

# Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

IIT Kanpur

Week - 12

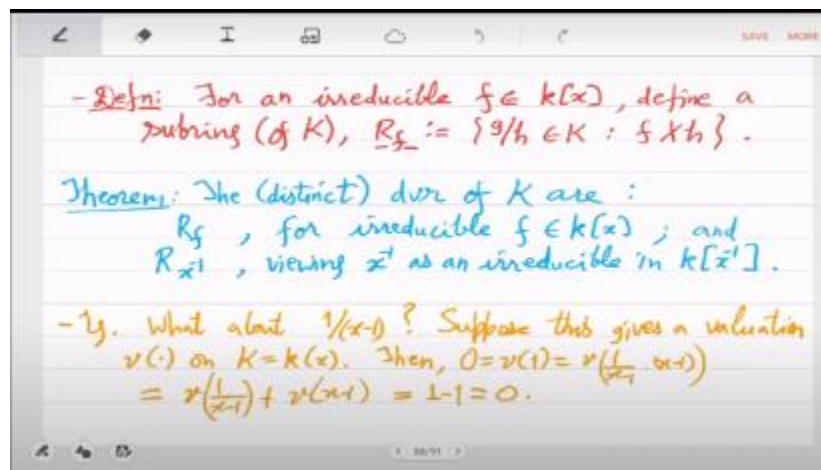
Lecture - 23

## Functional Equation and Point Counting

Yeah, you asked a good question, so I have changed the notes; I still need to upload them. So basically, this is an example, right? This is  $1/x - 1$ . So what you can show is that  $1/x$  and  $1/(x - 1)$  are the same up to a unit multiple. For example, if you look at the valuation with respect to  $1/x - 1$ , then this identity states that  $1/x - 1$  is equal to a unit. Thus, this expression is a unit model of this times  $x$ . Similarly, you can also show that if you look at the valuation  $1/x$ , there is again a reverse identity.

Therefore, in both valuations... Basically, what it means is that the maximal unique ideal can be generated by both.

So, yes,  $x - 1$  and  $x$  provide identical valuations and yield the same DVR. So for that, I actually had to change the proof slightly as well. So, Case 2 was not properly studied before. You divide it into two cases: 1 case is that  $x \in R$ . Let  $R$  be a valuation ring, and we are looking at the function field with the transcendental element  $x$ .



We are basically looking at the projective line. So, you then divide it into two cases: whether your DVR contains the variable  $x$  or not. So, the containment of  $x$  gives you an irreducible  $f$ , while the non-containment of  $x$  gives you  $1/x$ . Yes.

Yes. So,  $f$  is an irreducible polynomial in 1 variable,  $x$ . Correct. But this proof is also written in general. So, we don't make assumptions.

Yes. In case 2, since  $x \notin R$ ,  $R$  is a DVR. So, its inverse is in  $R$ , which means that  $k(1/x)$  is also a subring of  $R$ . And now, from the above case, the unique maximal ideal is generated by some polynomial in  $1/x$ . The only observation that was missing before is that  $x^{-1}$  is not a unit in  $R$ . If it were a unit, then  $x$  would be in  $R$ , but in case 2, we have assumed that  $x \notin R$ .

This means that  $x^{-1}$  is not a unit, which implies that it is in the maximal ideal. This means that  $f^{-1}(x)$  divides  $x^{-1}$ . So, they are the same; they can differ only by a constant multiple. So, that is it. So, this part that was previously muddy is now fine.

Yeah, so when you look at  $x - 1$ , you actually get this property. Somewhere, I have added, "Yeah, this property you get in blue." So,  $1/x - \alpha$  for any constant  $\alpha$  gives you the same valuations; they are all generators of the principal ideal. That is the example. We had not observed this before; it is not a contradiction; it is fine.

Okay. I guess we can start. Any questions about this part? Yes. So, we have shown that the  $Z$  function is a rational polynomial in  $T$ , and we can think of this as the analytic continuation of the power series. We can now use, let us say,  $g(t) / h(t)$  or  $a(t) / b(t)$  as the function defined over all complex values of  $T$ . This function satisfies the functional symmetry equation, where  $T$  is replaced by  $1/QT$ , resulting in this relationship.

So, we did this, and hence we also obtain, in classical form, this  $Z(1-s)$  related to  $Z(s)$  via the norm of the canonical divisor class. We have information about poles; there was 1 typo here: the residue is not  $Zt$  but  $Q-1$  times  $Zt$ , because we had already multiplied our  $Z / Q-1$ . The residue of  $Z_t$  is actually the class number divided by  $\delta \cdot Q - 1$ . Okay, that came from what happened in the formula. The residue at  $t = 1$  means that you have a univariate polynomial which you multiplied by  $t - 1$  and then set  $t = 1$ .

So, the answer you get is called the residue. In other words, if you have a polynomial,

you can first divide it by  $t - 1$  to get the remainder, meaning you get the quotient and then substitute  $t = 1$  into the quotient. However, here it is very explicit, so you do not have to think about integrals. The motivation comes from there, so now the final thing is to.

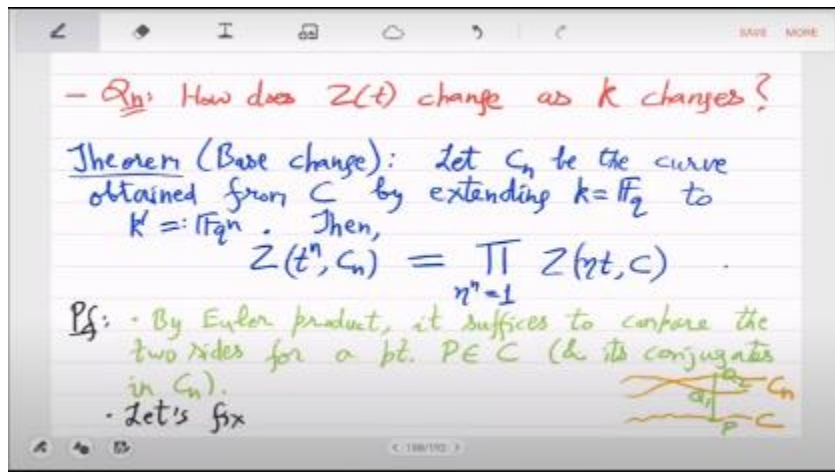
I deduce that  $\delta = 1$ . So, for that, we need this Bayes' change theorem. So, let us prove this. Yes, we want to relate the  $Z(C_n)$ , which is the same curve in a higher field, with  $C$ , which is the curve defined over the finite field  $F_q$ . So, by the Euler product, it suffices to compare the two sides for a point  $P$  on the curve and its conjugates on the curve.

Thus, the picture is that you have the curve  $C$ , and then you have the curve  $C_n$ . So, points on the curve, when you move to the same curve but in a higher field, may actually ramify or split and give you more points because you have a bigger field. Well, the problem is that the point  $P$  is actually not a real point; it is a prime ideal. Essentially, the prime ideal factors; thus, the prime ideal may factor, and the cloud of points factorizes into smaller clouds, which are again prime ideals in this  $C_n$ . So,  $P$  here may give you  $Q_1$  and  $Q_2$ ; this is what is happening.

So, we will see that the part of  $P$  on both the left-hand side and the right-hand side behaves as claimed, and then by the Euler product, you can take the product over all the points, and you will obtain the theorem. So, let us consider this point  $P$  now. The Euler product is that the  $Z$  function factorizes according to primes. There is no experience. Yeah, but there is no experience; we have not defined it.

Obviously not;  $z(t)$  is simply  $\sigma(t)$  raised to the power of the divisor. Sure! So, the definition we started with is essentially the same as the ordinary Riemann definition. This is the sigma of  $1/n^s$  in the case of numbers. So we are simply using the same analog definition of it for curves. What you are saying will be reduced after this theorem.

But anyway, the main technical content is actually the same, which we will now examine at a specific point. So, what is happening there? So, for this point, let us fix point  $P$  for the proof; we will not change it. So, let  $M_P$  be the unique maximal ideal of the DVR corresponding to  $P$ . Since  $P$  is a smooth point, the germs essentially give you this local ring with the unique maximal ideal  $M_P$ . So, this is a DVR, and the DVR data indicates that this field,  $R_P \text{ mod } M_P$ , is a finite extension of  $K$ , right? So  $K_P$  is the field where, I believe,  $P$  completely splits, and it is still a finite extension of  $K$ .



It sits between  $F_q$  and  $F_{q^n}$ ; if  $K$  is true, then  $K$  is  $F_{q^n}$ . So,  $KP$  basically has this model:  $KT \bmod F$ . Is it an irreducible polynomial over  $F_q$ ? So, this is just a description of where the point completely splits. Yes, so what did we have? We had this field  $K'$ . Over this field  $K'$ , which is slightly larger than  $F_q$  and has size  $Q^n$ , what will happen is that  $F$  may split further.

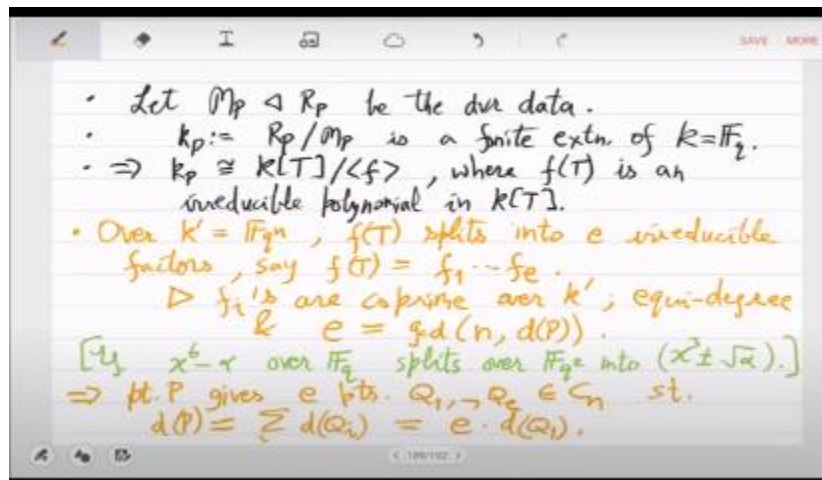
No, not that. Yeah, okay, fine. So,  $F$  is irreducible in  $KT$ , which is  $FQT$ , but when you go to  $FQ$  in the end,  $F$  may split; let us say it splits into  $E$  polynomials or  $E$  factors. So, what can you say about the factorization such that  $FT$  splits into  $E$  factors? Over the new field, they are now irreducible over the prime field  $K$ .

So,  $F$  splits into  $F_1, F_2, \dots, F_e$ . So, what can you tell me about them? So, it is not difficult to prove; just use the properties of finite fields. You can reduce  $F_1$  to  $F_e$ , as they are mutually coprime. Their degree is the same, and regarding  $E$ , you can say that whatever the degree of  $F$  is, you take the GCD of that with  $N$ , and that will be  $E$ . Since the  $F_i$  are coprime, their degrees are the same, and  $E$  is nothing but the GCD of  $N$  and the degree of  $F$ , which is also the degree of the point.

As an example, if you take an irreducible polynomial  $x^6 - \alpha$ , then it is supposed to be irreducible over  $F_q$ . So, what will happen when you go to  $F_{q^2}$ ? So, when you go to  $F_{q^2}$ , this degree 6 polynomial will essentially split into two degree 3 polynomials, each of which will be irreducible. So,  $x^3 +$  or  $-$  the square root of  $\alpha$ , okay? Also, if it were just  $x^2 - \alpha$  that you had, then  $x^2 - \alpha$  would completely factor when you go to  $f(u^2)$ , and for any other even degree, it will simply split into factors of degree divided by 2. This can be shown easily; these are the properties of the main polynomial at the point when you move to an extension.

That is what we must deduce. What it says about the point is that point P corresponds to the points Q1 through QE. In  $C_n$ , the degree of the point is equal to the degree of  $Q_i$ , and all these degrees are the same. So, it is E times d of  $q_1$ . Okay, so you can rehash this polynomial factorization into our degree operator at this point. Essentially, what is happening is that this point, which was a prime ideal in  $F_q$ , gives you the prime ideal factors into prime ideals in the new world when you go from  $F_q$  to  $F_q$  to the n.

In the new field,  $Q_1$  to  $Q_e$  and their degrees are the same, which will then be equal to  $d(p / e)$ . This is an equivalent formulation at the level of points. So, what is the current contribution to the Z function? Let us check that. Thus, the contribution in  $Z_{t^n} C_n$  is the left-hand side of the theorem. The contribution coming from point P is as follows.



Do we believe this? So  $t^n$  comes for free because we have already substituted  $t^n$  into the Z function. The degree of  $Q_1$  is  $d(P) / E$ , so that is in the exponent, and the contributions are coming from  $Q_1$  to  $Q_E$ ; they are the same contribution, so we have multiplied that, right? So, corresponding to P, when you look at the conjugates that split above as you approach  $F_q$  to the N, you get these E factors in the product. This, we can say, is the exact contribution from P on the left-hand side. Is that fine? We have to match this with the right side. What we will show is the following identity: Yes, the above expression is simply  $1 - t^{n \cdot d(P) / e}$ .

Now, we want to study that expression. So, regarding that expression with E in the exponent, we want to see how it factorizes. Once we establish this claim, you can fit it in and see that the RHS contribution is the same, right? So what we basically have to show is this factorization, which is a bit strange because on the left-hand side, you have multiplicity E, but on the right-hand side, you seem to be getting different results. Right, but are you hitting different things? Since  $\eta$  is an nth root of unity, and n and the degree

dp share a common factor, their gcd is e. After a few steps, the term  $\eta$  raised to the dp repeats, and you can show that it repeats exactly with a multiplicity of e. That is what we will check now; it is actually easy to verify.

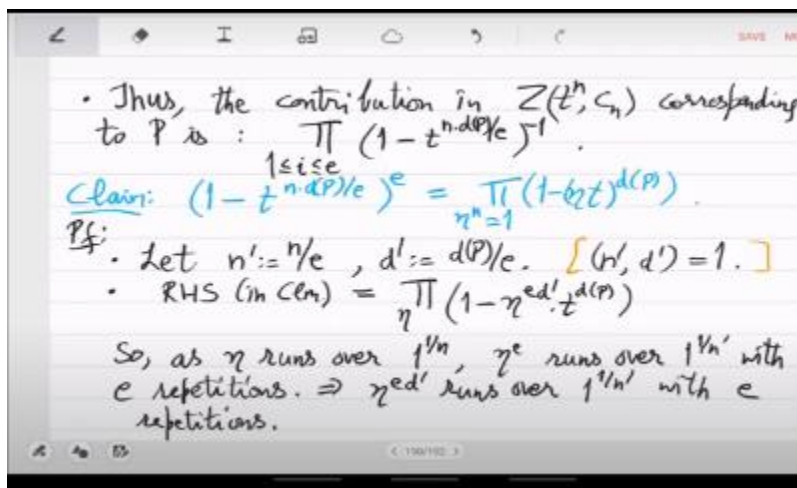
Let  $N'$  be  $N$  divided by  $\text{GCD}(E)$ ,  $D'$  be  $DP$  divided by  $\text{GCD}(E)$ , and you know that this is true because the GCD of  $N$  and  $DP$  is  $E$ . Therefore, when you divide them out, they become coprime. The right-hand side of this claim equals the sum of the  $\eta$ 's,  $1 - \eta$ , and the degree of the point raised to the power of  $t$ . So, as  $\eta$  runs over the  $n$ th roots of unity, all of them are raised to the  $ed'$ , or  $\eta^e$  runs with  $e$  repetitions. What we are saying is that as  $\eta$  goes over these  $n$  roots of unity,  $\eta^e$ , since  $e$  divides  $n$ .

What  $\eta$  raised to  $E$  is just the  $n$ th prime root of unity, so you will actually see things repeated  $E$  times; every value gets repeated  $E$  times.  $D'$  is co-prime to  $n'$ , so if you raise this to  $D'$ , the same behavior can be observed. So,  $\eta^{ed'}$  runs over with the same number of repetitions; that is all. This indicates that the multiplicity =  $E$ . All we have to check is whether the base is also correct:  $T^{N/D} / E$ .

Let us also verify that. Essentially, what you can say is... You have a product, so you get  $\eta^e \cdot t$  raised to the power of  $dp$ . Can I say this? This whole thing is raised to  $E$ - I hope this is correct.

So,  $\eta^{ED'}$  is nothing but this  $\eta^e$ , which is the  $N$ -th root of unity. You go over the distinct ones and then raise the whole thing to  $E$ ; that is the repetition, and that is the multiplicity. So, what is this now, the thing inside? I guess that should just be  $T$  raised to  $dp^{n'E}$ , right? That is as promised. So, that is the left-hand side. Is that fine? Yes, we have verified this factorization using the  $n$ th roots of unity, and this essentially informs you about the  $Z$  function.

So, the contribution of  $P$  in this  $Z$  function substitution is exactly that. Which, yes, is already the factorization of  $Z$  in terms of  $T$  and  $C$ . Okay, because this  $1 - \eta t^{dp-1}$  is the contribution of  $p$  in this particular substitution of  $z$ , which is  $z(\eta t, c)$ . We have checked the contributions in all these  $z$  substitutions, and the product matches the left-hand side. Is that fine? Okay, yeah, so we did this mainly to understand  $\delta$  and how it would help.



The corollary of this is that there are exactly two poles.  $\Delta = 1$ . Let us prove this. The calculation of the functional equation we performed essentially tells you that the Z function, after you perform the infinite series summation, is a polynomial  $L_T$  multiplied by  $(1 - t^\delta)(1 - q t^\delta)$ , where  $L_T$  is an integral polynomial in the variable  $t$ .

Yes, I am not saying anything about the degree of  $L$ . I am just saying that the denominator consists only of these two terms:  $1 - t^\delta$  and  $1 - q t^\delta$ , which is easy to verify. Yes, we now want to use this base change theorem. So, what should we change the base to in order to obtain some information on  $\delta$ ? So, here is an interesting trick. So let us change the base to  $n = \delta$ . Okay, so this  $\delta$ , or so, remember that this is happening over the integers.

So it is not clear why we should choose this as our base change, because the field was  $\mathbb{F}_q$  and we are going to  $\mathbb{F}_q^n$ . Now, I am suggesting that instead of  $\mathbb{F}_q^n$ , we go to  $\mathbb{F}_q^\delta$ . Okay, that is, then apply the base change theorem. What you will receive is the following formula.  $z t^\delta c$ ,  $\delta =$  the product of  $\eta^\delta = 1$  So,  $\eta$  is a  $\delta$ -th root of unity, and it goes over all of them:  $Z$ ,  $\eta$ ,  $t$ , and  $c$ .

What happens here? So, something interesting is going to happen now. The reason is that when you substitute  $\eta t$  and replace  $t$  with  $\eta t$ , the denominator will not change; that is why we did this. So, you will get  $L(\eta t)$  that changes, but not the denominator, right? So, this means that you are essentially getting the numerator as the product of  $L(\eta t)$  over all  $\eta$ . This will become  $t^\delta$ . That is not very important; what is more important here is that the denominator is exponentiated, resulting in this.

That is the important thing, so in the denominator, you are essentially getting poles with multiplicity  $\delta$ , correct? And why is that a problem? Yes, on the left-hand side, we have substituted  $T^\delta$ , so we need to deduce this carefully. You simply substitute  $T$  raised to the  $\delta$  in the formula above. The above formula, yes, with the different  $L$ . So, let us do that carefully. On the other hand,  $ZT^\delta C^\delta$  is another  $L'$  function where you substitute  $T^\delta$ , and in the denominator, you have.

$$\Rightarrow \text{RHS} = \left( \prod_{\substack{p \text{ is in } |Y| \\ p \neq \infty}} (1 - \gamma^p t^{d(p)}) \right)^e = (1 - t^{n/d(p)})^e$$

$$= (1 - t^{n/d(p)})^e = \text{LHS} \quad \square$$

- Going back to  $Z(\cdot)$ : the contribution of  $P$  in  $Z(t^n, c^n)$  is  $= \prod_p (1 - \gamma^p t^{d(p)})^{-1}$ .

$$\Rightarrow Z(t^n, c^n) = \prod_p Z(\gamma^p t, c) \quad \square$$

Corollary (Two poles):  $\delta = 1$ .

So, let us not do this in 1 step; let us do it in two steps. The  $Z$  function for  $C_\delta$  looks like this, which implies that the  $Z$  function, when substituting  $T_\delta$  for that curve, is  $L'_T_\delta$ . Is that correct? Okay So, yes, we have these two expressions. The place where you will find a contradiction is that, in this case, all the poles are simple, which means they are simple poles. Yes, his point is correct.

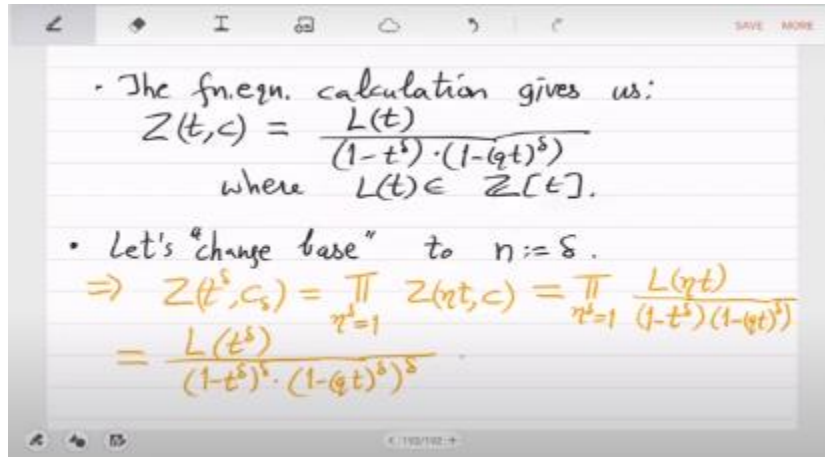
But let's, yeah, which is why this needed to be done carefully. So let's do that. Let's call this  $\delta'$ . Still, it should be okay; do you see that? We are doing this properly now. Today, I think the projector is not good; it does not show the colors.

So, even if it is different, the form is still the same. So, when you substitute  $T^\delta$  in this form, you see that there are more poles, but they are all simple. There may be more poles, but they are all simple. So there is no repeated pole; however, in this expression, you seem to be obtaining a multiplicity  $\delta$ . The only way to achieve this is for  $\delta = 1$ . So, in the calculation of the functional equation, the term we have is  $q - 1 \cdot z_t$ .

If I multiply it by  $t - 1$  and then set  $t = 1$ , we see that we obtain the class number  $h_c$  when  $\delta = 1$ . So in the calculation, we had this  $h_c/t - 1$ , correct? So, if you clear out  $t - 1$  and then set  $t = 1$ , you will obtain the class number, and now you can gather information about  $L(t)$ . This means that  $(q - 1)$  times  $L(t) \cdot (1 - t)$  is eliminated. So, you get  $1 - qt$  and  $qt - 1$  at  $t = 1$ , which is equal to the class number, which means that.



So, on the left-hand side,  $q - 1$  will cancel. So, you understand that  $h = hc$ . Okay, so  $L$  of 0 is trivially 1, but  $L$  of 1 is an interesting invariant: it is the class number of the curve.



The fn. eqn. calculation gives us:

$$Z(t, c) = \frac{L(t)}{(1-t^\delta) \cdot (1-qt)^\delta}$$

where  $L(t) \in \mathbb{Z}[t]$ .

Let's "change base" to  $n := \delta$ .

$$\Rightarrow Z(t^\delta, c_s) = \prod_{\gamma^2=1} Z(\gamma t, c) = \prod_{\gamma^2=1} \frac{L(\gamma t)}{(1-t^\delta)(1-qt)^\delta}$$

$$= \frac{L(t^\delta)}{(1-t^\delta)^\delta \cdot (1-qt^\delta)^\delta}$$

That's an interesting fact, so let's compile these facts into a major theorem. The properties of L-functions are, well, this is simply a property of the curve, not of the L-function, but we have demonstrated it using this as an intermediate function. So the following sequence is now exact, correct? So this was the containment, and this was the extent.

So, the degree of the class group is subjective, okay? The content here is that there is a divisor whose degree is 1; that was the only thing missing from our understanding, so now we have it. There is a degree 1 divisor, and this is true over any field of constants. You can take the finite field  $F_p$ , and that is correct. The second property is that we have just seen the Z function is  $L(t) / |1 - t| \cdot |1 - qt|$ , where  $L(t)$  is integral. And its degree is equal to what? Now, with  $\delta = 1$ , you can go back and check the calculation of the functional equation.

There was a  $2g - 2$  appearing, and there were terms in the denominator. You multiply by them, and  $2g - 2$  becomes degree  $2g$ , so the degree is equal to  $2g$ . It satisfies the functional equation, which is as follows. You can also check the calculation we did by simply eliminating the denominator. The functional equation for  $z$  provides you with the functional equation for  $1$ , which is  $qt$  squared raised to  $g$ .

That's how the L function transforms, which, by the way, is a polynomial. It's a degree  $2g$  polynomial. So that you can also deduce from this. There is a  $t$  raised to  $2g$  appearing. So, it makes sense. That can only happen for degree  $2g$  because you are essentially substituting  $1/t$  on the other side.

$L_0$  is 1, and  $L_1$  is the class group, which represents the class number, okay? So, these are the properties of this L-function. Are there any questions? Yes, that's a good question. Uh, I did not think about it. Yes, that is a good point. So, even if this degree were not 1, suppose you wanted to reach this  $\delta$  degree divisor.

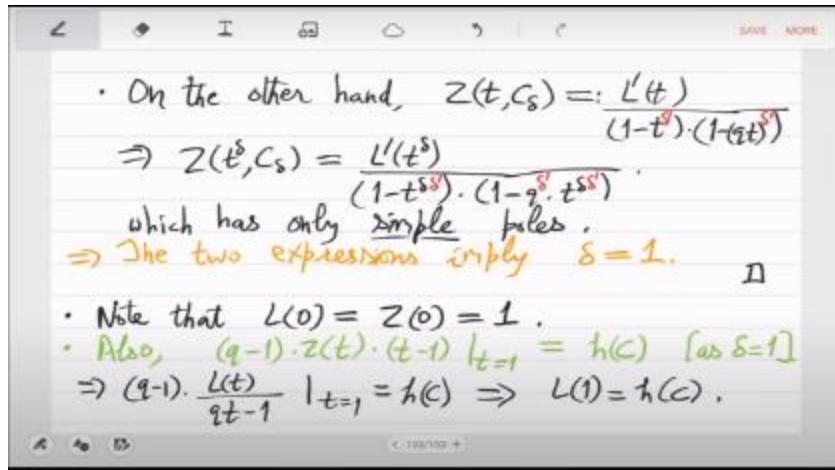
So, what you should do is sample two random points and then consider  $p_1 + p_2$ . Actually,  $p_1$  will have an order of something,  $p_1$  will have a degree of  $d_1$ , and  $p_2$  will have a degree of  $d_2$ . You use Euclid's algorithm to express  $d_1$  and  $d_2$  as a combination equal to  $\delta$ . Suppose  $a_1 d_1 + a_2 d_2 = \delta$ ; then the divisor should be  $a_1 p_1 + a_2 p_2$ , and the same thing will yield. Those are abstract points; this is an actual point of degree 1.

No, that is not the claim. Is there an actual point. No, this is a claim only for the class group. What you are saying is not true. It may not even be the total of the actual points.

The divisor may simply be a sum of prime ideals. Since you can use both positive and negative integers, you can understand what Euclid's algorithm is. Yes, that is the correct way to understand it. See, asking anything about actual points is very difficult because we have not yet proven the Riemann Hypothesis. Right, so we do not know whether these actual points even exist. Your curve may have nothing in the field of constants  $k$ , so you have to go to a very large field.

Unless we prove the Riemann Hypothesis, all your questions are somewhat based on the hypothesis. So, let us just consider that as a computational question here. Compute a divisor  $D$  that is in the pre-image of 1. This would essentially involve sampling not 2 points, but 2 prime ideals, and you still have to do this; it is not immediately clear.

Because you may not have any actual points. Since you do not have any actual points, you will either need to sample from prime ideals or wait until we prove the Riemann Hypothesis. Once that happens, we will have many points in the base field, and you will be able to sample from them. That would be the correct algorithm, but then you would have to wait for it. The second question is, "Can we compute LT?" Given, of course, the curve over the field of constants, right? So, we know that when we proved Riemann's theorem, we observed that the genus is not too large and that the computation of the genus can be done efficiently. In terms of the degree of the curve or the degree of the planar representation of the curve, the genus is maximally quadratic. The degree of  $L$  is not large; it is only quadratic in the input.



We are asking two questions: How big are the coefficients of the L function? If these coefficients, which are integers, are too large, then you cannot even output them correctly. So, how big are these coefficients? If they are small, can you compute them? That is the second question, and it is a harder 1. As Madhavan will tell you, there is no solution. Even after a lot of work, there is no algorithm to do this; the best you can achieve is exponential-time algorithms.

Even that is not clear; it will only become clear through the hypothesis. Because if nature were too harsh, and if these curves were too poor, then the coefficients of L could have been doubly exponentially large, and there would be no way to output that. Is there even anything that exists? Yes, yes. Among these questions, the second 1 is definitely open. The first question will be easy once we have solved the Riemann hypothesis.

Also, this question will be easy because the L function has small coefficients. So, 1 can present them efficiently in the output. But we do not know how to compute them; the presentation will not be a problem, okay? So, yes, now let us come to this hallowed connection to counting points on the curve in the field of constants, shall we? So, what does that have to do with the Z function? So, I mean that the way we have defined the Z function is the way Riemann defined his function, which is via the sum of  $1/n^s$ . In our case, it is the sum of  $t$  raised to the degree of the divisors, which are like numbers. In Riemann's hypothesis, it is also unclear how his function connects to counting primes, right? A systematic way to go from there to counting primes exists. We can do something similar here; it will involve simple algebra to connect our Z function with counting actual points on the curve in the base field of constants.

So, let's do that next. Let's start with the Euler product, which we have been using all the time. To simplify, let's denote it as  $z$ ;  $z$  will represent the Z function of the curve  $C$  over the field of constants  $k$ .

It factors as follows. So, by definition, this is not a case we encountered when we defined the Z function,  $\sigma(t)^d$ , which sums  $\sigma(t)^d$  of a divisor over all the positive divisors that factor in this way over points. That is why, in fact, we go over non-negative divisors, so that the matter will ultimately resolve itself into points. Now, this is a strange product because the points, which are even the main ideas, are infinite, right? So you are actually multiplying infinitely many things, but you can see that everything is well defined. There is a notion of convergence in power series, so it's okay; you can actually perform the multiplication.

The next thing we will do is something even stranger: we will differentiate this identity. Okay, so it's already an infinite product, but let's make it even stranger by actually performing two operations. Let us apply the logarithm and then take the derivative. So, use the logarithmic derivative. What you do is take the logarithm of both sides and then differentiate with respect to the only variable,  $t$ . So, what does that accomplish? We are doing this so that the product—I mean, the logarithm of the product—is the sum of the logarithms.

So, you convert the product into a sum using logarithms and then differentiate it. So let us see what you have. So let us not worry about  $z$  for now. The  $d \log(z)$  is equal to the sum over all the points, and the summand is  $d \cdot \log((1 - t)^{-1})$ . Okay. So just remember this identity: the derivative of the logarithm of a function is equal to the derivative of the function divided by the function itself; that is what we want to use.

Right, so the left-hand side has become  $z' / z$ , and here you will get the derivative of this:  $1 - t$  raised to the power of negative 1, divided by itself. So, let's do that. So, what is the derivative of this?  $-1 \cdot dt \cdot (1 - t)^{-2}$ , divided by itself.

Oh, sorry, I messed something up.  $-1$ , then you get  $1 - A$ ,  $dp - 2$ , so you actually get 1 here. Okay. There is a  $-1$ , so when you differentiate, you will get  $-1$ , but  $-1$  will become  $-2$  in the exponent. Yeah, yeah, but let's not do that.

This is just using  $f' / f$ ; that is all—no further tricks. So it becomes this, and there is no  $-1$ . This is also not present because, yes,  $-1$  times  $-1$ , the quantity  $(1 - t)$  raised to  $dp$  gives you  $-1$  as well. Yes, this is the expression. And, right, how would you like to see this? I want to see it this way.

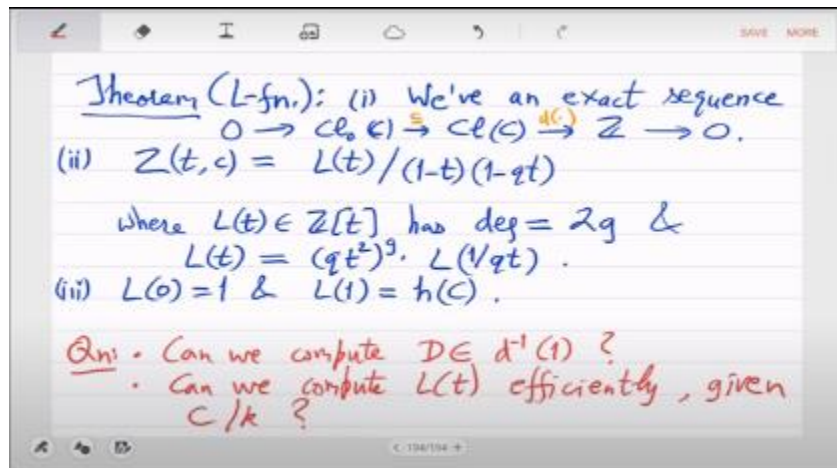
Go over all the points. The degree of the point multiplied by all the numbers is correct. So,  $\sum dp$  is out, and  $t^{-1}$  is also out. Now, what we are doing is taking  $t$  raised to the  $d$  power divided by  $1 - t$  raised to the  $d$  power, and we are simply expanding it back into a power series. Right, so you get powers of  $t^d$ , with  $t^{n \cdot d}$ , where  $n$  starts at 1.

That is what it is. Whenever you see a summation, you should try to swap it. So let us swap this. What will you get? This is  $T^{-1}$  times the summation. Suppose I went over the numbers  $m$  to get  $T$  raised to  $m$ . What is the coefficient of  $T$  raised to  $m$ ? What is it counting? Yeah, let's go over the numbers first and then look at the points they are counting. So,  $t$  raised to  $m$  will be counted and will appear here only when  $d$  of  $p$  divides it, and it will then come with  $dp$ , right? The coefficient, in simpler terms, of  $t^m$  inside this inner sum comes from those points whose degree divides  $m$ .

The contribution, or weight, of that is  $d(p)$ . That is what we have just swapped in the summation; so what does this mean? How can you read this off now? In the finite field of size  $q^m$ , is that clear? So, if the degree divides, think of the field  $\mathbb{Q}^M$ , right? Its size is  $q^M$ . In that field, since the degree of this point divides  $M$ , that prime ideal actually completely factorizes. For that cloud, you are actually in the splitting field, in 1 of the splitting fields. So, how many factors will you receive?

Exactly  $d$  of  $p$ . So all the conjugates are present in this field, which has a size of  $q^n$ , correct? So you are actually counting points in that field; that's all you are doing.

So, what is the number of points in that field? So  $N_m$  is the number of points on the curve above that constant. That's all, isn't it? That's all you have in the RSS feed. So, essentially, there is a mysterious connection between the Z function, as we defined it from first principles, and the generating function of the points we wanted.



There is a clear connection. So, let us finish this. So, let us integrate it. To remove the "d" on the left side, the derivative from 0 to  $t$  gives, so when you integrate from 0 to  $t$ , the

derivative of the log of  $z$  will become the log of  $zt$ . Sorry, what will the right-hand side become? There is  $T$  raised to  $M - 1$ , right? So this will just become  $T$  raised to  $M$  divided by  $M$ , starting from 1. Yes, that is it. In other words, if you do not like logarithms, then you have to use exponentials, so the exponential of  $\sigma$ , okay? So, that is the connection between the ordinary  $Z$  function definition and the generator you would want; they are exponentially related, okay? So, this is brilliant.

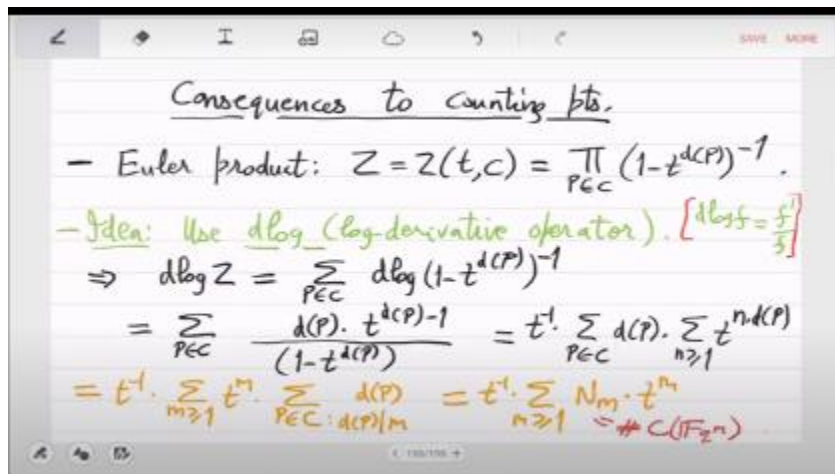
It is especially brilliant because, as we have written it as an  $L$  function, it is  $L(t) / (1 - t)(1 - qt)$ . So now, if you also expand  $Lt$  using its roots, you can proceed. We'll achieve a magical result because we are using the first identity. Uh, so the logarithm of  $L_t$  can be expressed as expressed a product.

So, you find the sum of the logarithms of the factors, compare both sides, and arrive at a formula for  $N_m$ . Let's do that. Um, so now use the fact that  $Z_t = \frac{L_t}{(1 - t)(1 - Qt)}$ . Furthermore, do not think of  $L_t$  as a polynomial; think of it as a product. It is univariate, so it completely factors. We do not know about its fundamental properties—perhaps its roots are not simple, and they may repeat, and so on.

However, over the complex numbers, there are roots, so let us just factor it. You know how many roots there are when counted with multiplicity, which is  $2G$  roots.

Its degree is... so I will write in the... I will write this differently, and the reason will become clear soon, because I essentially want to take the logarithm of both sides, right? So if I write  $1 - \alpha_i t$ , the logarithm of that gives me a better expression. Instead of expressing this as  $t - \alpha_i$ , I write  $1 - \alpha_i t$  so that the logarithm will work better.

So,  $A$  and  $I$  are complex numbers, and let's check. Just, yeah, just that. Correct. The roots of  $L$  are actually units in the complex field. So, you can invert them. So, that is what we have done. So, these are actually the inverse roots of  $L$ , or the inverse zeros of  $L$ .



Now,  $Z$  is also a product that will help with the first formula. So, let us plug it in. What we have now is the log of  $1 - \alpha_i t$  from  $i = 1$  to  $2g$ , which is the L-function part, - the log of  $1 - t$ , - the log of  $1 - qt$ . And this is equal to  $\sigma(nm)$ , the generating function, essentially, right? So now, from here, you can read off the formula for  $n_m$ , which is  $n_m = q^{m+1} - \sum \alpha_i^m$  raised to the  $m$ . Right? That is the formula. So,  $\frac{1}{m}$  can be, I mean, basically just the logarithm; you recall that the logarithm of  $1 - t$  is, or rather, - the logarithm of  $1 - t$  is just  $t + \frac{t^2}{2} + \frac{t^3}{3}$ , and so on.

So,  $t$  raised to the power of  $m$  is present everywhere. So forget that;  $n_m = q$  raised to the power of  $m + 1$ , which comes from the denominator of the  $Z$  function. The interesting part comes from the roots of  $L$ , the inverse roots of the  $L$  function, and many others related to  $2g$ . So this part,  $\alpha_i$  to the  $m$ , is regarded as the error term. Why is there an error term? Well, if this were not present in the projective line, the curve would have  $q^{m+1}$  points, right? So, that is another way to view it.

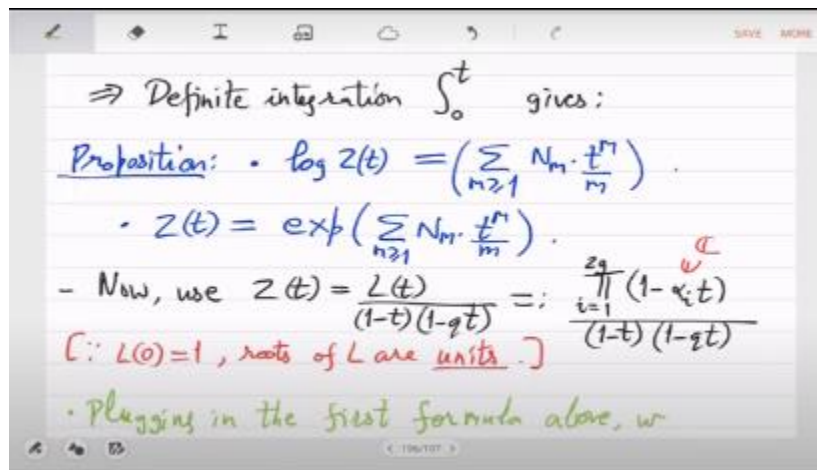
So, this is the projective line plus an error. So, the projective line has  $q^{m+1}$  points, right? The point at infinity is positive 1, and the others are from the affine. So, this error is 0 only in the case of the projective line. For all other smooth projective curves, you will have some error term, + or -. So, since you are summing over complex numbers, I should have said  $\sum \alpha_i$  or  $\sum \alpha_i$  to the  $m$ .

Since this comes from an integral polynomial, it will always be real. In fact, it will always be an integer in this instance. So, this integer can be positive, negative, or zero. So when it is 0, you see that this is the case of the projective line. In other cases, you will be slightly above or below the average. Yes, that is true because it is a statement for all  $m$ .

In small  $m$ , weird things can happen, but if it is true for all  $m$ , then your curve must be a line. Yes, the fundamental question that was asked more than 100 years ago is: How big is the error? So, what is your guess? So, how big can the error be? Right, so the version of the Riemann hypothesis basically states that the error cannot be too large. In fact, the error term will be the square root of the main term; it is bounded by the square root multiplied by the genus  $g$ . Thus, it aligns very nicely with what happens over the numbers. So, for the estimate of primes, the error term is conjectured to be the square root of the main term.

The same thing you would conjecture here; the difference is that we will actually prove it. In fact, we will prove something very significant: we will prove that the  $\alpha$  i's are not arbitrary. So, the  $\alpha$  i's themselves will prove that their norm is very special; it is equal to the square root of  $q$ . So, that's the version of the Riemann hypothesis that we will prove. 1 last thing I want to mention is that, through this functional symmetry, we immediately obtain the following observation: the property that we can label  $\alpha$  i's such that  $\alpha$  i times  $\alpha_{i+g}$  equals  $q$ .

Let us see why it is actually true that you obtain this immediately from the symmetry. So, the symmetry basically relates  $L(t)$  to  $L(1/t)$ , right? So, if  $\alpha$  i is an inverse root, then it indicates that there is another inverse root, which I am calling  $\alpha$  of  $i + g$ , such that the product is  $q$ . This follows from the symmetry. So, you have  $2G$  roots; you can label them and arrange them so that this property holds for each pair. But, as I said, when we prove the Riemann hypothesis, we will actually demonstrate something very powerful: we will show that the norms of these two are equal as well.



So, we will show that the norms are equal, which means that the only option is the square root of  $q$ . This is part of the symmetry; I mean, you can try to deduce it from the



symmetry, but it is much more than that. So, I don't know why people would have conjectured that. This thing is amazing because it is what causes the discussions now. We have to fight this other pair so that everything is resolved. Yes. So, okay.

Handwritten mathematical derivation on a digital notepad:

$$\Rightarrow \sum_{i=1}^{29} \log(1-x^i t) - \log(1-t) - \log(1-t^2) = \sum_{m \geq 1} N_m \cdot \frac{t^m}{m}$$

$$\Rightarrow \forall m \geq 1, N_m = 29 + 1 - \sum_{i=1}^{29} \alpha_i^m = |P_1(V_{29}^m)| + \text{error}$$

$\triangleright \sum_{i=1}^{29} \alpha_i^m$  is viewed as the error-term.