Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

IIT Kanpur

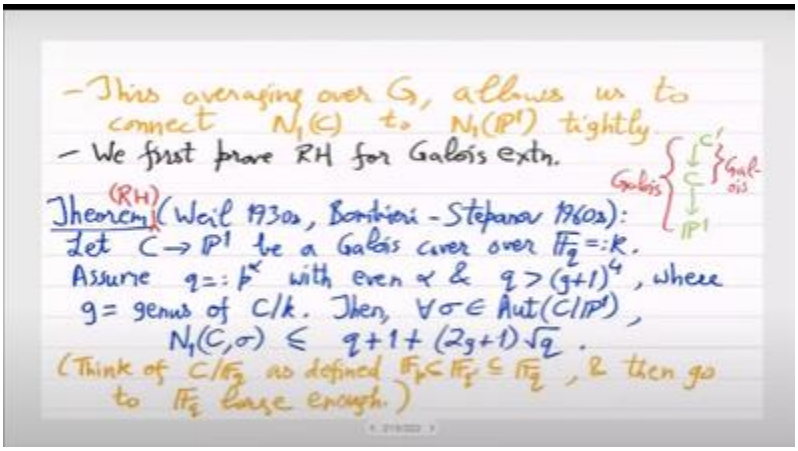
Week - 12

Lecture – 27

Cohomological Interpretation of Zeta function

Any questions? No, there you don't see the poles, right, because a function is not defined at the pole. Well, what it means is this DVR represents non-negative valuation. I mean when you are looking at a point the germs is basically this it gives you the DVR. No polynomial is just one element, I am saying the set of all functions that's the DVR. So that represents around the point, so in the germs this is non-negative valuation, 0 represents unique maximal ideal, sorry positive represents unique maximal ideal, 0 represents outside the maximal ideal, the germs. and then the negative which you are asking about pole when is the point pole those are the functions that are in the that are outside the DVR.

So, it is K - DVR those are the functions which actually are undefined at the germ and they have valuations that are negative in all possible integers. there is no geometric picture so because those functions are not defined at the point so they are in the complement of germs so the oh that is not clear yeah that I said in the very beginning that why Riemann came up with his Riemann theorem that is not clear to me.



I think it was natural for them in that century because genus was already defined geometrically and they wanted a computational way to compute genus. So, for them they were just looking at an alternate algebraic criterion and that happens I mean they must have tried many things and this thing must have worked.

But this you are talking about the Zariski topology. No, this is not enough for, to make sense of genus or holes. No, that is too weak. That is simply this algebraic property that close set you are looking at the zeros, so zeros are few, non-zeros are far more. So non-zeros basically is the open set and zero is the close set.

But that is a concept which is independent of genus. it doesn't know about genus, genus can be anything open sets will always be dense that's not enough. In fact anyways open set is something which is just sitting in the at the level of geometry while whatever interesting we are doing it's actually is happening in the functions. So functions are above the points and the functions are of three types. which are in the germ with positive valuation or in the germ but invertible and the ones which are not even in the germs.

So that for that precision you need the valuation negative 0 positive. But this still is not enough to see why, so this LD sheaf is actually technically it is called a vector bundle. So these are rank one vector bundles on a curve. Why the vector bundles are defined this way? I think I gave this motivation via the approximation theorem. So you want to understand what are the functions whose poles only come from this set of points.

So that must have been the basic starting point but it is still we are not bringing the holes here. So, why will such a thing measure holes that must have been just an accident, accident mainly by Riemann. So, it is really coming from one mind, whose Riemann hypothesis today we will finish. So, let us start any other question. Okay so the place where the theorem that we want to prove is in this format.

So for a Galois cover of the projective line and over a finite field of size q the prime being p just assume that the size of the field is sufficiently bigger than the genus. this we can always ensure because genus is limited by the degree of the curve while q is unlimited so we can take sufficiently with q. Then we will show that these points n1c sigma the Frobenius action is the same as his sigma action those points are q + error term upper bounded by that. So, this is not saying anything about lower bound, lower bound can also be 0. If you show this then we have seen that Riemann hypothesis is implied.

So, what is the proof of this? So, if N1c sigma happens to have one point, take call that point P on the curve and then with respect to that define these LD sheaves. so use L of AP take A to be big enough so that is one and second is LB again B is big enough and we

use two different pullbacks so we use the φ which is basically sigma $^{-1}$ Frobenius that is La φ and we use a different Frobenius which is the basic absolute Frobenius raised by prime p μ times, so p raise to μ Frobenius that is Lb p μ is the pullback of this sheaf which is explicitly just that, it is just f composed with the morphism, f comes from Lb. So remember that this F has, if it has a pole it can only be the point P, it cannot have any other poles. So we are focusing on really this, outside the germs at P, the point P. And we have these injections, LFI functions are basically just, they are sitting in L of aq and similarly Lb p μ is sitting inside L of b p μ.

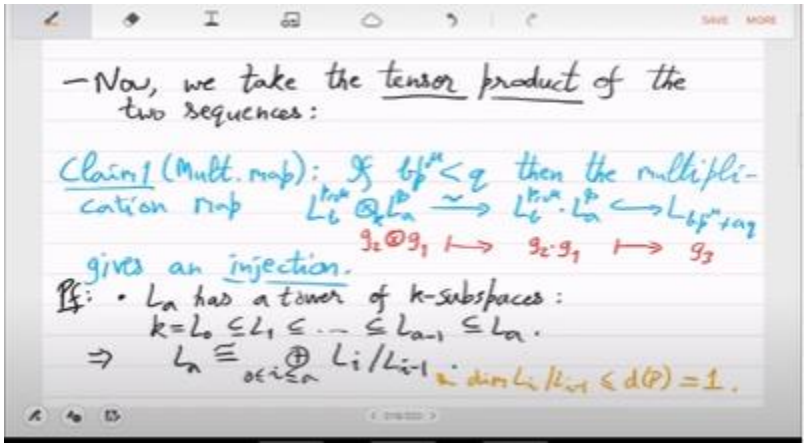
This is simply by the definition of the map. And now what we will do is we will multiply these two sequences. So, how do we multiply? We just basically we formalize it by tensor product of vector spaces. so that is the multiplication map so we are saying that as long as q is big enough compared to bp μ this multiplication map what it does is that it takes a sum of tensor products and maps it to a sum of actual products so now g1 g2 is just a function and by the sequence by the two sequences you can see that g1 g2 is actually a function in L of bp μ + aq. So we are just so I am simply calling g1 g2 as g3 in general it will be the way this action will extend is you will have a sum of rank 1 tensors each rank 1 tensor will be converted to a polynomial by multiplication and then you sum it up.

so you remain in L of bp μ + aq that is an injection. The first arrow may not be an injection because well it is a sum of rank 1 tensors when you multiply it may be 0 that is very much possible because tensor may not behave well with functional multiplication, ring multiplication. So, for that we need the assumption Q is large. So, why will it that suffice? So, yeah this is a tricky proof, it is not immediately clear what is the connection of this injection with Q being large. but you will see very soon that this q being big is important, is critical in fact.

So, L a has a tower of k sub k spaces. So, k is L 0 then you have L1, LA - 1 and LA and so this actually gives you a decomposition of LA as this sum So this is recall what l1 is, l1 is just l of p, the point p and l2 is and la-1 is just l of a-1 times p and so on and so they are naturally, there is a sequence of subspaces, tower of subspaces. So you can do mod li vector space modulo of subspace. some now we do not know which ones of these are 0 and which ones of these are non-zero, because sometimes Li - 1 may be Li. The theorem we had was only about subspace in LD sheaf, we did not have exact result.

So, we had exact result for Adels right, but not for the LD sheaf, but anyways there some will be La. and we know that the dimension of this is less than equal to degree of the point which we have 1. So these are really either these are 0 or these are cyclic subspaces vector spaces dimension so which means that there exists a k basis f1, f2, fr are at most a

of La such that for strictly increasing valuation right. This is possible because you just look at these 0 or cyclic quotient vector spaces and the generator which you get for example, from L1 | L0| versus L2 | L1| by the definition of this LDC if you can see that the valuation is actually decreasing So basically what li | li – 1| is, is l of ip | l of i – 1| p. So if a function exist here f then it means that, what does it mean? So the function of course can have only poles from the point P, it has no other poles.



So whatever you will get from Li + 1 | Li| and whatever you will get from Li | Li – 1|, there will be a difference in the valuation. Should I say like that? so now valuation which way is it so f2 will have a bigger valuation right hopefully this should be clear because f2 comes from more possibility of more multiplicity of P its I + 1P, while F1 comes only from IP. And notice that LIP is being is the modulus in the second one, so since it is the modulus what you will get will genuinely have a higher order of P, I mean higher pole. p will be a pole of higher multiplicity. But then may be since it is negative I think it is the opposite way, it is like this, it is - i versus - i + 1.

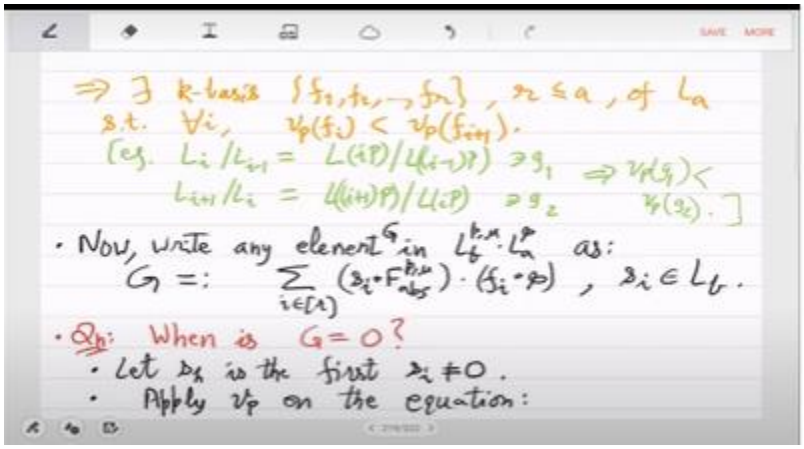
Yeah, so these are different valuations and you can just arrange them in this way. so let us not use the same f so we have found this basis and now we write from the hypothesis this LB tensor LA. So, any element g in the product or equivalently from the pre-image which is the tensor product, any element g will can be written like this. It is Si composed with absolute Frobenius p μ times Fi composed with φ, i goes from 1 to the Si's come from Lb, because something from Lb p μ that's Si composed with absolute Frobenius p μ and something from La φ which is, which La we have fixed a basis using Fi's, so just write in that basis Fi composed with φ in this order. Yeah, but you just LA has a basis F1 to FR.

So you just have to look at that and for each FIFI collect everything as SI. No it is not a dot, no it is not really a dot product, it is just simply a product. I am just writing in terms of the basis of second component which is F1 to Fr. So with F1 whatever kind of think of

it as collecting the coefficient of F1. So the coefficient of Fi is Si.

So I am just collecting the coefficients together. So the question is when is g 0 because we want to show injection. So that is violated only when g = 0. So let us check this. So this the way we have sorted Fi increasing valuation what will happen and the Fi φ actually raises to Q.

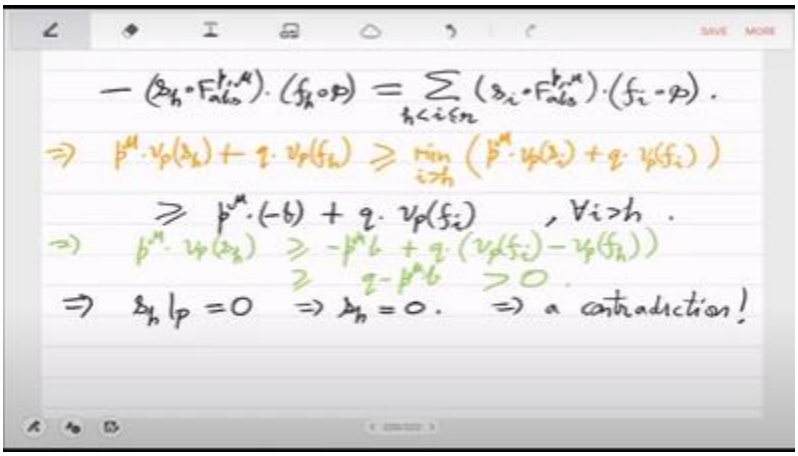
So the gap of 1 in the multiplicity or in the order of P actually scales up by Q. So what is happening is in the second component the valuation with respect to P is growing very fast, it is in step of Q. and so somehow intuitively si's cannot cancel. So, we will show this by the only order we have which is order of p. So, let us apply let us first say that sh is the first non-zero si and let us apply valuation on g.



So let me write down the equation, equation is - SH, sigma i goes from H to R, so on this when we apply the valuation we will get so p raise to μ times the valuation of sh that's for the first factor at the sh factor for fh factor you will get q times this and then it is a sum, so valuation on sum is greater than equal to min over i + q times fi. Right, this is clear. Left hand side valuation has to be at least valuation of each of the summands and valuation on product is additive. So, we only have this operator available because both SH and FH only poles we know are this point. So, we just apply this, we do not have any other information.

This will suffice actually. so now this is greater than equal, so the min of this is at least, min of Vpsi is, it is all coming from lb, so it is at least - b and which implies that, P^{μ} VPSH is at least - $P^{\mu B}$ + Q times and sorry this was all Yeah and valuation of Fi - Fh is at least this difference is at least 1. So you get that this is at least Q - $P^{\mu B}$ which by the way is positive because we assume Q to be large. So what this is saying is that Sh has P as a 0, point P as a 0. but sh the only possible pole is this point p and you are saying that

this is a 0, so that is not possible this means that actually sh is 0. It is a rational function it should have 0s and poles, but if both of them only possibilities point p then essentially 0, it is a 0 function and that is a contradiction.



so this contradiction implies that g is not 0 which basically means that g was an arbitrary element in this lb times la so you get that to be an injection. so this is a really neat trick that we can now actually combine the two sequences by tensor product and the replacing it by multiplication keeps it there is no information loss so let's draw that diagram now no sh was the first si not equal to 0 by definition of sh so this is the diagram So, this will be the most important diagram of this course, because this is what proves the Riemann hypothesis. So, there is a map from here to and this is the tensor product version so this is by claim 1, by claim 1 this is actually an isomorphism, it is injective but also these were finite dimensional vector spaces. So, we actually get an isomorphism and this is the multiplication happening. So, you can think of this as a commutative diagram which takes from Lb p μ La tensile product to La φ then it multiplies which is there is no information loss and tau maps that thing to Lb p μ La.

What is the map? I mean φ is the essentially this Frobenius map. So if you apply the inverse Frobenius then every element on the LHS has a associated natural image in LB p μ LA. So that is the well defined linear map, just applying φ^{-1} on the this component. Yeah so this I mean the multiplication map or equivalently the tau map, this may not be injective. So claim 1 does not say that it is injective.

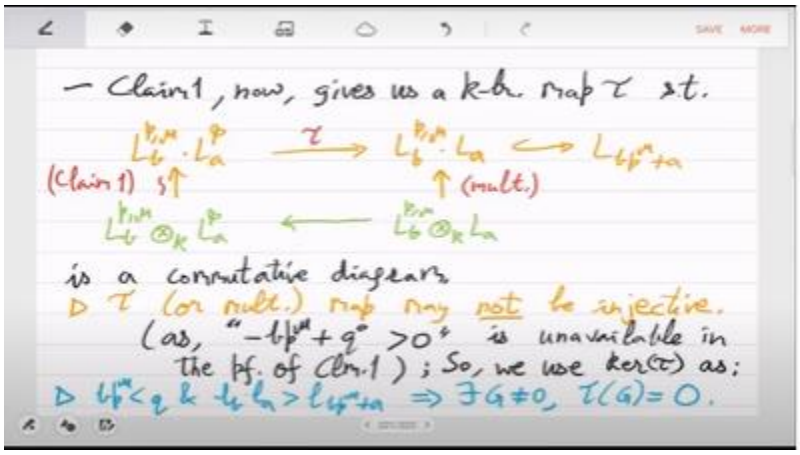
why not because see this its La it is not La $^{\varphi}$ so La $^{\varphi}$ had the advantage of Q being there which is bigger than Bp μ but in the middle one this La. this actually there is no q present, there is only bp μ is present but with a there is no q. So claim 1 does not apply here as - bp μ + q^0 is not positive. So claim 1 required - bp μ + q to be positive, but there is no q, so here actually you only have q^0, there is no φ present, so you cannot run that proof here. So claim 1 only applies on the first vector space, not on the second vector

space.

So multiplication is not, may not be injective and then tau may not be injective and what this will give us. is the possibility of a polynomial g such that tau g is 0 and that is what will prove the Riemann hypothesis. So just observe that. if we assume b p μ <q and we assume that l b l a > l of b p μ + a then there exists a non zero g such that tau g is 0.

Okay that was fine. Implicitly g is in the first vector space and its image is 0, so it is in the kernel of tau. This exists because I mean bp μ < q gives you the injection by claim 1. lb times la big means that the middle vector space sorry the first vector space that it has dimension exactly LB times LA, right because it is actually isomorphic to the tensor product and the tensor product has dimension LB LA. So, the domain is big while the range is small. So, there has to be an element in the middle which is vanishing under tau.

so we use kernel of tau as follows. We pick this element big G which is now guaranteed to exist in the kernel and let us study that. So the representation of G is exactly as before i 1 to r write in that basis such that tau g what does tau g do so tau g is it just removes the φ in the end. and then it vanishes. So, with φ it was not 0, but without φ this is vanishing.



So, we have found this polynomial. Observe that g is a p raise to μ th power is this clear because the si part is clearly p raise to μ th power, the fi part is q th power and q is at least p raise to μ. So, the whole thing is actually a p raise to μ th power. So, g is a p raise to μ th power polynomial with this property tau of g is vanishing. Now let us, so the interesting thing is that these points that we were interested in N1C sigma, so any point big P or Q, any point big Q which is fixed by φ, notice what will happen.

When you evaluate G at Q, φ Q will become Q. so you are evaluating tau g at q that is 0. So all the points that we want to count are 0s of g. So that is the major property this was

Bombery's construction such that φ q is q g evaluated at q is actually tau g evaluated at q which is equal to 0, right. So the points that we want to count they are actually roots of this, they are zeros of this polynomial g.

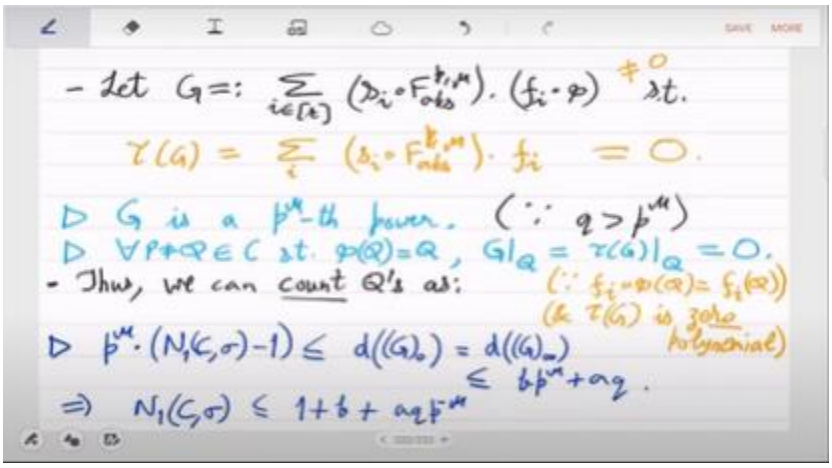
Just look at the evaluation of G on Q. So, the Si part on Q and the Fi φ part on Q. So, Fi φ part on Q is what? Fi Q. So it is as if φ is absent there which means that you are actually evaluating tau g, but tau g is identically zero. As a polynomial it is zero without any evaluation.

So tau g is absolutely 0. That is the magical thing. So we have actually constructed a polynomial g which contains all these roots that we want to count. Now all we have to do is control the degree of g. What is the degree of g? Thus we can count q's as. So first of all p raise to μ times n1 c sigma - 1 because we have I do not want to take the point p because the point p this s i f i they actually may become infinity. So I do not want to take p but for all other q's g vanishes.

So that is n1 - 1 + g is a p raise to μ with power so we have a saving there right. So it is actually p raise to μ times this that is less than equal to degree of the 0 part of this principle divisor. we cannot directly say degree of g we have to do it formally so the formal way is you look at the principal divisor of g look at how many zeros it has that's the degree of g0 which you know is equal to because of rational function also g infinity which means the poles of g but what are the poles of g well poles of g are given by the Rn sequence, so poles of G Rn multiplicity is bp μ + a. Is that right? That is not right.

Let me draw a branch here. branch is that this is, it embeds in b p μ + a q this branch. The g sits there and it is really an element of l b p μ + a q. So, that is the how many poles it can have, what is the multiplicity. which means that we have a count on n 1 c sigma that is 1 + b + sorry. Yeah the d of a divisor is the both the coefficient and the degree of the point.

So, degree of the point is 1 because we are in k bar, f q bar and multiplicity is what you are summing up. So, that is LHS and then the 0s you can switch to now poles. For poles you have information of g because of the embedding in that LD sheaf. So now N1 C sigma is this, correct. But remember that we have A, B and μ all free, we never fix them.



So once we fix them, you will recover Riemann hypothesis. So let us just fix and finish. So we can fix A, B, μ by parameter chasing. So, let us see we have to ensure all the constraints. So, take μ α by 2, which basically means that whenever you see p raise to μ, it is actually √ q, q was p raise to α.

So, p raise to μ is basically √ q. So, what that will give you is a big saving, the √ q is multiplying n 1. in this calculation. So, there is a saving which is happening in the multiplicity and a q p - μ becomes a √ q. So, that a part will basically become the main term and b part will become the error term that is the plan.

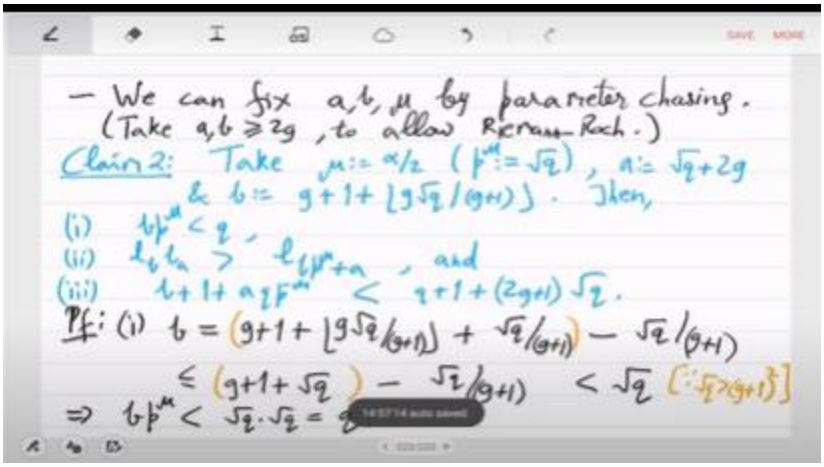
So, for that let me fix a to b. and b to be. So, these are the conditions that will be simultaneously satisfied q is bigger than bp μ. L a is big and finally, this bound b + 1 + a q p - μ this is smaller than q + 1 + 2 g + 1 √ q. So this is the fixing, so we take AB to be just bigger than 2G to allow Riemann rock application. So, for Riemann-Roch this LDC correspondingly this A and B parameters they should be bigger than twice the genus. So, I have made sure that A and B are just slightly above 2G, B is in fact Well a is clearly bigger than 2g, b is a bit more complicated because it seems that it is close to √ q but remember that √ q is bigger than g^2.

So b is also much bigger than 2g. So both a and b are sufficiently large. So we will have control on lb and la and p raise to μ is √ q. there is some intuition in this fixing and once you fix this you can just do the calculation it works. So, this is now just simple verification. So, what is b? So, let us first see what b is, b is g + 1 + and what is this part? So, this part is less than equal to √ q + g + 1 Why is that? Yeah, that should be just let me write in the correct order then it's clear.

Write the third and the fourth term when you sum it up. you can see that it cannot exceed

√ q because you get basically g + 1 by g + 1 and this overall < √ q. Why is that? That is because this g + 1 - √ q by g + 1 is negative. We took q big enough, so because of that it is smaller than √ q. √ q is basically greater than g + 1 ^{2} right.

So, this is negative. So, you have less than √ q correct. So, now b is upper bounded and which means that b p μ < √ q times √ q which is q. So, that is the first property b p μ < q. So, your claim 1 will work fine. Let us now check the existence of G by checking condition 2. So, condition 2 is LB LA by Riemann rock, this will be b + 1 - g times a + 1 - g.



So, let us check whether this is greater than bp μ + a + 1 - g right that is the bp μ + a LDC. So, all three expressions are given by Riemann-Roch theorem because we have made sure that these numbers are bigger than twice the genus. So, when is this greater? So, that is another sequence of calculations. So, when b - g times a + 1 - g > bp μ. right that is just subtraction on both sides if and only if > g.

so you multiplied by g brought on the right side and brought bp μ on the left fine if and only if So what is this? This must be coming from e I think, e √ q + 2g, just coming from there. and p raise to μ is √ q. So, left hand side simplifies right hand side also simplifies and which means that you want b to be greater than g times 1 + √ g over q + 1 or g + 1. and is that true b indeed is bigger than that right we took it to b to be 1 more than that that is also checked and the last condition now which is b + a √ q + 1. So, what is the upper bound for this? so this is equal to b is g + 1 + and a √ q is what + 1.

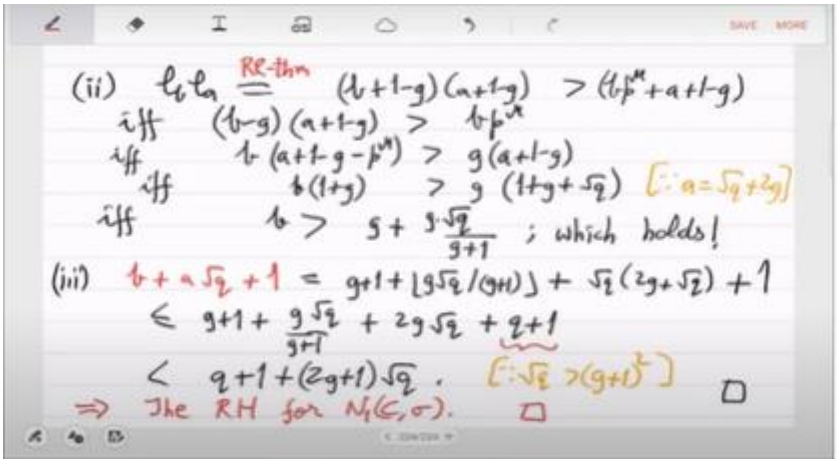
what the LHS is, we have to upper bound this. So, this is less than equal to + q + so essentially the main term that you see here is this q everything else is error. The main term is q + 1 and others are just yeah they will basically give you this 2g + 1 times √ q

which we wanted that's the error term in the Riemann hypothesis. is that right. Here again this last this g + 1 + g √ q by g + 1 this is less than √ q that is what we are using. Yeah that is all, so this all the conditions are checked and ultimately we have an upper bound on n1 c sigma to be q + 1 + 2g + 1 √ q, so that finishes the proof of the Riemann hypothesis.

and then from n1 c sigma you can go back to the to the reductions and for all curves it is proved correct. So, can just state it for any smooth projective curve C over Fq, genus G, the roots α of L t, the L function satisfy the norm of α is √ q and number of points on the curve. and on the projective line that is q + 1, this difference is at most 2g √ q or - between - 2g √ q and + 2g √ q. because l function has only 2g roots, each has norm √ q. So, you get the error s, I mean sigma α i is 2g times √ q + -.

That is the major theorem which took 4 months to prove and so this implies that. if you take q the main term I mean you should have to take main term much bigger than the error term for this to be interesting which means that you take q to be more than g^2. the number of curves is around q + 1. So, if you go to a field which is sufficiently big then the main term is almost q + 1. So, you for a large enough finite field you start getting as many points on the curve as you have on the projective line.

Yeah, yes exactly that is the Riemann hypothesis. and this has innumerable applications, we do not even have time to name them. So, one thing which is quite popular is whale estimates. So, RH has tons of implications for example in computer science we generally use this vale estimate let's state it so vale estimate for character sum so let chi be the character which maps finite field elements to + - 1. So what this character does is essentially it on α chi α is 1 if and only if α is a square. So we can write this explicitly also be the character that maps $\alpha^{q-1/2}$.



So, this is yeah Q is not may not be a prime even then do we call it logian symbol I do not know yeah, but when Q is a prime. So, this is exactly logian symbol, but in bigger finite fields this is basically the criterion of when α is a square. inside that field. Of course, it is called square in FQ bar, but in FQ half are squares half are non squares. So, that is the that is given by this character it is a multiplicative function of course.

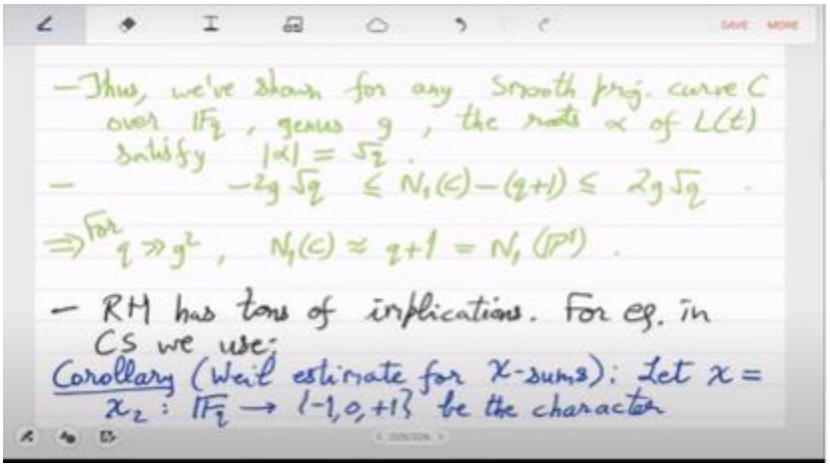
So, what is the Whale estimate? So, Whale estimate is interesting in looking at let fx be degree delta polynomial, then the character sum is chi f α over all α. So, what can you say about the character sum over an arbitrary polynomial? So what do you think and you are summing it up on the, essentially on the projective line, on the whole line you are summing it up over the whole field basically. So the thing is f α or fx sometimes it will be a square, sometimes not square, sometimes 0. Yeah, so it should be something like sigma chi α, now sigma chi α is actually 0, because pluses and minuses are equal distributed. So, Weil estimate says that this also is almost equally distributed with the error √ q constants in delta.

So, this is called the vale estimate for character sums. Now, it is very easy to prove. It is a major thing we use it in many, many applications. Wherever finite fields are involved you will see a vale estimate. So, all you have to do is consider the curve C for the function field. fq x y mod y^2 - f. So, the function field is given by this polynomial fx like this y^2 - f, this by the way is called a hyperleptic curve, you will see this in assignments.

So, for this transcendence degree one field there is a smooth projective curve, there is a model. and on that you apply a Riemann hypothesis. So, why will it help in character sum, well because character sum is measuring, how many times is this 1, how many times is it - 1. and how many times is it 0, well when it is 0 it won't count. So basically the difference of 1s and - 1 incidents, so let us rewrite it as so what i have done is i have added number of times its 1 both sides so then now in the second summand i am looking the first summand becomes double second summand i am looking at - 1 0 and + 1 actually should not say 0, 0 does not count.

So, how many times - 1 and + 1. So, that is essentially q except the places where f α vanishes which will be at most q - delta. So, I can write this as the first one is essentially the number of points on the curve and the second is q + something dependent on delta. Is that correct? The twice of ones is the number of curves because whenever f α is a square it gives you 2 y's. So, that is why it is counted 2 times. So, that is the number of points on the curve which you know which - q you know is √ q.

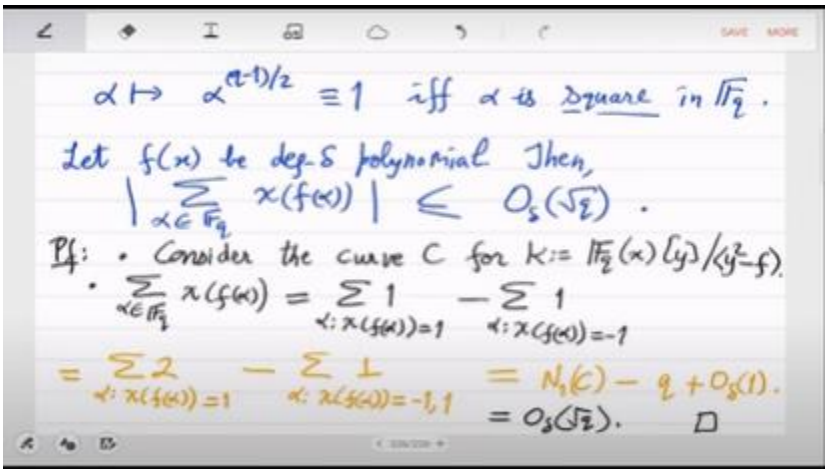
So that is all, that is you get this by Riemann hypothesis that no matter what polynomial you take I mean as long as it is not of a very big degree the residuosity is equidistributed all over the field.



So you can do this for other exponential sums. In analytic number theory there are many other exponential sums available, Gauss sum and variants of that, where you can use both a multiplicative character and an additive character. and you can mix them. So, for those you will have to look at the appropriate Riemann hypothesis and you will get these bounds.

So, this is a very powerful translation of Riemann hypothesis. What else? Yes, so the computational questions are open. given a curve over fq, how do you compute n1c, in poly log q time. So, assuming that the finite field is very large, so you can see q only in binary if you did brute force it will take q time which is exponential can you do faster so this question is open we have proved Riemann hypothesis and we also have this L function etcetera which knows everything but it is not clear how to compute the L function the zeta function computation is equivalent to this question The second is, is there another interpretation of LT that can help in computation. So, is there another interpretation of the zeta function I mean alternate to what the way we started which is counting points over all finite fields.

because that is the question one. So, we cannot rely on counting to compute zeta function, we want something else, something more geometric or linear algebraic that we can implement in an algorithm without worrying about counting. So, Weil himself actually gave at least one more interpretation. on which much of modern math is based, so it is called the cohomological interpretation of the zeta function. So, I will just quickly sketch that and then we will finish the course.



So, cohomological interpretation of So, essentially what he observed with some very clever tricks is that this L function, L polynomial it is the characteristic polynomial of the Frobenius map.

So how did you reduce that, so let us quickly see this. So we have to see the Frobenius which for us is Qth Frobenius as an isogeny. So what is an isogeny? Well it is too late to define in this course now, but let us anyway do it. So, isogeny is essentially it will at least be a morphism from curve to itself, but it will be more because now on the Jacobian we have a group structure. So, isogeny will also preserve the group structure.

So, an isogeny α, so let me say here isogeny on j. on the Jacobian. So, isogeny α is a map from the Jacobian to itself. which is surjective with finite kernel. So, essentially it is an it is an automorphism but just a bit more relaxed because it is not saying that it is injective, it is just saying that it is the kernel is finite because there could have been infinitely many points in the kernel but no there are only finitely many. For the Frobenius actually the kernel is 0, it is only the 0 point which can go to 0. but this doesn't work for other interesting morphisms, so which is why we need to add this finite kernel into it.

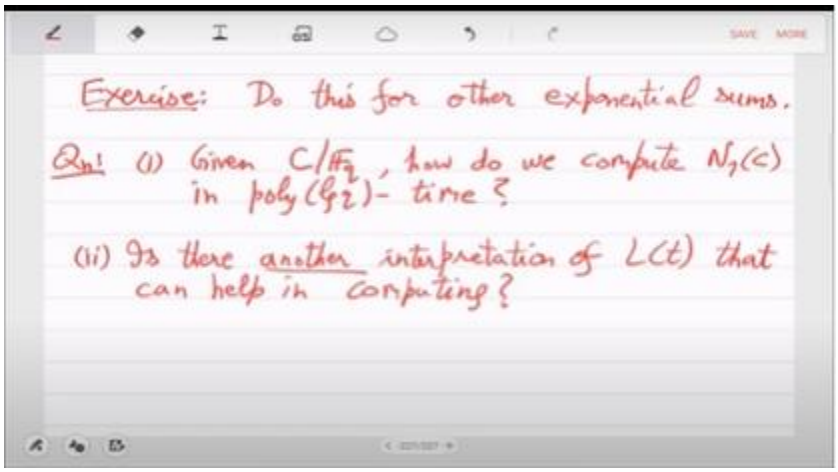
Otherwise you will be restricted to only Frobenius and then you can't build a theory. So let me describe that later, so it's finite kernel and it respects, it's not just geometric It respects the group and the variety, because we want the group to be preserved also. Now we have a abelian group structure. So, which is why it is we have invented a new word it is not morphism, but it is isogeny.

It is morphism in the category of abelian varieties. varieties which are abelian roots. So, the right term is isogeny here and since the kernel is finite we can define that as the degree of the isogeny. So, this is basically the size of the kernel. So, isogeny and its associated degree these are the two things So example 1 is of course Frobenius, let me call Frobenius as π throughout.

So Frobenius is an isogeny with degree 0, sorry degree 1. the kernel is the zero point. So, it is basically an automorphism of the Jacobian, but there are more interesting isogenies. So, take a number and define multiplication by n. right because J is a abelian group, so any point D sum of basically it is a divisor, any divisor you can multiply by 2, 3 or even - 2, - 3, - 1 so on. So this is an isogeny, this respects the group structure of course and why is this an isogeny, why is it subjective. It is subjective because any d prime that you want in the image, you can essentially identify 1 by n times d prime in the algebraic closure.

So intuitively it is subjective and why is it finite kernel, because for that you have to see how many d's are there such that nd = 0. This is another constraint. I mean you can, we will actually see that this also will be only finitely many ds. I mean anyways the, if you restrict the finite field then j is a finite object, it is a finite group. So, you will go to a big enough field where all the nd = 0 are present so that also is intuitive that this is an isogeny.

N is an isogeny, what is its degree? Yeah, so surjection and finite degree is still intuitive. what is very tricky is calculating the degree, for this we will have to work hard, but now since we have the Riemann hypothesis and all we can actually reach it pretty fast.



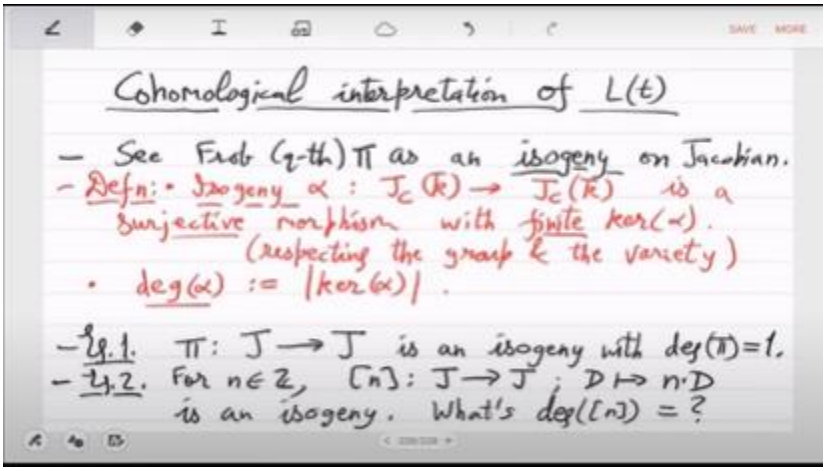
So let us do that, let us do the degree calculation, so for that I will need one more thing for prime L, define this kernel which is a finite set, it is a finite subgroup of J. So, this we call L torsion of J. the L torsion of the Jacobian and we denote it by JL. So for example, for 2, l = 2, 2 torsion is, they are all these points in J whose order is 2, 2 times that point is 0.

This was also a question in the assignment, identifying the 2 torsion, but you do not have to stop at 2, you can do not have to stop at l, you can do l^2, l^3 and so on. that kind of gives you j of l infinity look at all the powers of l look at all these torsion points that is

called t l j or the tate module well let me not called it tate module let us just continue with l torsion so the T l j basically just the l power torsion part of j is kind of j l infinity. How do I write kind of this. So, TLJ contains all the L power torsion points.

and finally any isogeny α from j to j gives an isogeny on the alytic torsion. simply d to α d. Note that since α is an isogeny it respects the group structure if L times d is 0 then L times α d is also 0. So isogeny naturally maps this L torsion or L adictorsion points. to alladic torsion points. So, we will basically work with TLJ and TL α that was originally wales idea and what wales showed.

T L α for α which are kind of combinations of the Frobenius and numbers. So, you can basically take. powers of π and you can take powers of π you can multiply with n that is again an isogeny and you can add such things. So, you can actually develop polynomials in π and n all these are isogenies and we will see what it does on the eladic torsion. that is how we will prove some fundamental new properties of the Frobenius map and zeta function. So here is the list and these are actually not difficult to prove, we will see the sketch very quickly.



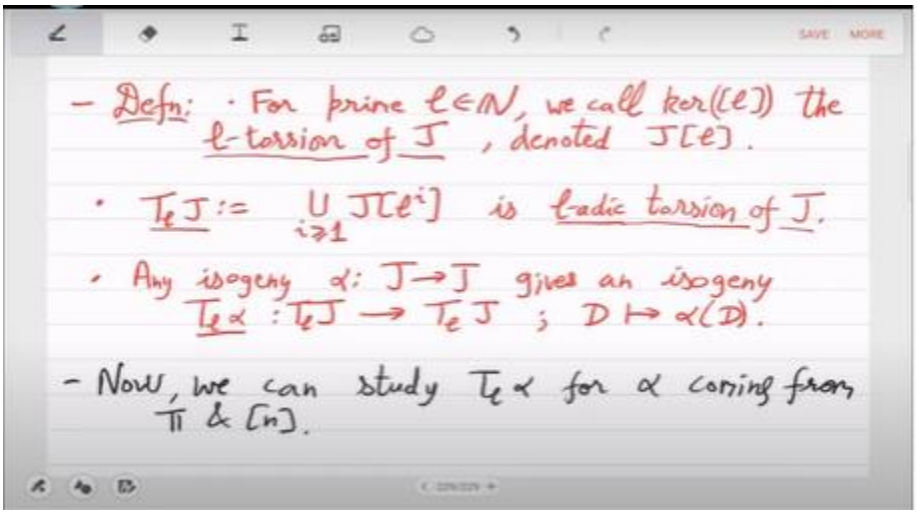
So first is that linear map. π on t l j has characteristic polynomial l t. So, this is the cohomological interpretation I was talking about that if you see well Frobenius is a linear map because on 2 or d 1 + d 2 π acts as first + second. So, you can ask about its characteristic polynomial that happens to be the L function.

Second is TLG has a nice structure. So, in particular TLJ is a finite rank ZL module. So, ZL is the alladic numbers. You can think of this as Z model, Z model ^{2}, Z model ^{3}. So,

whatever power you see That part of TLJ is actually just direct sum of say Z mod L^i and even in the Eladix it is actually a finite rank saddle module. So this basically follows from the first. The reason is that if characteristic polynomial is l t which is degree 2g, so from that you learn that Frobenius is acting on a 2g dimensional vector space.

So that makes TLJ essentially 2g dimension. And third is for any n, degree of n now gets calculated is the same proof as b, so it comes out to be n^{2g}. And so, if you look at the n torsion points that structure is C $|n^{2g}|$. So, the n torsion points are again it B was for L prime, C is the composite n, but it is the same result. So, you can count now how many n torsion points there are, they are exactly n^{2g} and that group is basically Z |n|. 2G many cycles. So, these are the structure theorems that Weil obtained with the cohomological interpretation. So, why does A work? What is the idea for that? We actually have all the machinery available. So, look at the isogeny π - 1, what is the degree of this? So this essentially is N1j, like these are all the points that are fixed by Qth Frobenius, so Fq rational points. So this is jk size of k rational points on j, which is also the same as the degree 0 class group. which we called hc and which is equal to l1, this we have seen before and l1 is the product of 1 - α i, so I can actually reverse it also.

So degree of π - 1 is product of α i - 1 where α i are the 2g roots of the L polynomial. This we have seen, this we know, so that is just a recall and similarly for all m what is the degree of π^{m-1} is the same thing instead of fq you are now going to q^m right which should be what which now will be α_i^{m-1}. because of the base change of L. So, you change the base field we have seen that all that happens is L function the L polynomial change the α is get exponentiated by m right this we had seen in detail. So we have now an understanding of degree of π raise to m - 1 for all m, it's just product of α_i^{m-1}.



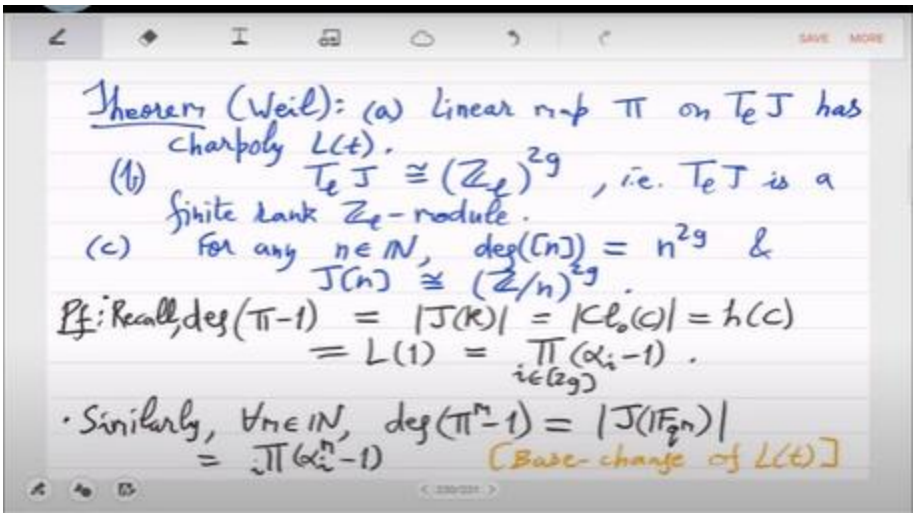
So that's all you have to interpret and then you will get Whale's theorem. So α i's were in complex, but we can also see them as alladic. so they are in complex, but they are also in now QL bar. You go to alladics instead of integers, you go to alladic integers and then take the algebraic closure, so that is QL bar. So, we can think of α a as being simultaneously a complex number, but also an alladic complex number.

This can be formalized it is quite straight forward. So, the important thing is that now So, let π act on t l j with eigen values β i, suppose that so π is definitely on t l j it is a linear map. suppose that its Eigen values are these β i's which are unknown we do not know them currently. But once you make this assumption what should be the degree of pi^{m-1}. Because we have a formula for π^{m-1} that we have written before in terms of α is.

Let us now look at the meaning of degree of π^{m-1} acting on TLJ. So this is equal to TLJ mod, do you agree? So the kernel of size of the kernel of π raise to m - 1 or any α, size of the kernel of α is essentially the space, the vector space on which it is acting modulo α image of that vector space, the size of that. Kernel size is basically equal to co-kernel size, this you can prove just by I mean this is straight forward by linear algebra and now what is this, this co-kernel size is the determinant of the α, where this is acting I mean the TL version of this. and the determinant is equal to product of eigenvalues. So, eigenvalues of these are β i m - 1 is that clear.

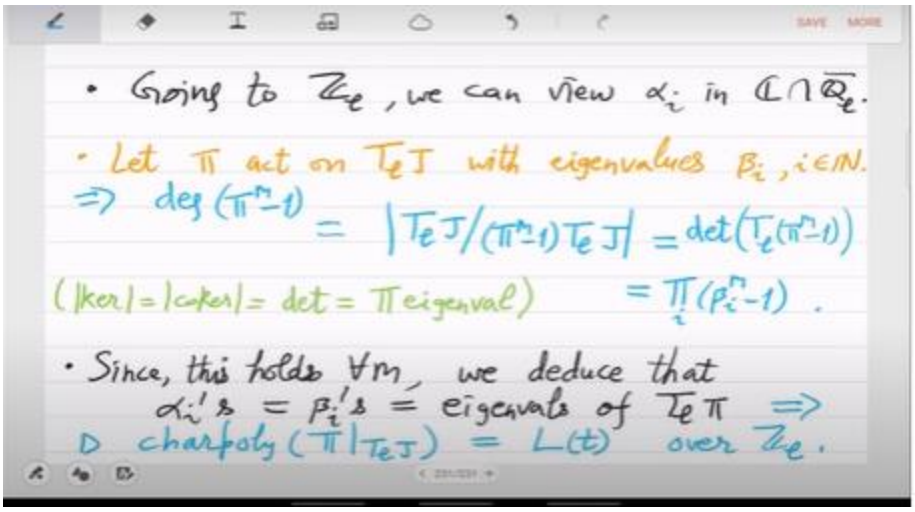
So, basically kernel size is equal to co-kernel size is equal to determinant which is equal to product of eigenvalues. That is the sequence of purely linear algebraic connections that we are using. So, degree of π^{m-1} is nothing but product of eigenvalues which if π has eigenvalue β i then π^{m-1} has βi^{m-1} eigenvalue and now you compare the two formulas. this is the β e formula and that is the α e formula they are the same which means α i's are the eigen values of π which means l is the characteristic polynomial of π.

Since this holds for all m. we deduce that α = β = eigen value of t l π which means that π on t l j. has characteristic polynomial. L t over Z L. So, if you just look at the eladic torsion part of J, characteristic polynomial of π matches that of L t, right.



But, eladic is characteristic 0. So, it actually matches exactly over integers. So that is it right, so this is the cohomological interpretation of the Frobenius, if Frobenius on the Jacobian has characteristic polynomial L t. okay and it actually implies b and c, b and c are implied by the degree of by degree of l equal to 2g and l torsion respectively, so l ^{i} torsion respectively n torsion Basically these L torsion, N torsion they will be finitely many points. So, the group that you are looking at is actually a finite group. What is the size of the group? What is the rank of the group? Those things get I mean basically come from the degree of the characteristic polynomial that is 2g.

So, this immediately you get the main thing is part a. that is an amazing result. This is in addition to the Riemann hypothesis, I mean this is not really using √ q norm of the α i's. So, it is an additional result how Frobenius acts on eladic torsion. But yeah once we have this it is a great computational insight, there are algorithms based on this and still there are open questions.



So, this has not been used completely. So, these are computationally, these results are computationally useful. as one can do model computations. So, instead of trying to compute the integral polynomial of L t, you can just say that I want it mod 2 or mod 3 and mod 5. So, it is really this insight of Vale is really made for algorithms. great thing. So the current algorithms time complexity is, so there are two kinds of result, polynomial in PG and the degree of the curve and the other is polynomial in delta.

So, log genus, w exponential in the genus and delta. So, there are two family of algorithms I am not providing the reference because there are many results that lead to this. So, first one is used when the characteristic p is small because then it is a fast algorithm. The second one is used when characteristic is very large but genus is small. So when both genus, both g and p are big it is an open question. Yeah, so that finishes almost everything that is known about algebraic curves.