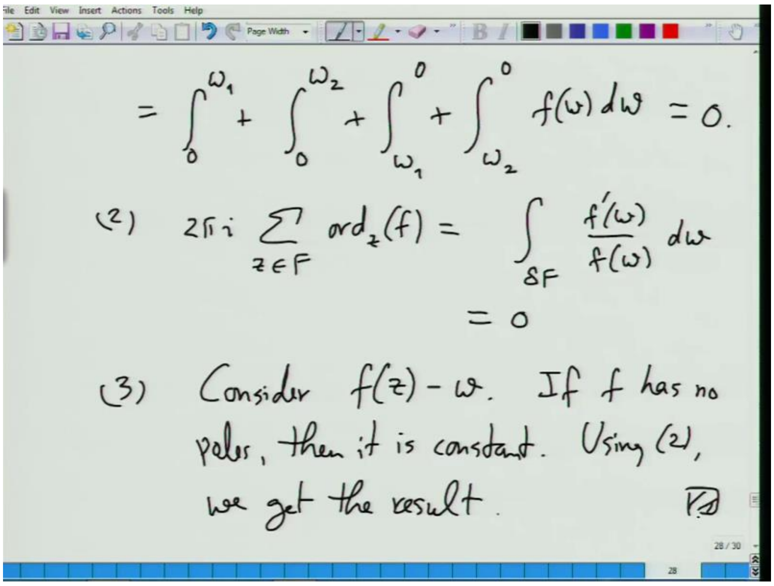
Second the same, the sum over all such points in f, the order of f at z. The sum of that is zero but, the order of f at z. Well, if f is a 0 at z, then the order is the smallest power of, smallest non zero power of the power series at z. And if f has a pole at z, then it is the largest negative power that is nonsense. So, if sum over the orders is also zero, then order is define to be zero. Residue and order, both are defined to be zero, if there is well residue is driven. Now, obviously zero but, order is also defined to be zero.

And third another very interesting property that, f is a subjective map. Not only a subjective map, it has the interesting property. That is given any value on the complex plane, f takes a value z w for exactly l values of z, counting multiplicities. This is another way of saying that f z minus w has a zero of order L. So far, this is not necessary that the l distinct values of z, taking value zero here because, for one particular value of z the order of zero may be higher.

So, if you just add up the order of all the zeroes for all z's of f z minus w that is exactly there, where l is precisely the sum of the order of f at all the poles, inside f. So, if you look at the order of all the poles of f inside is, sum them up. They are all negative of course. And then take minus of that. That is in the proof is fairly simple. This just uses the standard cautious theorem.

So, if you look at this, what is the sum equal by cautious theorem? By cautious theorem, this is simply the integral over delta f boundary of f w d zeta. And the boundary of f is defined to be 0 to omega 1 plus omega 1 to omega 1 plus omega 2 plus omega 1 plus omega 2 to omega 2 omega 2 to 0 of f w d zeta. And this is equal to, let us go to the next page.

(Refer Slide Time: 29:44)



Now, integral from omega 1 to omega 1 plus omega 2 omega 1 plus omega 2 of f w d w, you can do a change of variables. And transform it from integral from 0 to omega 2 of f w plus omega 1. Now, since omega 1 is a period of f, it is same as the f w d w. So, it is I can write this as 0 to omega 2. And exactly the same fashion, I can eliminate omega 2 from here. So, it goes omega 1 to 0 which is of course, is 0.

There is small point here, which I am skipping over that. I am not, am I assuming implicitly here. There on the boundary of f, there is no pole of. Boundary of capital f, there is no pole of function f. Then, this argument goes. So, if there is a pole, then you cannot really run through the integral, line integrals of that. So, what one needs to do is, as we come to a pole, you just make a tiny circle around it.

Now, by periodicity if there is a pole on one edge, there will be a corresponding pole on the other parallelized here. So, whatever circle you do, you do the same circle you do there. So, again they will cancel out each other. And then we will get this theorem. Similarly, if you look at the second one, sum of this. Again this is straight forward because, this again by. Let them, this is by Gaussian integral formula.

That, this is equal to, can be derive this? The residues of f prime over f, is precisely the orders of the vanishing, either the zero or pole with positive negative sign. So, that is this. Now, f time over f is also a doubly periodic function, with the same period. Why, if f is doubly periodic, that is the there is a period. If you look at f prime, it will be again the same doubly periodic function because, it is the values remain the same.

So, as you move across the one piece to the next piece, you will again get the same derivatives all over the point. So, f prime is also doubly periodic with the same periods. So, f prime over f is also doubly periodic with the same periods. And therefore, this integral we just showed is a zero. For any doubly periodic function, this integral was zero. So, this would be 0. And third one was to, is to show that given. So, you just consider f z minus w.

This function, w is fixed. So, this function is also doubly periodic with the same periods. So, say doubly periodic with the same periods, if you look at the fundamental parallelepiped, which again the same fundamental parallelepiped, it will hold. It will be exist for this also. All you are doing is, you are shifting every value at every point in, for f by this among w. So, it is a remains a doubly periodic with the same fundamental parallelepiped.

If you focus inside the fundamental parallelepiped, the sum of this is going to be. Let us just use this, the second one. Sum of the orders of this function inside fundamental parallelepiped is, it is zero. Now, there are two possibilities. Possibility one is that, it has no poles. If this function has no poles, then because this is doubly periodic function, f has no poles anyway. In fact, f is bounded. Now, if f is bounded, I should have gone back and modify this and f is not constant.

Because, if f is constant, now obviously it is doubly periodic and obviously, this part three is false, because it takes only one value everywhere. I should also say z in f. So, there is how many values, how many z's inside f, are there for which you in the value w. Because, again if it is since is periodic, then there are infinity values on which you take particular value. But, that is not were obtained. So, consider f z minus w.

Then, this is doubly periodic, the same period. So, summation sum of order is this. This is zero. Now, if f has no poles, then it is constant. And if f does have a pole, then say we are that, n is the sum of all the orders of poles. So, sum of the orders of pole is l. Then, by true sum of the orders of zero must also be l. In fact, sum of the orders of poles is minus l, sum of orders of zeroes must be l, which is another way of saying that.

The number of zeroes of this function inside the fundamental parallelepiped are l counting, multiples at the last one. So, now l is the sum of the orders or of all the poles or rather, minus l is the sum of the orders of all the poles, because orders of poles are negative. If f has no pole, then inside the fundamental parallelepiped the value of f is bounded, because it is a compact set. And if value is bounded, it remains bounded by periodicity, it remains bounded everywhere.

Now f, a function which is which value f is of course, f is metamorphic. So, this is an again a old theorem, we proved. That a meromorphic function, whose value is bounded over the entire complex plane, is actually a constant. So, now coming back to this, to say that sum of the orders of f is zero. Sum of the orders of f at all the points, inside the fundamental parallelepiped is zero. Now, if you just separate these, the points at poles are zeroes.

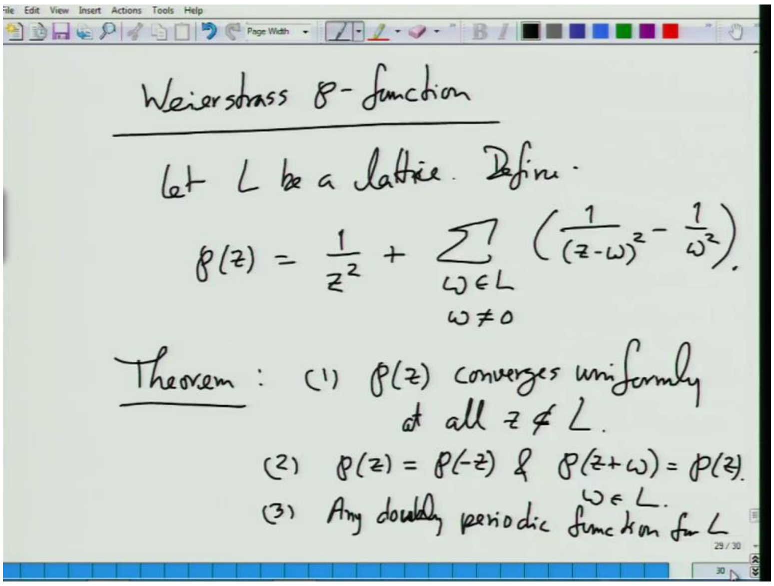
So, poles add up to minus l. So, zeroes will also the orders of zeroes, will also add up to l. So, what does the meaning of this? That, there are certainly zeroes of f in the fundamental parallelepiped. Further, their orders add up to l. So, applying that to this function, it means that there are points z inside the fundamental parallelepiped, on which this function is zero, in the f z minus w. So, it is a doubly periodic function with f capital F.

Student: ((Refer Time: 38:41))

Sorry. It is the same property because, this result that one and two hold for any doubly periodic function, which is meromorphic and as a fundamental parallelepiped l f. So, this f z minus w also in the same category. So, the point the theorem 2 or part of the theorem, part two of the theorem holds for this function as well. Now, poles of this function are same as poles of f. So, it borrows these poles from f.

But, zeroes of course it does not borrow from f, zeroes are other locations. But, what is guaranteed is that, some of the orders of zeroes is exactly here. So, that is a kind of function, we need. If you have to define a map from a torus to complex in plane, so what kind of maps can exist, which satisfy, because it is certainly well it in non trivial, in order to satisfy all these properties. So, there has this very nice.

(Refer Slide Time: 40:00)



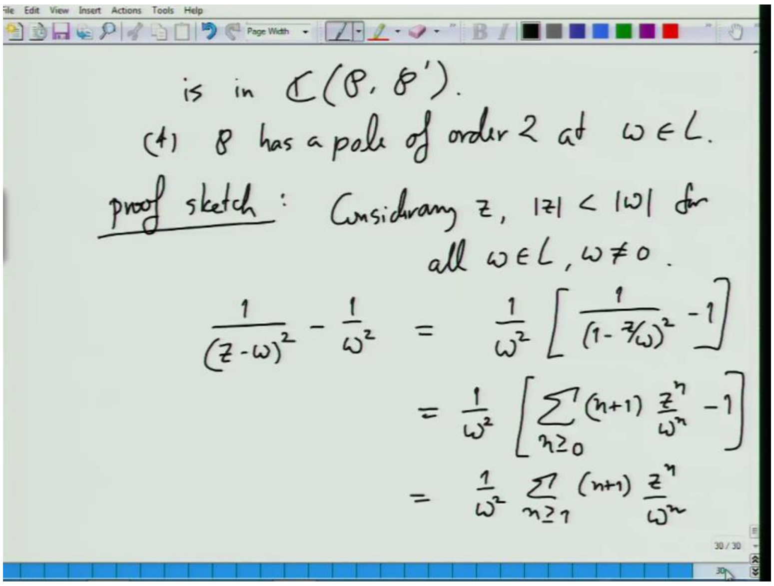
Weierstrass is, well I do not know. This is probably rho. Anybody expert in Greek alpha word, it does not matter. It is.

Student: ((Refer Time: 40:25))

What? Yes. It is, that is right. It is w l, does not matter. Let us call it whatever. Let us call it as rho, rho function. As long as we are clear, what it means. So, let L be a lattice. Then, define rho z to be this. So, it is 1 over z square plus sum over all lattice points, except zero. Because, in zero this will get messed up. 1 by z minus omega square minus 1 over z. So, here is a nice theorem about this. Says that, first ensures the convergence of f is well defined at every non lattice point.

At every lattice point of course, there is a pole. Second one is that, z is equal to rho minus z and rho of z plus omega equals rho of z. So, it is and this is for all w omega in l. So, this is doubly periodic for the lattice, over the lattice. And third is, this is even more interesting.

(Refer Slide Time: 43:15)

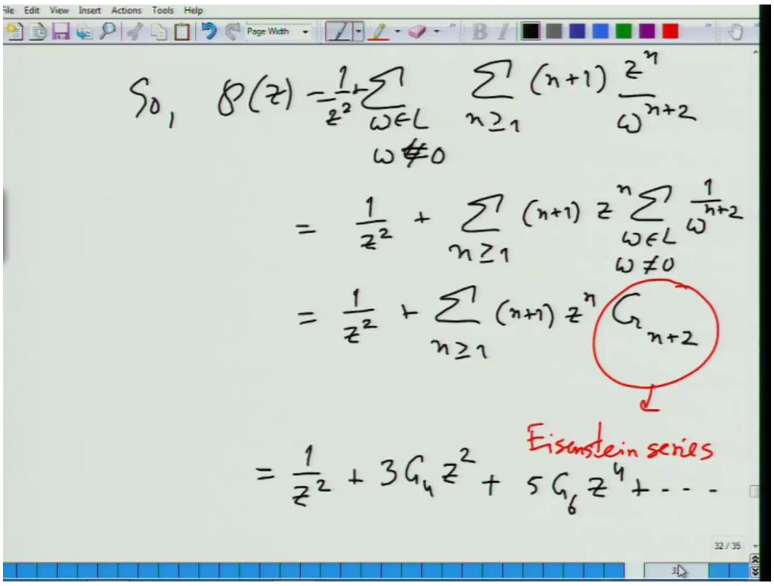


That any doubly periodic function over l, has this form. It is a rational function, which involves rho and rho prime. So, it is a rational function in rho and rho prime, over complex numbers. Any rational function over rho and rho prime is, obviously doubly periodic for lattice. And this part says that, that is all there is nothing more. And of course, rho has a pole of order 2 at every point in the lattice. That is also fairly obvious.

Just look at this definition. Any point in the lattice, there is a pole of order 2. To do a little bit of, or to ensure that the rest of the sum in the series convergent but, that is follow the essentially from part one. The proof of all of this is fairly straight forward not part three, which I am not going to prove. Even part one, I am not going to prove. But, I will give you a very brief sketch. So, if you look at. So, start by considering any point z.

So, that is absolute value of z is less than absolute value of omega, for all lattice points except zero. Then, for that particular z if you consider this expression, I can rewrite this as. And this, I am going to now use the fact, that absolute value of z by omega is less than 1, by using this property. And therefore, I can expand it as a power series. And the power series is this over this square, 1 minus x whole square. If you remember the power series of this, this is equal to. It means if I can write this. So, you get this.

(Refer Slide Time: 47:08)



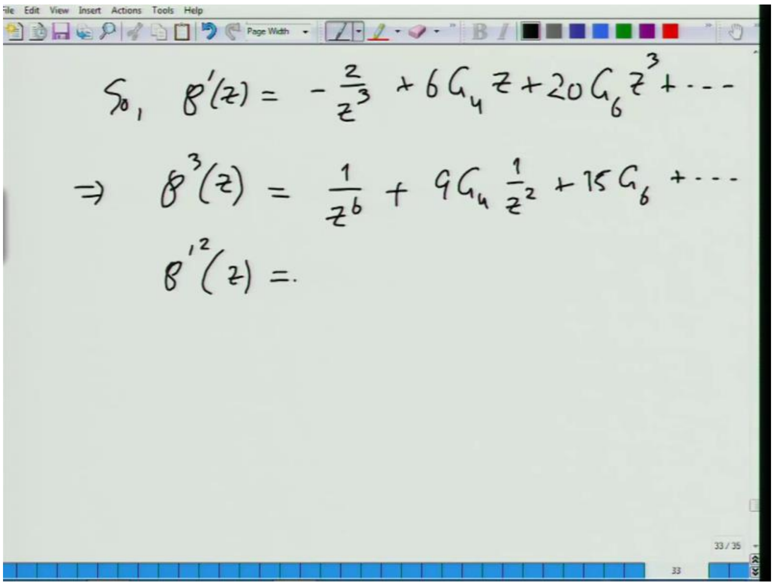
And so just swap over this sum, you get 1 by z square plus. So, just rearranging some essentially you get this power series. It is a Lorentz series with the coefficient here, which is sum over all lattice point, except zero of 1 over omega to the n plus 2. These actually on ensure converges and converges to the value, which is called the Eisenstein series. So, this is the n plus 2, Eisenstein series defined for that lattice.

So, this sum is an Eisenstein series. And in sum, it is like this. And simple fact about this is that. So, let me just we write plus few terms of this, 1 by z square plus. If you will consider n equals 1, then this is G 3. If you consider G 3, the sum is 0. That is G 3 is 0. Why? G 3 is 0 because, if omega is in the lattice, then minus omega also in the lattice. And so if you have an odd power of omega sitting here, then they will just cancel each other.

In fact, G odd is zero. So, this actually would be the smallest value. This will survive is 3 G 4 z squared plus next one will be z to the 4, with 5 G 6 z to the 4 plus so on. So, that is the power series expansion of rho around z equals 0. So, what were? Because, zero in the lattice. So, all linear combinations of, so zero. Say if omega 1 is in the lattice, omega 2 is in the lattice and all linear, integer linear combination omega, omega 2 are in the lattice.

So, basically that shows that, it converges. Convergence is essentially comes out of this fact that, you have. Let us do a bit of manipulation to get a convergent. That I am, I will skip over there. I will my mostly interested in this. And now, I am ready to give this map, which I promised that from a torus to an elliptic curve. So, this rho z expanded in a Lorentz series that on z equals zero, where it has a double port.

(Refer Slide Time: 51:46)



Now, consider the derivative of this. Rho prime of z, if you just look at this, what is rho prime of z, going to be minus 2 over z cube plus 6 G z plus 20 G 6 z cube plus etcetera. Now, let us do a bit more work. What is rho cube of z? And will only focus on those powers of z, which are negative or zero. The rest, we will just ignore. What are the non, what are the negative less and equal to zero powers of rho cube that exists.

Cube of this, square of this times this, that is also negative. Square of this times this is zero. No. Cube the whole upon, anything else. So, that is it they get only three terms, cube of this, square of this times this and square of this time this. Any other term will be higher power. So, what are those terms? So, you get 1 over z to be 6. That is a cube plus square of this times this. These three rho's, there is a three choose two times this. There are three times these, times this is a 9 by that z square plus square of this times this, which is 15 G 6 plus the rest and square rho prime.