Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

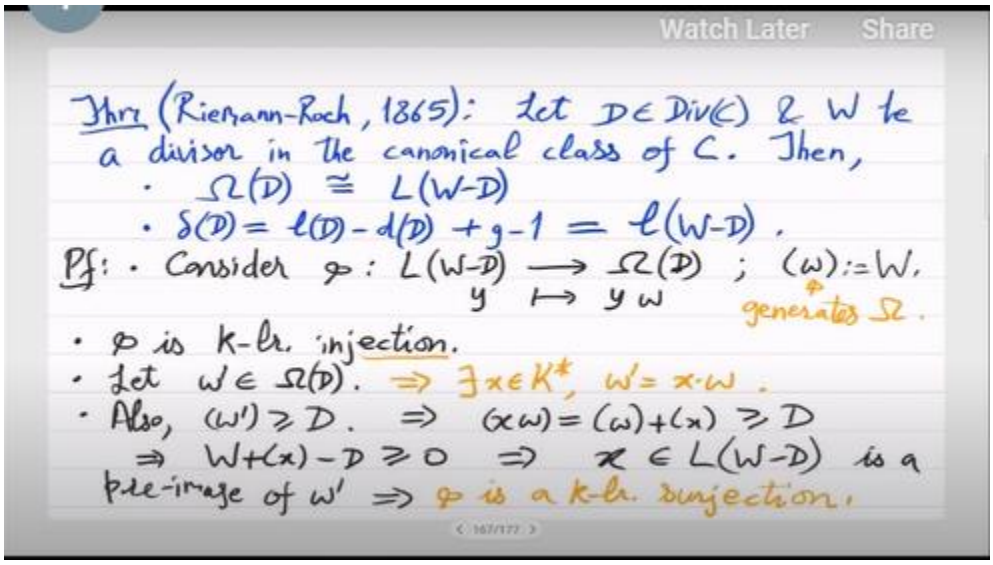
IIT Kanpur

Week - 11

Lecture – 21

Jacobian of a curve

We finished the Riemann-Roch theorem with one glitch: this y is the x Ω differential, and its canonical associated maximal divisor y = Ω plus the principal divisor of x . So for this, I have to go back. I have corrected that in the notes, which I will upload. So, when we define differentials here, specifically when we define this x in terms of Ω , right? So, what does x Ω do? Instead of applying Ω on R, you will now apply Ω on r times x, where r is the adel. So, previously, if Ω would kill r, then now x Ω will kill r x because 1 x is also a function. So, we can look at r in terms of x.



If you remember this equivalence, everything else will follow. So, Ω is given in Ω D, which means r + d >= 0. So, where does R x live? R x actually lives in D + X, which is the last property. X Ω lives in Ω D + X.

Therefore, the proof is as I just stated: if Ω annihilates AD + K, then X Ω actually annihilates 1 over X . AD + K. And so, this is that r + d >= 0; r/x+ d + x >= 0. They

are equivalent. So, you go from Ω d to Ω d + x. It is actually a plus; that was the mistake, and the rest is fine.

I have also completed the proof. So, why is this the case? When you send a function x to x Ω , why does d + e become -e ? Again, recall that Ω r = 0 if and only if x/Ω r} = 0 , and here the x that you are given is... So, X + D + E >= 0, and Ω highlights AD.

So, you take any R such that R + D, Adele R + D >= 0. So, for R x, you will get the principal divisor X + D >= 0. From which you use the property that x + d + e >= 0. So, you understand that r / x - e >= 0. So, r x actually lives in - e, Ω - e; that is where x Ω will now live.

I mean, r x lives in a - e, the adel, and so x Ω annihilates that. So, this is just to show that everything is consistent, and that's what is used in Riemann rock. So, ultimately, Riemann rock will, and here the correction is that Ω is in Ω , associated with the maximal associated divisor of Ω (bracket Ω). So, x Ω will be in this, and it's an if and only if. So this is Ω + x, not minus.

Yeah, that's if and only if. From this, you will get the identity that x Ω = Ω + x. The Riemann rock is now a one-line proof; you just look at the map that sends y from L w - d to Ω d by multiplying by Ω. And then, if everything works, you can show that this phi is an isomorphism. So, yeah, that finishes ribbon rock and corollaries in Jacobian varieties.

So, let us recall that the Jacobian variety will be given by essentially partitioning degree 0 divisor classes into subsets, which we call c_γ . But how does this come about? You essentially consider those degree 0 divisors D such that L(D) should have dimension equal to 1. Yesterday I said 2, but 1 is also fine. So, basically, the L sheaf should not be empty; that is all. As long as something is present, even a constant is fine.

You pick that D and put it in D γ. And you do this for all possible fixings of this thing: 2g - 1, ∞ - d, γ. So, you will basically partition your degree 0 divisors into these d γ chunks; they will be clustered, and the advantage of this d ' = 1 is that you can now write d ' as a sum of points. It is just a positive divisor. So, two things: it is a positive divisor, and its degree is g.

It is a sum of g points. The property of this d is that the corresponding d ' is the sum of points, and you just take that sum of points, then subtract g ∞ and call that c γ. Okay, so you have these C_γ as the clusters, and these clusters, the way we have defined them,

are actually a variety; it is potentially a high-dimensional variety. Again, the way we have defined them, you can look at the union, which will also be a variety. You can glue them, and that variety covers everything in the class.

The degree 0 class group, viewed as a variety, is called the Jacobian variety; however, as a set, it is the same. So, that is the Jacobian variety. It is a very special object and one of the most famous in mathematics because it is a variety that comes from a system of polynomial equations. The points can actually be added together, resulting in another point. Which, basically, means these things only happen in vector spaces.

But this is not a vector space; it's a variety. Here, it has this; it affords an addition. It actually has many other aspects that I will point out, but let us first revisit the elliptic curve case. So, when g = 1, genus 1 refers to the elliptic curve case. So, in that case, we will actually show that the Jacobian is the curve itself, and we will see how the addition occurs.

So, basically, the way we have defined C γs is that we are only looking at a point - ∞ that is an element of JC. If you want to add two points, what will happen is that p1 - ∞ has to be added to p2 - ∞. The claim is that this should be equal to a third element that again has to resemble P3 - ∞. So, what should that be? So, for this, I actually have to define what - P3 - ∞ is. So, what I should do next to make this clearer is show you what the negative of p3 - ∞ is.

For now, let me call that p3 ‘ - ∞. See, because before doing addition, you should at least know how to negate an element. So, what is the negative of p3 - ∞? So, let us call that p3 ‘ - ∞. So, then you will have to satisfy the equation $p_1 + p_2 + p_3' - 3\infty$ being equal to some function, the principal divisor of that function. And $p_3' - \infty = -p_3 - \infty$.

So, this sum should also be a function. So, you need to come up with two functions. So, as you already know how this is done, I have drawn a better elliptic curve now. So, here you see that the elliptic curve, along with the x-axis, y-axis, and the origin, is represented by the red curve. So, it should intersect the x-axis at three points because it is basically like $y^2 = x^3 + x$.

The equation $x^3 + x$ has three roots, which correspond to the three intersections with the x-axis. You take P1, then you take P2 and P3. What is the function of the line that passes through them? That is L. And what should p_3' be: p_3' and p_3 and - 2 ∞? So, ∞

should be a pole of multiplicity 2, and p, 3, and p, 3 ‘ should be the zeros. So, this is the line l' , and we generally draw it vertically parallel to the y-axis because the point at ∞ is like vertically upwards; y = ∞ is basically the point at ∞.

So, the vertical line will give you the opposite of P3 - ∞. So, that is P3 ‘ - ∞, and it has to be in line with P1 and P2. So, this is the algorithm for performing addition and finding the inverse on an elliptic curve. So, you can understand this from the way we have defined the Jacobian variety, which, in this case, happens to be the elliptic curve, and it does not grow. What you learn is that when the genus is 1, the Jacobian of the curve is the same as the class group of degree 0, which is the same as the points - ∞.

So these points, - ∞, are the distinct elements in J(C) and in C(L_0). Why are they distinct? You just need to show that for different points P and Q on the elliptic curve, P - ∞ and Q - ∞ are not the same modulo the principal divisors, which again follows from the picture. But why does it follow? So, if you take, let us say, P1 and P, what you have to do is look at the above; actually, it will be the same as the above equation. Let's say P3' and P3 are written separately. Basically, if they are, then what will happen is you have to.

.. You basically have to have this: if these two are the same, then essentially p - q has to be equal to a principal divisor of a function. Functions on the elliptic curve are just lines; they are linear functions. So you have to come up with a linear function g which has p as a pole of order 0 and q as a pole. That is impossible because every line on the elliptic curve gives you a minimum of three solutions, and with the point at ∞, you get a minimum of four solutions. So, for different points, you cannot have equivalence.

So, all these different points give you p - ∞ different elements in the degree 0 class group. So, you have completely classified the degree 0 class group. You can also classify the canonical divisor w because the degree of the canonical divisor is 2g - 2 , which is 0. So, the only element is, I mean, it is in Cl0, and in Cl0, the only thing that works is ∞ - ∞, so that is 0. So, the canonical divisor in the case of an elliptic curve is actually just 0, which means that the Riemann rock has this form.

So, Ω d = L(- d), which you can calculate again. So, for d = 0, these are just constants; for positive d , it is empty, and for all other cases, it will be something non-trivial. So, Ω d for all divisors is quite explicit because it is simply the L of the negative. So, this tells you almost everything you want to know about elliptic curves in a field-independent way; you do not need information about the field in these proofs. What were you thinking about the diagram? Whether it follows from the diagram or not.

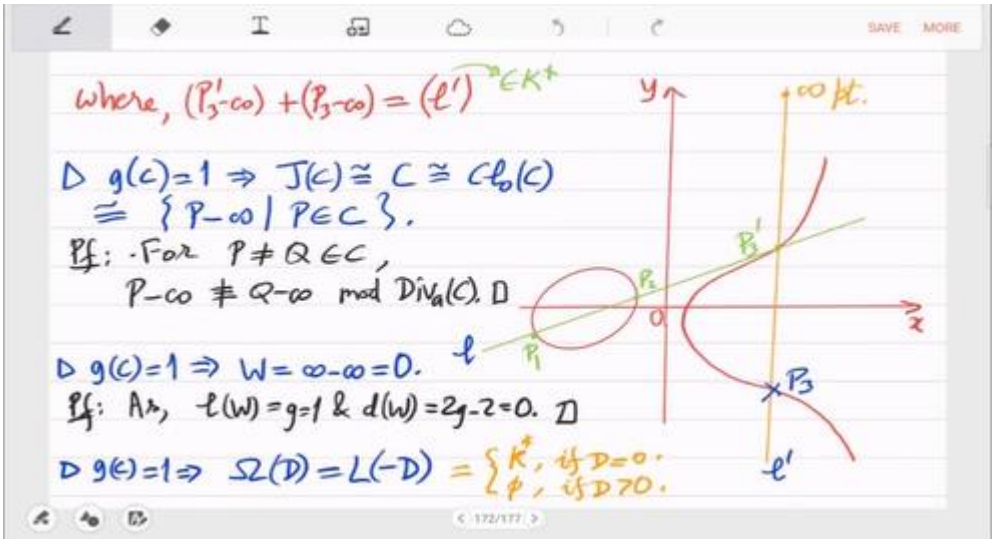
In the diagram, when you draw a line, you always have to have three points that you see,

and one point possibly at ∞. No, there will be three points that will be zeros of that line. Yes. There will be three poles at ∞.

Correct. Yes, the ∞ part will simply balance. Yes. Having only two things in the union of zeros and poles is not possible. I mean, it can be done.

I don't think you can do it. Just by looking, you first have to realize that g is a linear function, and then substitute the linear function. For example, if y = mx + c , you substitute it into the elliptic curve equation, which will become a univariate equation. Now, the univariate equation over an algebraically closed field has three solutions, and from there you can see that all those solutions must be p . But then, if all of them are p, then they have high multiplicity, and you are saying that the multiplicity of p is 1, so you always get a contradiction. Yeah, I hope this Jacobian variety part is clear.

Especially when looking at the elliptic curve, you can imagine how it will behave for higher genus. The problem with higher genus is that you will not be drawing lines; you will be drawing non-linear objects because, for example, g can be quadratic. So, you are actually drawing a quadratic curve through the points. So, it is not easy to analyze it either pictorially or algebraically; however, this picture can be used as a guide. So, the Jacobian varieties are, as I said, the most important objects in mathematics.



So, it is essentially a junction of many areas of math. So, what are those areas? So it is now obviously a smooth projective variety of high dimension, making it a geometric object with geometry. It is not a curve; it is actually a high-dimensional variety. By the way, it will not be an affine variety because I mentioned gluing. So whenever you want to

glue, you should think of these affine patches.

So you glue, and then you actually obtain a projective variety. So, this is another reason why we will prefer projective over affine: in these more general situations, you actually want to glue things. So, when you glue affine varieties, you will not get an affine variety; you will get something else. This is where projective varieties are more fundamental, as they possess geometry from which they derive.

Furthermore, they also have a group structure. This group structure is not arbitrary; it is actually an abelian group, and it also has an automorphism that comes from the Galois group of finite fields. So, the Galois group of the finite field that you saw in assignment 1 actually acts on it. So, the first thing gives you the abelian group structure, so you can try to use theorems related to abelian group structures, such as the product of cycles, etc. And the second thing is that, because the Galois group is acting, you can develop more complicated theories. For example, Galois cohomology theory is one way to study this, but we will not cover that in this course.

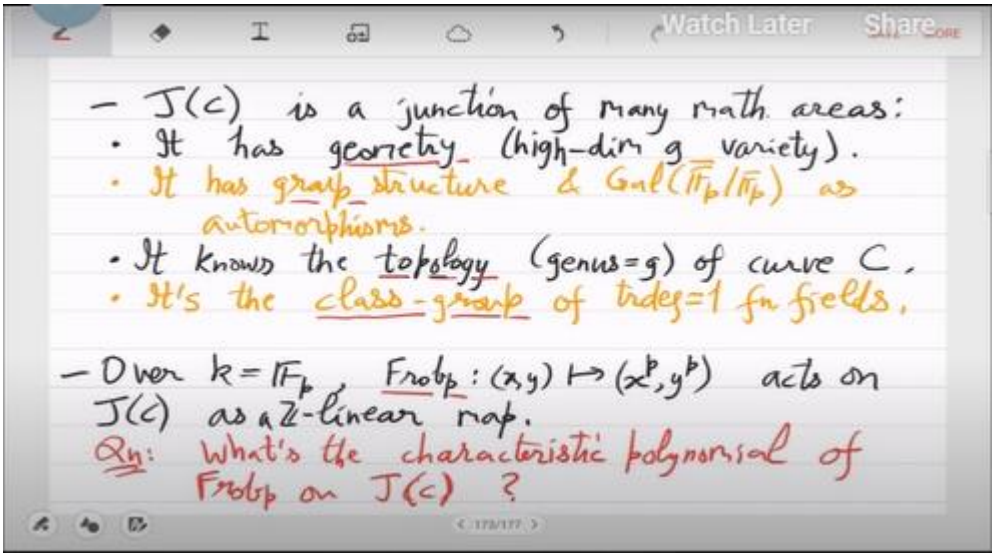
So, each of these bullet points actually leads to many areas of math, and it knows the topology of the curve. So, this was one of the main motivations for defining it because we wanted to compute the topological invariant of a curve. So, it clearly has topological motivation, and it is also the class group of function fields with a transcendence degree of 1. So, this was the other thing we showed: it is also equal to CL0 of a curve, which is basically the function field translation degree 1. So, it is a class group; it is topological, which is essentially the Zariski topology, but classical topology is also embedded in it.

When you have a complex field, the classical topological concepts can also be recovered. Like this, although the proofs will be very different, we are not covering those proofs in this course. There is a whole group theory, representation theory, cohomology theory here, and of course, algebraic geometry is also present. So, needless to say, all great mathematicians have dabbled in this because it covers so many areas of math. So, what we will do next is study one primary aspect of JC or CL0C, which is the Frobenius action on it and counting points.

So, take the field to be a finite field; in fact, take the base field of constants to be the ‘ field. So, in that case, you have a special map, which is the Frobenius map. So, what does the Frobenius map do? It points to this definition, which will be the definition of Frobenius in this course. So, there is a special map called Frobenius, which, by the way, is also the source of the Galois group action of F_p ; you are basically applying this map. So, it is an automorphism of the class group because a key aspect is that a point maps to another point.

So, this is acting on JC or the class CL0 as a linear map, right? Because clearly, if you have a point P1 and a point P2, then the Frobenius at P1 + P2 will be the same as the Frobenius at P1 + the Frobenius at P2. That again comes from the way we defined addition in the divisor group. So, it is almost, by definition, a linear map. By "linear," we mean Z-linear; actually, this is over integers.

Right now, it's a Z-linear map. You can ask about its characteristic polynomial, so you have a map and a vector space. The first thing you should ask is: What is the characteristic polynomial of this action? Of Frobenius on J_c . So this will be the guiding principle of the next chapter we will start, which is the study of the zeta function of the curve. So the zeta function will ultimately turn out to be the characteristic polynomial of this action. So the rest of the course will be devoted to that study and proving the Riemann hypothesis related to it.



The zeta function of this curve is the same as that of a transcendence degree 1 function field, but in computation, we are more interested in counting points on the curve. So, it will turn out to be equivalent as well. Yeah, the curve is just the geometric object; the actual object is the function field. Whenever we write C, especially div C, it's very hard to make sense of it geometrically because the points P1 and P2 are not actually points; as I mentioned, it's a cloud of points. When you take your field of constants to be just f_p , your p_1 and p_2 are actually ‘ ideals.

So, c is just the formal sum of ‘ ideals; you are not actually adding the ideals, it is just a formal sum. However, when you go to k , they actually become points. So, when it is

inherently an algebraic definition, you can think of it independently of the field. So, yes, I do not think I have defined this before.

So, what is the zeta function of a curve? Let us do it today. So, we will now assume the field of constants to be F_q for some ‘ power q , where p is a ‘. So, it is a finite field, and c is a smooth projective variety that has coefficients from that base field. So, this is what we mean by over small k: the coefficients come from this base field. Also, this C is isomorphic to the abstract curve; I mean, it is just modeling of its function field. So, in other words, if you were given a curve in the input that is not smooth and has a singularity.

So, you will go to its function field, and then from the function field big K, you will arrive at a curve that is smooth and projective, and this study will focus solely on that. It will not study the singular points; it will only study the function field of your given curve model, which is smooth and projective. So, it is inherently a study of the function field, not the curve itself. So, of course, our computational interest is in point counting on the curve. That is for n: how well can we estimate the number of points, which I can also write like this? which is the number of FQN points on the curve.

So, FQN points mean that if you have a planar curve given by F(x, y) = 0, then x and y are only allowed from this field. So, for example, when n equals 1, what is n 1? n 1 refers to the x, y pairs that are on the curve where both x and y are constant in the base field. This is not a simple thing because when you are given, even if you are given $y^2 = x^3$, I think this is an example we saw at the beginning of the course. Even in the case of $y^2 = x^3$, you have to consider that you do not really know; maybe it is too simple, but $y^2 = x^3 + x$. So, definitely for $y^2 = x^3 + x$, you do not really know for what value of x .

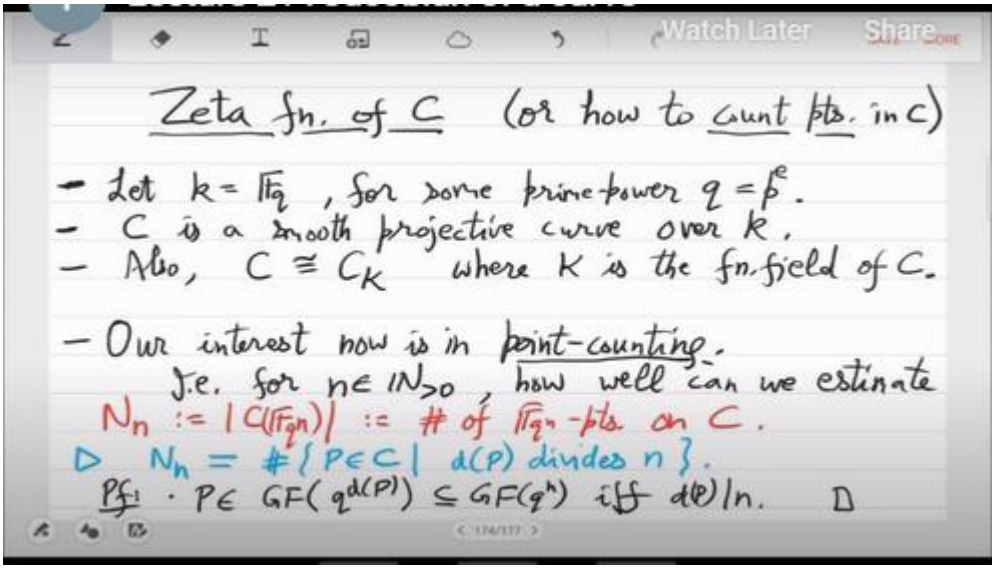
You will get a y because when you fix x, you have xq + x, but when is it a square in the base field Fq? So, sometimes you have a square, and sometimes you do not, so you have to divide the computation into two parts. Both outcomes are unpredictable; it is almost a random event. So, this N1 even N1 is actually a very difficult thing. There is a lot of randomness in it, even in the case of elliptic curves. So, it is a well-defined question: Can you estimate, or can you actually compute N1? That is what we are interested in.

This question appears frequently in computer science and its applications. So nn is the same as the number of points on the curve such that the degree of the point divides n. Is this believable, or should I prove it? For example, when you take n to be 1, you are essentially saying that you want the degree of P to be 1, which means that they will all lie in FQ. When you take n = 2, n^2 is essentially N^2 , which means that the degree of the point should be either 1 or 2. This indicates that it is either in the base field F_q or

in Fq^2 . Right, because the degree is defined by the least field, the smallest field in which your point exists.

So, you are actually asking for all the points in that field, its subfields, and so on. So, p essentially lives in this finite field. Yeah, this will be hard to write; let me use Galois field notation. So, the Galois field q^{dp} is okay. So, this will be contained in the Galois field q^n if and only if dp divides n ; that's all.

So, by definition, a point on the curve exists in the finite field of size q to the dp, and if your point also happens to exist in q to the n, then it essentially means that the degree is a factor of n. This is due to the property of how finite fields are structured as a lattice, which gives rise to this relationship. So, you have this condition. Yes, we will study its generating function, let us say. So, what is n1, n2, and so on? It is a series of numbers; its generating function is.



Σ n n t to the n is seen as a power series. So, are you aware of this notation: z ((t^2)? So, basically, this is the set of functions that are not polynomials in t . You are allowed to go up to t to ∞; you can have infinite sums in this, which is the difference from polynomials, unlike z_t , because I want to include all of these big N and small n 's. So, there are infinitely many. So, I need the ability to take infinite sums. So, this is the power series; essentially, it is viewed as the larger you get to t^n , the smaller the quantity becomes.

This is how the convergence can be seen, but we do not need to talk about convergence; you can just define it algebraically and symbolically. It is a set of all these expressions

\sum a_i t^i where i goes from 0 to ∞. So, it is just that these formal sums are infinite sums. So, usually this is what you would want to study: you would want to study the generating function of this count, but this is not the zeta function. So, if you already know the zeta function, do you know what the difference is between this and the zeta function? Yes, that is a property in the end.

However, can you state it simply at this point? We will not use this because it is defined by this black box neural network, and we have no idea what the neural network is. Instead of using this, we will use something more compatible with our divisor definition. Yes, with this as the goal, we define another power series.

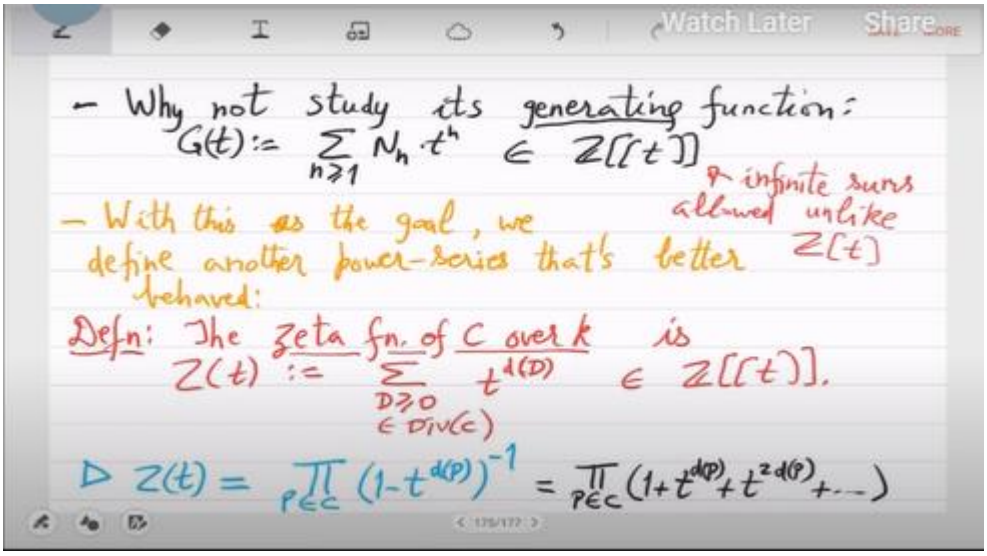
That is better behaved. So, that is the Zeta function. The zeta function Z of a curve over k is defined as the sum over all the divisors t raised to the degree of the divisor. So, this clearly lives in power series over integers, and this is what we will use. Right now, it is not clear what the relationship is between the thing we are interested in computationally—that is, the count of points—and this more abstract concept, because it took us so much development to get to divisors. This involves summing over all the positive or non-negative divisors.

Summing over all the non-negative divisors. So, this is what I mean: you can expect a relationship because a divisor is nothing but a formal sum of points, denoted as σ(p_i). For example, this can possibly be factored into points; every divisor is a sum of points, and the degree is additive. So, every monomial here, t raised to a degree, can actually be written as a product of t raised to the degrees of points, and then the entire zeta function can be factored.

So, let's do that. Yes. So now you can go back to your function. Yes. What is the function? The last Zeta function. Yes. So the divisors that will have the degree as a — no, but that was for a point. I have said nothing about the degree of a divisor.

If the divisor is P1, then it is compatible with that lemma. But if your divisor is P1 + P2, what does P1 + P2 have to do with P1 or P2? P1 + P2 is not a point on the curve; I mean, this is another thing: the Jacobian is much bigger than the curve, right? So, P1 and P2 are actually not curve points; they are somewhere else—they are points on the Jacobian. So, you cannot interpret the degree of P1 + P2 so easily. But the one good thing about this sum is that it factors into points like this. Do you agree with this formula? So, if you could just go over all the points. So, this is an infinite product, right? So, I have now replaced the infinite sum with an infinite product, but now the product is over points, not divisors.

So, the proof is simply this: you just observe that this is equal to one + the degree of the point multiplied by t, plus twice the degree of the point multiplied by t, and so on, until ∞. So, it is an infinite product of infinite sums, but you can see that any non-negative divisor d appears here uniquely, right? So, the two things are the same.



Degree of what? Yes. Yes. Let us write it down. $t^{p1} \cdot t^{p2} = t^{p1+p2}$; that is all. Moreover, t^{i_1} degree of p_1 and t^{i_2} degree(p_2) = degree (I_1 P_1 + I_2 P_2) , which is the divisor form. So, when you look at the product of two things within that larger product, the monomials actually multiply, and in the exponent, you obtain the degree of a divisor, which serves as proof that the zeta function now factors over the points. So that's a very nice thing; it's much better looking than your original generating function.

I mean, your hope is that it at least knows about all the points. So, in a way, ultimately we will also be able to count them. Every point is contributing to a factor. No, I was confused by the degree of divisor notation.

We studied the divisor degree and some of the coefficients. No, no, no. What we agreed upon is the degree of a divisor, such as I1p. It is equal to I1 times the coefficient times the degree of the point. It is not I1 + I2; it is I1 times the degree of the point, which is what is being used. Because a point is not merely a point, it can be considered a cloud of points.

You have to count all of them. If the point is our actual point, then you get degree 1; consequently, you get I1 + I2. Otherwise, you have to weigh it against the cloud size. So, it was defined carefully so that this thing works. Do you have any questions? So, we have done this not just because it factors, but also because we now have a pretty good understanding, even up to Riemann-Roch, of the divisor group, and we will actually use all of that built-up machinery inside the zeta function.

For example, our ultimate goal is to provide an expression for the zeta function. Which is computable right now? It is an infinite sum that we cannot compute, and we also do not know the points. So, all of this does not seem to help much. However, by using all the machinery, especially Riemann-Rock, what we will do is break this sum up into, first of all, degree 0 divisors, then degree 1 divisors, degree 2 divisors, and within a degree d divisor. We will compute the sum locally and then add everything together.

So, what I mean is that with the kind of methods we have developed, this will be pretty easy now. Although it took people a lot of time to achieve this, we now have the right tools. So, nice things will follow pretty quickly. So, the first observation is that we recall that the degree does not change up to principal divisors. So, in any divisor, you can add a bracket around x; the degree will not change because the degree of bracket x is 0, and the degree is additive.

We recall that this exact sequence shows that the degree 0 class group is contained in the class group. The degree is mapping that to integers. So, anything you take from the degree 0 class group will be in the kernel of the degree map; that is all this is actually saying. What we don't know is what the image of degree is. Is it all integers or just a few integers? We actually know that there are infinitely many integers.

Do we know about that in the class group? Yes, certainly. I mean, you can simply take different degree divisors. So, you know that, formally, you should be able to show it. However, just because this class group is a free sum, it is expected that there will be infinitely many integers, although you do not know whether all integers are included. For example, it is not clear whether there is a divisor whose degree is 1.

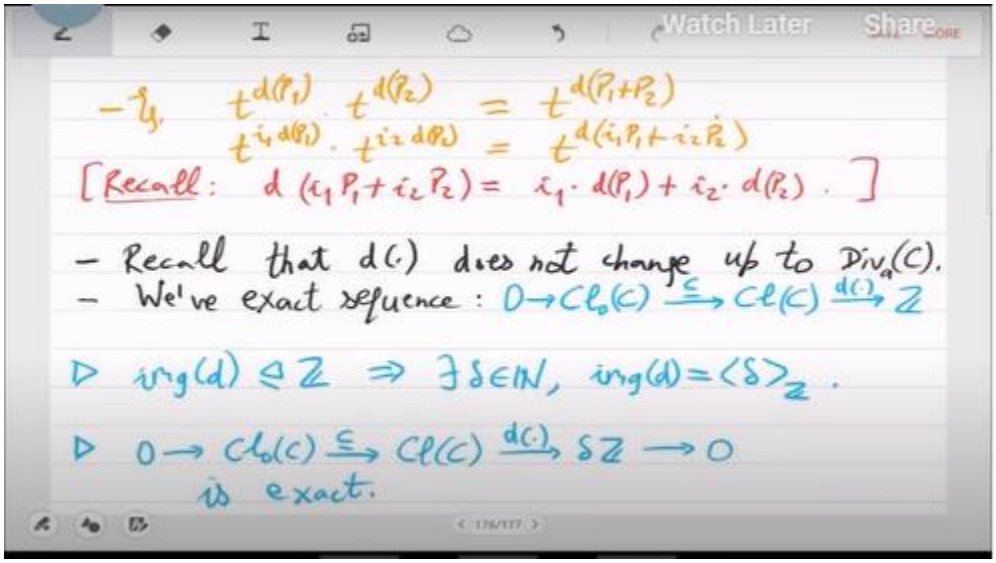
Degree 0 is known to us because any principal divisor will have a degree of 0 for any function. But is there a divisor whose degree is one? That is not clear because what may happen is that your curve might not have any points at all in the base field. You cannot simply say that I will take point P, because there may not be any point at all. So, you have to go to an extension. But when you go to an extension, say FQ^2, all points there have degree 2.

So it seems that you are jumping from 0 to 2. Exactly. Why will the GCD help? But degrees are additive, right? Oh, I see. What you have shown is that the image of D is an ideal, specifically a principal ideal. Therefore, you are only considering multiples of delta.

This results in a step function, and that step function encompasses the entire image. Let's

write that down. The image of D is actually an ideal of Z, which means that it is a principal ideal. Yes, but you do not know whether delta is 1; delta may be 2. So you only get even degrees, which is possible because our base field is arbitrary. So, we have to stick with this delta for some time. In the end, we will show that delta = 1, but right now, I do not think it is easy to demonstrate that delta is 1.

So, with this definition, it follows that this exact sequence is exact. The only difference from above is that we have now fixed the image delta z. So, if you look at the arrow of degree, the image is in the kernel of the last map, making that part also exact. So, there are exactly three parts, where the image of the previous map is equal to the kernel of the next map. So, this is an exact sequence; we will remember that this is where delta comes from.



And now, for this last part of the course, we will be expanding the function z(t) . We will rewrite z(t) and continue calculating new properties of the zeta function until we have proved the Riemann hypothesis. So, in fact, I have not told you what the Riemann Hypothesis is, but that will be explained as we go through these expansions. So, define CLDC to be the set of divisor classes of degree D, and D is always chosen to be a multiple of delta; otherwise, the CLDC will be empty.

So, we expand with respect to the CLD. We can write, for example, set T as follows: these are all non-negative divisors. Let us go over the Ds that matter, and then let us review the divisor classes in CLD. And then finally, the divisors in that divisor class. So, what is the property of this normal D? It is greater than or equal to 0, its degree is D, and they are all equivalent modulo principal divisors.

So, we have these three sums, and in the end, the degree of D is D. Therefore, you obtain this. CLD has all those divisors of the degree of D. So, yes, we should be careful. So, like CL0, it was not the set of divisors; it was the set of equivalence classes modulo principal divisors.

So, yeah, the zeta function goes over all the non-negative divisors. So it doesn't care if two divisors are equivalent. So it's kind of an overcount. You cannot avoid that because, ultimately, your goal is to count points and not some equivalence. If two points look different, they are different. You don't care whether they are equivalent up to principal divisors. Goals are different, so this will be a longer expansion; we will do it in three parts: fix the degree, fix the class, and go inside the class.

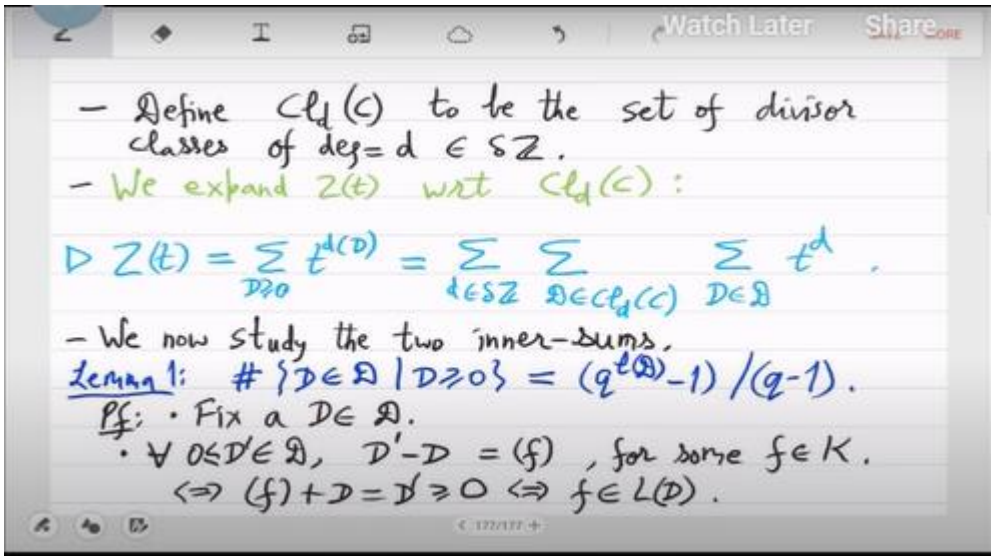
Now, we will study the two inner sums. You will see some interesting lemmas, but, as I said, nothing will be difficult now because of the significant development we have accomplished. So first, the lemma will tell you the count of the innermost sum. The number of divisors >= 0 = Q^{LD-1}/ Q - 1. So, now the LD sheaf appears magically; this was probably the result of reverse engineering that provided them with the LD sheaf.

So, the calculation of the zeta function will actually inform us about the LD sheaf. So, why is it appearing? So, you should remember that the LD sheaf does not change up to principal divisor addition; at least, the dimension will not change. So, little l of d is a property of that class. It is not a property of the divisor. So, that is why I have written "small l" for the class, because every element in that class has the same small l dimension, as we had seen before.

So, how do you prove the count? Fix a divisor in this class. Now, for all d' ‘ in the class, what do you know about d' - d ? It is equal to some principal divisor. Any d ‘ you take with the fixed d, the difference is a principal divisor of a function, which means that I should only take values greater than or equal to 0 because that is what appears in my count. So, for all non-negative devices d' in the same class, you have this property: d + f or, conversely, f + d (which is d') >= 0. What does this mean? No, that means, "Yeah, no.

So, this immediately means that f is in the LD sheaf, which is the definition of the LD sheaf. Therefore, for a fixed D , as you change D' in the property of being greater than or equal to 0, these non-negative divisors all come from functions in the LD sheaf, and we have established an association. But that would mean that there would be infinitely many D ‘ because functions are infinite. Is that correct? No, that's not correct because now you have to count functions in LDE that give you different D ‘. Many

functions, for example, if you take a function f and a function 2f, will yield different results.



Their principal divisors are the same. So, you have to count functions whose principal divisors are different, as this will give you different d '. So, for f and f' in LDE, the principal divisors are the same if and only if what happens is that it has to be a constant. Therefore, you should not consider these constant multiples of functions. So, what we have shown is that the number of distinct D ' >= 0 in this class is the same as the number of non-similar functions in the LD sheaf.

They have different divisors, which means they are not multiples. So, what is the count? So, let us look at the LD sheaf; it has an F12 field basis, and it is a small k-vector space. So, it has these basic elements. So, how many non-similar functions can you find here? Why shouldn't I have said "infinitely many functions"? Actually, sister, it's a finite-dimensional vector space, and the field "small key" is also finite. So, this is actually a finite-dimensional vector space, but I need the exact count.

The exact count comes out to be this: you just take all possible combinations, which is Q to the LD. But then you do not want to take the 0 combination, and you do not want to discount the multiples. So, that is divided by q - 1.

Fine, that is the expression. Why was this a - 1? Oh, the zero function. Yeah, and then you divide by Q - 1. So, you have some combinations, but you discount their multiples.

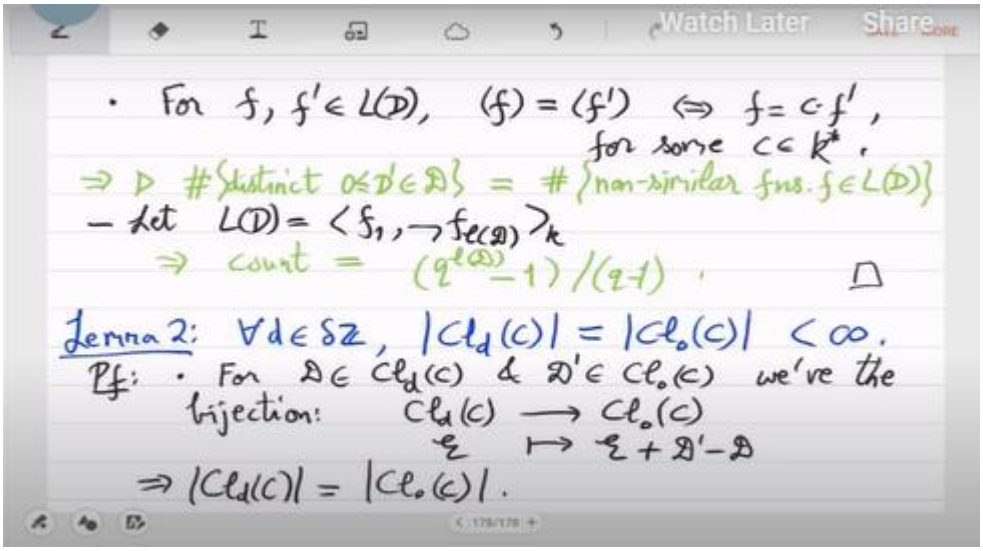
So, there are Q - 1 multiples. So, this gives you good information about the inner sum, right? Now, you can actually just simplify the inner sum; it is this number that is the L D sheaf dimension.

Times t raised to d. Now, let us move on to the second sum. So, what is the size of the CLD? That is the question. So, what we will show is the relationship between the correct degrees CLD and CL0. You would expect them to be equal, so they are equal, and therefore it is finite. Actually, do we know CL0 to be finite? We don't know it to be finite, right? Yeah, that will need a proof.

Okay, so this stuff will come from genus, from Riemann, or just from Riemann, actually. Yeah, you don't need rock for this. So, let us prove the equality. So, for a class in CLD and a class in CL0, we have the bijection. We will just provide a bijection from CLDC to CL0C, which will indicate where you should send D2 (sorry, D' ') and where you should send some arbitrary E2.

So, just do the obvious thing: send it to the right person. So, the degree of this fancy E is D. I mean, it is a class, but you can also think of it as just a representative divisor. So, I can talk about degrees and everything. So, the degree of that divisor is D; on the RHS, it is D + 0 - D, which equals 0.

You can clearly see that this is a bijection, as you can go both ways. Yes, it is trivial. So, that is the bijection that makes them actually equal in size. That was the easiest part. So, next is: why is it finite? Let us prove that.



So, because of the previous result, we actually do not need to study CL0; we can take a higher degree and study that instead. So, let us do it. So, consider D in delta z such that D is quite large and >= g. So, for larger degrees, we have nicer properties. So we are hoping that CLD will be understandable to us. So let D be a divisor in a class that is in CLD. According to Riemann's theorem, you can already conclude that the L of this, L - D difference is at least lower bounded by 1 - G, which, for high degree, is 1.

That is a good thing. So, there is a function in the LD sheaf. So, this means that there exists a non-negative divisor in D. Right, because there is a function you pick, add it to d , and then you get d + f >= 0.

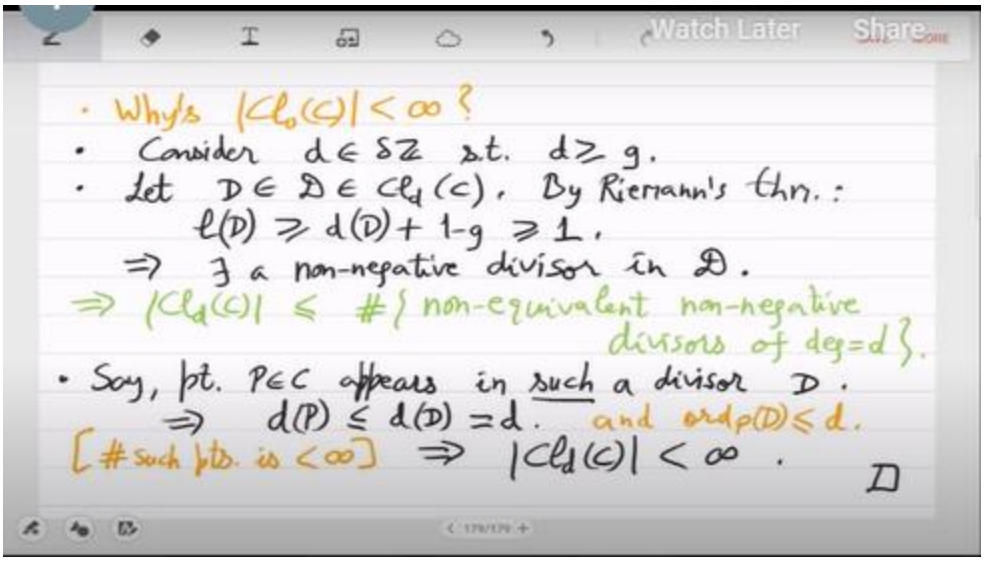
So, d + f >= 0, and d + f is in the same class. Therefore, you have found a non-negative divisor, which means that... CLDC is less than or equal to the number of non-equivalent non-negative divisors. of degree D. Because as you change this fancy D in CLD, you will find a non-negative divisor present each time, and they are all of degree D. So, you just have to count how many degree D non-negative non-equivalent divisors there are.

" So, suppose point P appears in such a non-negative divisor in CLD; let P be a point there. The degree of the point will be less than or equal to the degree of the divisor in which it is contained, which is d. So, just think about what we are doing: you have these non-negative divisors, and they are all non-equivalent. So, you are looking at the support. So, you see these points; whatever point you see, P, its degree is bounded by D. Therefore, you have to ask the question: how many points of degree D are there that are finite? Since the number of such points is finite, what you have learned is that the cumulative distribution function (CDF) is finite.

Is that enough? It is finite, but there is also this coefficient that appears; the point may appear many times. Yeah, that is also being used correctly; that is true.

Let us write that. The number of points is finite, and their multiplicities or orders are also finite. Overall, you get finite combinations. Yes, that’s good. There was no negative order. So, this is a finite set. I think that is good for today.

So, you can just let us know next time we will. So, we have computed the innermost sum, and the middle sum now depends on C L 0 as well. So, C L 0 is the size of the class group. So you will now get an expression in terms of. Two fundamental things are present in the zeta function: it is simply the sum of multiples of delta, where the sum depends on the L D sheaf and the size of the class group. So, it will be a simple expression, and then we will study its famous properties.



- Why is $|Cl_0(C)| < \infty$?
- Consider $d \in \delta\mathbb{Z}$ s.t. $d \geq g$.
- Let $D \in \mathcal{D} \in Cl_d(C)$. By Riemann's thm.:
  $\ell(D) \geq d(D) + 1 - g \geq 1$.
  $\Rightarrow$ $\exists$ a non-negative divisor in $\mathcal{D}$.

$\Rightarrow |Cl_d(C)| \leq \#\{$ non-equivalent non-negative divisors of $\deg = d\}$.

- Say, pt. $P \in C$ appears in such a divisor D.
  $\Rightarrow$ $d(P) \leq d(D) = d$. and $\operatorname{ord}_P(D) \leq d$.

[# such pts. is $< \infty$] $\Rightarrow$ $|Cl_d(C)| < \infty$. $\square$