Computational Arithmetic - Geometry for Algebraic Curves

Prof Nitin Saxena

Dept of Computer Science and Engineering

IIT Kanpur

Week - 12

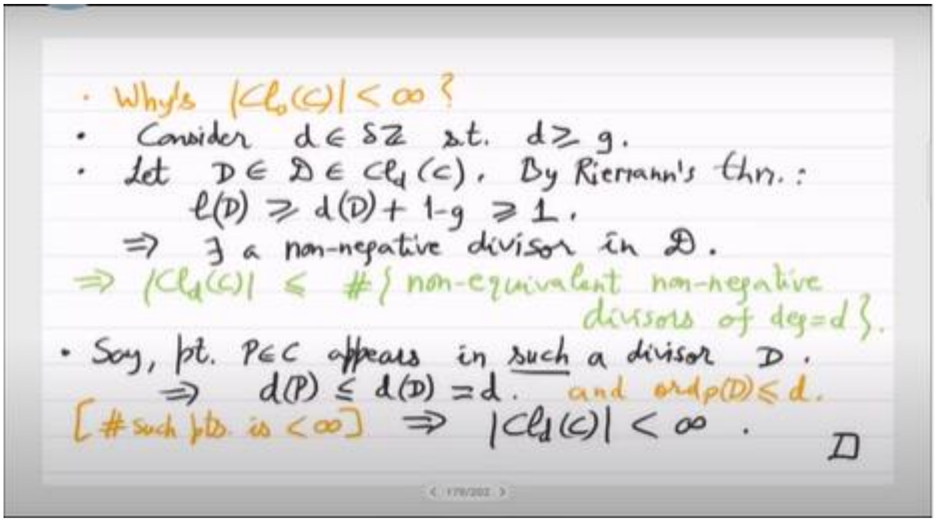
Lecture - 24

Riemann Hypothesis for Curves

Okay so last time we showed that this sequence is exact. So degree 0 to, degree 0 class group to class group to integers via the degree which means that all degrees are possible, all integers are possible and this surprisingly we got from the Z function definition which was not required to define the sequence, but to prove its exactness interestingly Z function was needed. And then we showed that it is z is equal to this l function divided by something very simple 1 - t . 1 - qt. So, degree of l is 2g that is the numerator degree of denominator is 2. so this is the rational function, L function has important properties, L of 0 is 1 and L (1) gives you the size of the class group, so H (C) we had defined. Yes h (c) was this definition size of the degree 0 class group that is called the class number of the curve.

Why is this number finite? The way we are defined class group it seemed to be infinite. Yeah, so actually that needed a proof we showed that yeah we showed on the first slide we showed that the degree 0 class group is actually finite. Yes, it is actually the number of non-equivalent non-negative divisors. No, so we showed this by I mean it is a non-trivial argument.

We reduced it to a non-negative divisor and then we use the definition of this LD, LD sheaf to show that we can now assume the divisor is positive. This proof, so this proof was via I mean once you find something in LD, LD >= 1, once you find something in LD then that function f you can add it to your D and it becomes positive. So ultimately it actually is only you only have to count these non-equivalent non-negative divisors of degree D that we showed is finite. So that is an interesting proof it goes via degree positive but it tells you something about degree 0 also. Yes, this argument was for D >= g.



- Why's $|Cl_0(C)| < \infty$?
- Consider $d \in \delta\mathbb{Z}$ s.t. $d \geq g$.
- Let $D \in \mathcal{D} \in Cl_d(C)$. By Riemann's thm.:

  $\ell(D) \geqslant d(D) + 1 - g \geqslant 1$.

  $\Rightarrow$ $\exists$ a non-negative divisor in $\mathcal{D}$.

$\Rightarrow$ $|Cl_d(C)| \leqslant \#\{$ 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 $\mathrm{ord}_P(D) \leq d$.

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

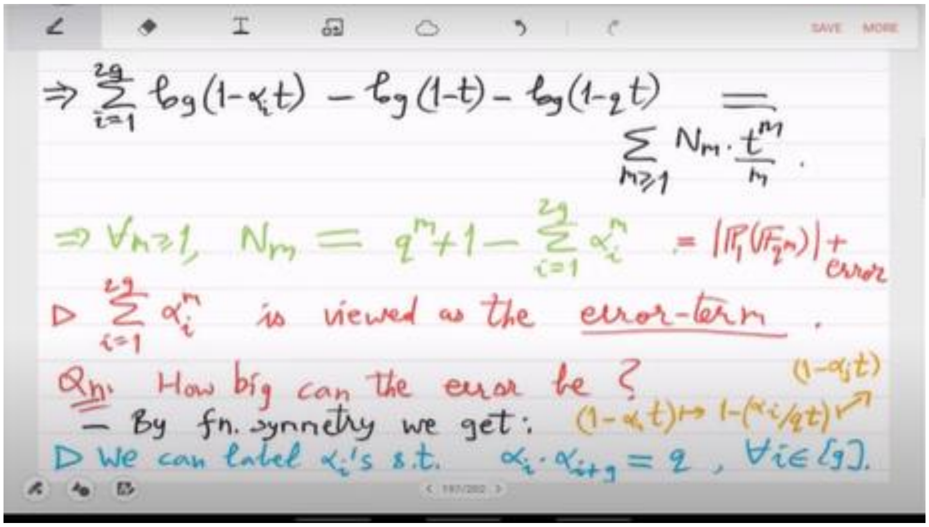
it was only for large d's for large degree you argue and then that gives you information about degree 0 class group. So, yeah after that we have shown this connection of Z function with counting points, so zt is equal to exponential of the generating function and from that we get this nice formula, we get this formula in green that counting points on the curve which are in the finite field q ^{m}, that is basically given by the number of points on the projective line plus some error and the error term is also given very exactly by the complex roots of L function, which at this point is totally black box, we do not know how these α is behave. But we do know by the functional equation symmetry that you can pair up the complex roots so that the product is Q, right. So we reach till this point. Now the magical thing that the functional yeah use L $^{(1)}$ / Qt.

So actually it is not α is not the root it is the inverse root we are looking at L t as product of 1 - α i t. So when you substitute 1 / Q t α i / Q will be equal to some other 1 / α j. Q / α i = α j. Yeah it is the same thing.

Yes. So, α i / Q will be equal to some other by that you get that the product = Q. yeah I mean this is a bit inverted. So, you will get 1 - α i t will become 1 - α i by q t. So, t also goes in the denominator. q / α i, we are inverting the root z $^{(1)}$ / q t.

Yeah so, T is replaced by 1 / Q T. So, this is the problem it is T is also in the determinators. So, you have to normalize by T and then see what is happening. So, α i / Q will be a root which means that α / i / Q will be equal to ∑ 1 / α j. that is the sequence of transformations.

Yes, so that will that means that α i α there is still something wrong, no it's okay, it's actually when you transform you have to see that t you have to look at this as t - α e / q, so α e / q = 1 / α g, that's the pairing, so functional equation gives you this symmetry. The next thing we will prove is the Riemann hypothesis which conjectures that the norms of α i's are equal which means that they have to be √ q.



$$\Rightarrow \sum_{i=1}^{2g} \log(1-\alpha_i t) - \log(1-t) - \log(1-qt) = \sum_{m\geq 1} N_m \cdot \frac{t^m}{m}.$$

$$\Rightarrow \forall m\geq 1,\ N_m = q^m+1-\sum_{i=1}^{2g}\alpha_i^m = |\mathbb{P}_1(\mathbb{F}_{q^m})| + \text{error}$$

▷ $\sum_{i=1}^{2g}\alpha_i^m$ is viewed as the error-term.

Qn. How big can the error be?

– By fn. symmetry we get: $(1-\alpha_i t)\mapsto 1-(\alpha_i/qt)$ ↗ $(1-\alpha_j t)$

▷ We can label α_i's s.t. $\alpha_i\cdot\alpha_{i+g} = q$, $\forall i\in[g]$.

So Riemann hypothesis conjectures a strong symmetry namely that all these α i norms are equal. Yes it is not clear why you would want to conjecture that it seems outrageous that all the norms of α all these complex roots they have equal norm, but once you conjecture this then you know what they should be then they should be equal to √ Q from the previous property. because the product has to be Q if they are equal then the norm has to be √ Q.

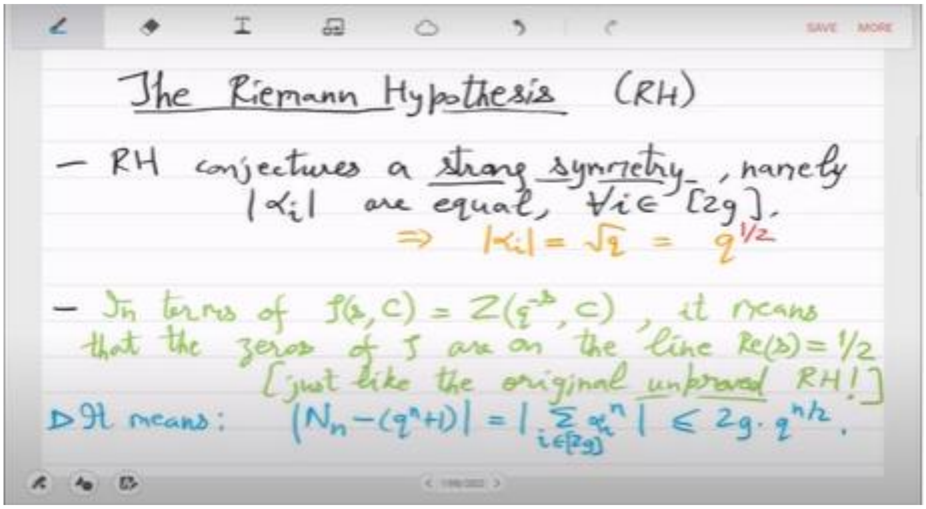
So this is what the Riemann hypothesis is. This jump to strong symmetry is obviously inspired by Riemann's original hypothesis where he jumped from functional symmetry to strong symmetry on the zeros. saying that all the zeros they lie on the line half, real part equal to 1/2. So that is the half which is also appearing here. So this half is the same, gives the same kind of picture.

Okay so yeah so what this comes from is you have to look at the Z S version. So in that Z version what it is saying is. that the 0's of Z are on the line real part equal to half ok, just like the original which is still an open question. So, the original Riemann hypothesis is still unproved, but that also boils down to such a statement that all the zeros of the Z function lie on real as equal to 1/2. So, that is what is actually true over finite fields curves over finite fields.

in terms of counting what this is saying is that the number of 0s of the curve in the finite field fq ^{n} this is equal to the norm of sigma α i $^{n\ i}$ going from 1 to which now will be upper bounded by 2g q ^{n} / 2. So, this is the you get this nice bound on the number of points. So, if you think of genus as small and q as big then you deduce that. The number of points on the curve in FQ is almost as many as Q + one. Right, which is a completely mysterious and out-of-scope statement because it is a general curve over a general finite field, and we currently do not know how many points there are even in the base field F_q .

However, this will essentially mean that the points are q + 1 pm text error, which we can assume is quite small because it is the square root of the main term. No, no, this was α, and it was the inverse root. Yes. No, since s = a + ib, we have shown that it should follow from this point. It should be correct because it is happening in the exponent; it is q ^{s} .

So, you get information; therefore, Q raised to S gives you, and Q raised to real S gives you the magnitude. Or maybe there's one more thing: a simple observation does indeed need to be made, but let me skip that part. We will proceed with our current Riemann hypothesis. This means that the number of FQ points on C, and when we say "curve," we obviously mean smooth and projective. On a curve, the points FQ are in the range of Q ± 1 ± 2√Q.



The Riemann Hypothesis (RH)

- RH conjectures a strong symmetry, namely $|\alpha_i|$ are equal, $\forall i \in [2g]$.

  $\Rightarrow |\alpha_i| = \sqrt{q} = q^{1/2}$

- In terms of $\zeta(s, C) = Z(q^{-s}, C)$, it means that the zeros of ζ are on the line $Re(s) = 1/2$ [just like the original unproved RH!]

▷ It means: $|N_n - (q^n+1)| = |\sum_{i\in[2g]} \alpha_i^n| \leq 2g \cdot q^{n/2}$.

This is the simple, elegant expression we obtain. It is as much about the line with the error in the square root and the genus. So, this is the fundamental result we want to demonstrate. We will prove this by performing a sequence of reductions and finally using the LD sheaf. So, the LD sheaf result we are using is quite mysterious, but the reductions we will perform will be more intuitive.

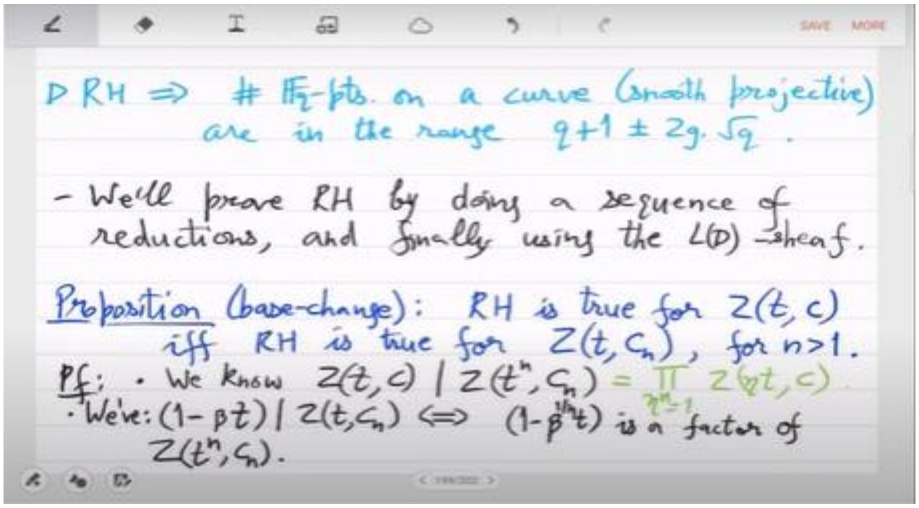
So, let us start with the reductions. So, the first reduction is again related to a change of base. So RH is true for ZTC if and only if it is true for CN. You can pick any n , and if you can show this—let's say you go to the F _q^2 and look at the curve as the F _q ^{2} curve—then if you prove the Riemann hypothesis, it will also be true for F _q . We want to go higher up; the advantage of doing so is that you may reach a very large finite field, which may make some things easier to prove.

So, let us first demonstrate this reduction. So, we know from the earlier identity that the Z function of the curve divides t^n c_n . We have demonstrated this previously. In fact, there was a strong identity in base change that we showed. We have shown that the identity z t^n, c_n factorizes using the base Z function by substituting t with η t , where η is an nth root of unity.

So we had this factorization proven. So let us remember that. So, in particular, Zt and C are factors of this; in fact, why not write it this way? So we know this; therefore, Zt and C are factors, and we take η to be equal to 1. So, this means that if you have the Riemann hypothesis for the right-hand side, then you also have it for the left-hand side, because of the Riemann hypothesis for Z_t, C_n , right? So, you will have information on that once you have information about the roots of t, comma cn. Actually, this needs to be done carefully.

So, if you have a √β_t or a factor β_t of z_t, c_n, then 1 - βη_t is a factor of Z_t ^{n}C_n, right? In fact, this is true if and only if it is specified. So, we have this property that if bη is an inverse root of Zt, then Cn. Then bη η is an inverse root of zt ^{n}, cn, where η is obviously arbitrary and a root of unity. Bη $^{1/n}$.

Yes, that is correct. Correct, so that is not good. Oh yes, that is the trick. Yes, you are right.



▷ RH ⟹ # $\mathbb{F}_q$-pts. on a curve (smooth projective) are in the range $q+1 \pm 2g.\sqrt{q}$.

- We'll prove RH by doing a sequence of reductions, and finally using the $L(D)$-sheaf.

<u>Proposition</u> (base-change): RH is true for $Z(t,c)$ iff RH is true for $Z(t,C_n)$, for $n>1$.

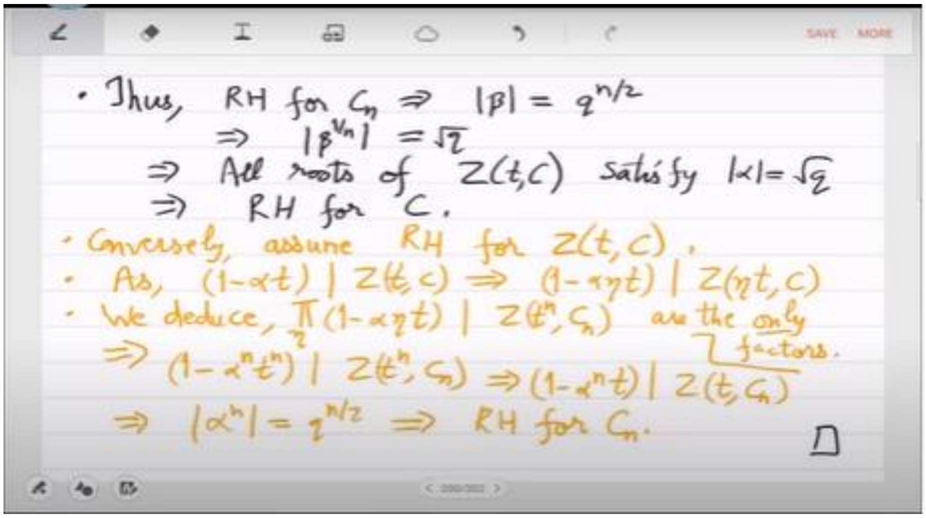
<u>Pf</u>: • We know $Z(t,c) \mid Z(t^n,C_n) = \prod_{\eta^n=1} Z(\eta t,c)$.

• We've: $(1-\beta t) \mid Z(t,C_n) \Longleftrightarrow (1-\beta^{1/n}t)$ is a factor of $Z(t^n,C_n)$.

That is a good point. Okay. So, the Riemann hypothesis for C_n would imply that bη^ 1 n = $q^{n/2}$, which means that bη^ 1 n = √ q , implying that all roots of z_t and C_n z_t satisfy this. This implies the Riemann hypothesis for the original curve, right? Because every 1 - α t that divides curve C also divides the RHS, and we have that information. So, we have information about C simply from the division. Conversely, what we need to demonstrate is the assumption of the Riemann hypothesis for Z(t, c) .

So, yes. Yes. So so So this means that 1 - α t is slightly different; you have to utilize this z, where η t, c, and all the roots come from α. H is related to k, and α comes from η t, c. Let us write that down: 1 - α t /z t, c implies that 1 -.

.. A η t divides η t, c. We can deduce that z t, for z t, c n, will first divide T n, C n. What does this tell you about z t, C n? These are the only factors. Yes, these are the only factors you know, but we only know them. Okay, we can take the product over η. We can do this because we actually have a product of z, η, t, and c.



- Thus, RH for $C_n \Rightarrow |\beta| = q^{n/2}$
  $\Rightarrow |\beta^{1/n}| = \sqrt{q}$
  $\Rightarrow$ All roots of $Z(t,C)$ satisfy $|\alpha| = \sqrt{q}$
  $\Rightarrow$ RH for C.
- Conversely, assume RH for $Z(t,C)$.
- As, $(1-\alpha t) \mid Z(t,C) \Rightarrow (1-\alpha\eta t) \mid Z(\eta t, C)$
- We deduce, $\prod_{\eta}(1-\alpha\eta t) \mid Z(t^n, C_n)$ are the only factors.
  $\Rightarrow (1-\alpha^n t^n) \mid Z(t^n, C_n) \Rightarrow (1-\alpha^n t) \mid Z(t, C_n)$
  $\Rightarrow |\alpha^n| = q^{n/2} \Rightarrow$ RH for C_n. □

Yes, this product actually divides z, tn, and cn, which is, I suppose, correct. So, it's 1 - α n t raised to the n. So, α n T divides T c n, which means that the inverse root norm is n-fold. So, that is $q^{n/2}$. I thought it was trivial, but actually, it requires some calculations.

So, we have shown both sides. So, that is one reduction. What happens when you make a Bayesian change? The Riemann hypothesis should be true in an equivalent way. The second proposition is now about a different kind of reduction. The following are equivalent: The Riemann hypothesis for Z states that the norm of the inverse roots is the √ Q. The second statement will pertain to the counting estimate rather than the root of the L-function for counting.

So, as long as $n - q^{d+1}$ < = $a + b\ .\ q^{d/2}$. For some constants a , b , and n , and for all multiples d of n . This is a bit complicated to read, but you should focus on the inequality first. As long as the count for Q raised to the D-sized finite field points is approximately Q raised to D divided by 2, with flexibility provided by the constants a and b for all multiples of n, where n is also a constant.

So, let n be 10. So, as long as you can prove this for, let us say, multiples of 10, that is also enough for d being a multiple of 10. So, you can jump over the d's; you do not need to demonstrate this for all d. But as long as you show it for a constant fraction of these, it will also imply the Riemann hypothesis. So, this is a relatively non-trivial equivalence. This must obviously be compared with what we said before, which is this line at the bottom.

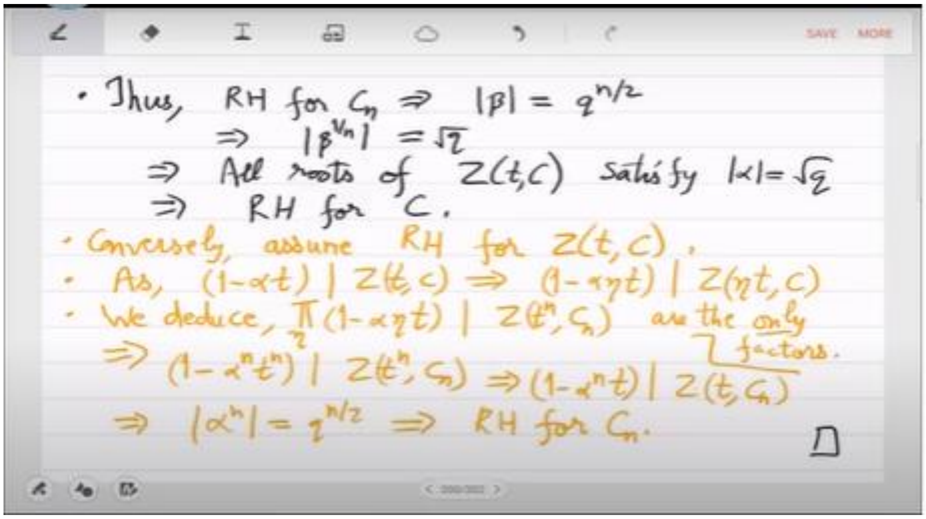
We stated here that it is less than or equal to 2g . Q^{n} / 2, and this is true for all small values of n. Now if we are saying that even if it is true for just constant tion of the small n's it is good enough. That is a significant weakness. Let me define what a constant is. Constant means independent of Q and D, or I think it is just independent of D.

So, AB Capital N has to be independent of D because you want to change D; that is what "constant" means, right? So, let us prove this. So, we have already seen one to two. For all d , the converse is the interesting part. How do we obtain the norm of α as the exact √ q from this approximate information? So, replace the base field with Q^n , which is constant, and now let us focus solely on extensions of Q^n. From Q^n, we move to Q^d because d is a multiple of n .

Q^n is contained in Q^d as we vary d; that is the context. So, the hypothesis implies the formula that we have. This is the strong property that actually shows $n - q^d + 1$, where the error term provides us with an exact formula. So, let's use that formula. The sigma α from a to the d norm < = $(a + b)^{(d/2)}$.

For all d divisible by n , that is exactly the hypothesis. From here, we must deduce that the α e norm is the √ q; it does not seem very easy. Because α is a random complex number, it could be anything. I mean, α can all be 0, so this inequality does not seem very strong.

So let us use the L function from which α derives. What is the product of A? The product of α can be used with symmetry. So, we can pair up the roots in such a way that each product equals Q. This is due to the symmetry of the functional equation. So, the product is actually Q^g; this is strong information that is available. So, α is not arbitrary; its product is actually Q^g, which means that if we show that the norm of each of them < = √ q, then we will be done, right? Because if all the norms are less than or equal to the √ q, that will suffice.



- Thus, RH for $C_n \Rightarrow |\beta| = q^{n/2}$
  $\Rightarrow |\beta^{1/n}| = \sqrt{q}$
  $\Rightarrow$ All roots of $Z(t,C)$ satisfy $|\alpha| = \sqrt{q}$
  $\Rightarrow$ RH for C.
- Conversely, assume RH for $Z(t,C)$.
- As, $(1-\alpha t) \mid Z(t,C) \Rightarrow (1-\alpha\eta t) \mid Z(\eta t, C)$
- We deduce, $\prod_{\eta}(1-\alpha\eta t) \mid Z(t^n, C_n)$ are the only factors.
  $\Rightarrow (1-\alpha^n t^n) \mid Z(t^n, C_n) \Rightarrow (1-\alpha^n t) \mid Z(t, C_n)$
  $\Rightarrow |\alpha^n| = q^{n/2} \Rightarrow$ RH for C_n. □

The product you want to be q^{2g} things needs to be q^{g}; thus, all the norms must be equal, and no single norm can be strictly less than $\sqrt{q}$. Therefore, we just need to show that the upper bound is that the α_i norm < = $\sqrt{q}$.

So, recall... The L function factors as follows, with α representing the inverse of the roots. So, let us take a look at this. So, that will be equal to that. So, we are taking the negative logarithm of both sides. So, the - log gives you log(1 / l t), and on the right-hand side (RHS), it essentially sums up the - log of (1 - α i t), which is just the sum of α i t^{d} divided by d.

The negative sign cancels, and then we rearrange. So, we obtain this expression. So, in fact, we could do this; that's the expression we receive. So, sigma α a to the d is sitting there in the coefficient of T raised to the d. So, there's something I need to change here: there is a typo.

So let's continue to refer to this as FQ. To simplify the notation, I have not only changed the base, but I also continue to refer to this q^{n} as f_q instead of introducing a new variable. Therefore, when I say q^{d}, what I actually mean is its original form, q^{nd}. So, yes, okay. So, if it is problematic, let us not do that; instead, let us call it q ‘. Thus, q is the input, and q ‘ is q^{n}, where n is the given constant.

So, if q^{d} is actually q^{nd}, now check that hypothesis 2 indeed gives me $q^{d/2}$. The correct product of α i is indeed q raised to g. I think q ‘ is the correct choice.

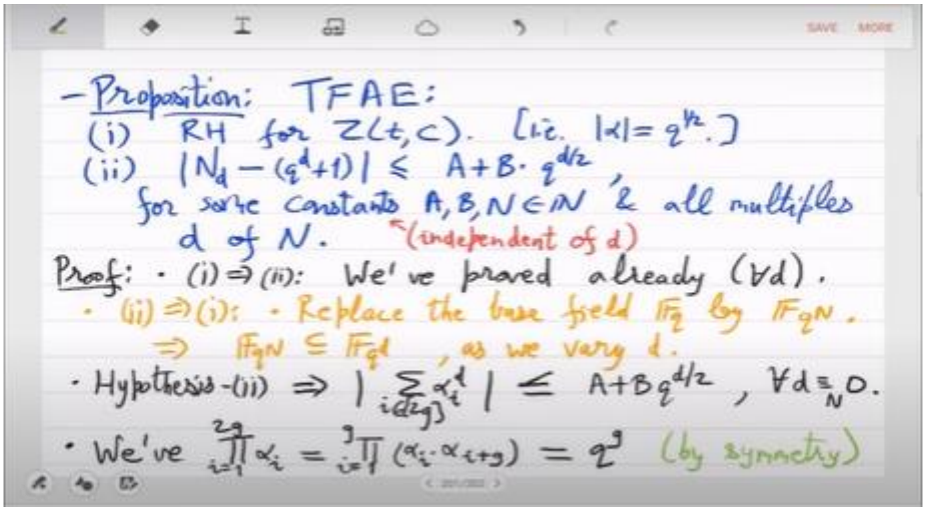
Let's see if it will work. So, I want to input the estimate now. So, what is that? The estimate is (a + b) . q^{d} div 2 . That's right. So, I can now take the norm of both sides. For the RHS, I can estimate the coefficient, which is the norm of a + b q^ d/2 and the norm of t^{d}, which I can rewrite as the a part. So, what is a part? It is σt ^{d} / d, which becomes the logarithm of the b part.

Is that correct? So, a times essentially - the log (1 – t), and b times - the log (1 - t √ q)—yeah, that is right. So, I expanded the negative logarithm and then wrote it again in closed form. So, this means that the RHS converges for any complex T . If the norm of t < √ q raised to the power of – 1/2. So, as long as you take t to be less than 1 √ q , you can see that both of these summands converge, and thus the logarithm of 1 L(t) will also converge.

This is done only to rule out the poles of the L function. So, this means that the poles are outside this range. No, it's not 1 / √ q; that is the logarithm of 1 divided by 1 -. No, no, no, this is the expression.

This is already a tion, isn't it? 1/2. Yes, q is a minimum of 2. So, it is less than 1/ √2 . So, that is important. From this, we learn that the zeros of L are indeed greater than or equal to this, because they would be in the magnetic norm. Because if the norm of the zeros of L(t) < 1/ √q , then you can choose that value for t since L(t) vanishes. So, the LHS becomes divergent, correct? So, we have learned about the zeros of L(t), which means that we have learned about the inverse of α.

Sir, can I repeat that answer as greater than 1 / √ q? When t is small. So, if the LHS is diverging, it means that t is large. No, the 0s of L indicate that when LT is 0, the LHS diverges. It is 1 / 0, which equals ∞.



– **Proposition:** TFAE:

(i) RH for $Z(t,c)$. [i.e. $|\alpha| = q^{1/2}$.]

(ii) $|N_d - (q^d+1)| \leq A + B \cdot q^{d/2}$,
for some constants $A, B, N \in \mathbb{N}$ & all multiples d of N. ↖(independent of d)

Proof: • (i) ⇒ (ii): We've proved already ($\forall d$).

• (ii) ⇒ (i): • Replace the base field $\mathbb{F}_q$ by $\mathbb{F}_{q^N}$.
⇒ $\mathbb{F}_{q^N} \subseteq \mathbb{F}_{q^d}$, as we vary d.

• Hypothesis-(ii) ⇒ $\left| \sum_{i \in [2g]} \alpha_i^d \right| \leq A + B q^{d/2}$, $\forall d \equiv_N 0$.

• We've $\prod_{i=1}^{2g} \alpha_i = \prod_{i=1}^{g} (\alpha_i \cdot \alpha_{i+g}) = q^g$ (by symmetry)

So, the logarithm of it will become the logarithm of ∞. So, this is now informing you about α i $^{-1}$. So, that is greater than or equal to 1/√q which means that α_i < = √q . This implies that for all i from 1 to n , the norm is exactly √q . Thus, this completes the proof of the Riemann Hypothesis for Z(t, c) .

That is a very interesting reduction of the Riemann Hypothesis. Yeah, so actually I did not need fq'; it is built-in. It becomes ingrained because there are multiple beginnings all the time. So, no, I think I need to change this; there is a problem. So, d > = 1.

Yeah, no α is fixed; they are coming from ZTC. Yes, that is not a problem. I think the problem is that this sum exceeds all of these. But the estimate I have is only for multiples of n. How should I handle that? Yes, Q ‘; that's Q ‘.

Yeah, so what should I change about this? Somewhere, I need to make a change. Oh. I see. So then I have to change everything except for q ‘.

This will be q ‘ to the g. Where α_i are the roots. They come from L.T. Comma C, which I believe we are now calling L.T. So, for this ID, when I sum up, I can go over all of these, and when I do, I review all of them, and this Q has to be Q ‘.

This is Q ‘. Yes, that is easy. The hypothesis is that d is a multiple of n, so you can think of q' as an arbitrary d', where d' includes all integers and all natural numbers, and replace q with q'. Yeah, so α, no, this was only a statement about the count; there is no α here. Yes, but when you change the base, α i will become α i to the power of n. So, it will become α i to the power of n x d ‘.

So, yes, that part is actually implicit, and for those, you will have q raised to ng. I think we are using the fact that in a base change, α e becomes α e^n , as we showed in the previous proof. This has to be placed here. Well, if you want, we can change α i to α i ‘ to avoid confusion.

So, α i ‘ is actually α i to the n. Yes, let's do it properly. Now I can use it. So, sigma α e ‘ to the d < = a + b $q^{‘d / 2}$, simply because it is a multiple of n that is now embedded there. This was a typo that requires this kind of notation, actually. So, what did we learn from this? So, this means that RH for ZTC holds true. So, we are actually using the first reduction. So we first prove it for the changed base, and then from there we move to the original curve C.

Yes, that's great. So now you see why we actually need multiples of n. If you miss a multiple, then this argument may run into trouble because what we are really doing is first changing the base to Q raised to n. Therefore, we should have an estimate for all multiples of n. Then, it is actually equivalent. So, the next step we need to take is to make the cover.

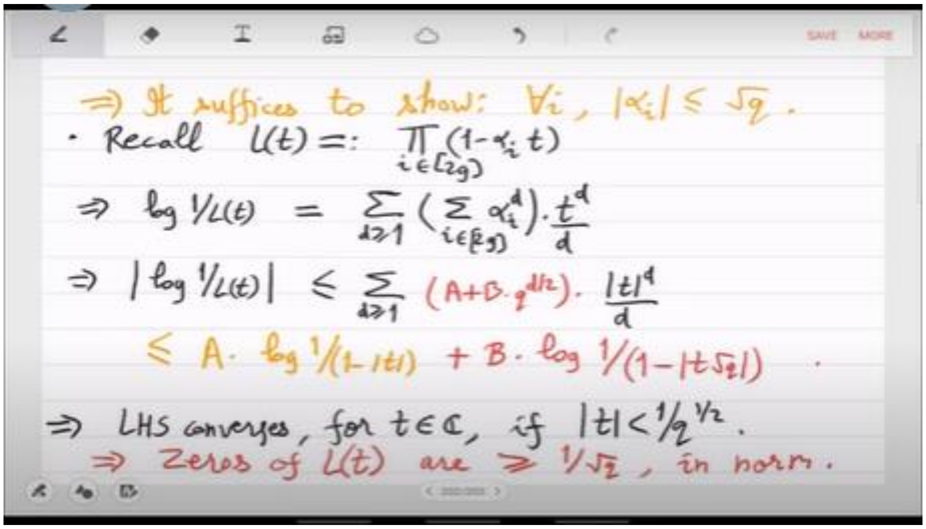
Every smooth projective curve we have seen can be viewed as a cover of the projective line. However, this is not the best cover because, at the level of fields, we have k(x_1, x_2) , and the curve is defined by some equation. It contains kx1. So, there is an arrow from the curve to the line, and there is an arrow from the function field k(x_1) to the function field of the curve, corresponding to its opposite arrow. Which means that the arrow is essentially contained within the larger field.

The problem is that the field extension we are looking at may not be Galois. So it is a finite algebraic extension, but it would be better if we made it Galois. So we make it Galois, and then we study the Riemann hypothesis only in that context. Yes, in a Galois extension, all the roots are present. If you think of x1 as fixed, then all the x2s should be available.

So, what is happening right now is that for an x1, only one x2 may be available. So, we will examine this in more dηil through an example. So we want to make it Galois; that is the one-word reduction. That is, we want this Kc; we want Kc to have all the roots for x². The function field of this extension may not have all the roots of x^2 ; we want to provide all the roots.

Sorry. x² or capital F. Yes, when I refer to roots, I mean x² for F. Yes. We cannot talk about both variables together because the transcendence degree is 1. So, we cannot say, "I want all x1," because x1 is infinite. x1 takes values from k-bar. I do not want to talk about x1; let us consider x1 as something fixed.

We are properly examining the function field k(x1), which is the function field of the projective line. So, above it now, there are only a few x2s. Out of those few x2s, we currently have only one.



$\Rightarrow$ It suffices to show: $\forall i$, $|\alpha_i| \leq \sqrt{q}$.

• Recall $L(t) =: \prod_{i \in [2g]} (1 - \alpha_i t)$

$$\Rightarrow \log 1/L(t) = \sum_{d \geq 1} \Big(\sum_{i \in [2g]} \alpha_i^d \Big) \cdot \frac{t^d}{d}$$

$$\Rightarrow |\log 1/L(t)| \leq \sum_{d \geq 1} (A + B \cdot q^{d/2}) \cdot \frac{|t|^d}{d}$$

$$\leq A \cdot \log 1/(1-|t|) + B \cdot \log 1/(1 - |t\sqrt{q}|) .$$

$\Rightarrow$ LHS converges, for $t \in \mathbb{C}$, if $|t| < 1/q^{1/2}$.

$\Rightarrow$ Zeros of $L(t)$ are $\geq 1/\sqrt{q}$, in norm.

I want all of them. So I have to go to a larger location. And that is called a Galois cover of the line. So, you want K_c to have all the roots of f with respect to x_2 while considering x_1 as fixed. So, that is the rough intuition: x1 is fixed on the projective line, and I want all the x2s for a fixed x1. So that is the move to the Galois cover. FQ, all the roots of FQ of x, and FQ to the power of n of x—all the roots are somewhere within this capital F.

Please say that again. Again, FQ x. Yes. Now, FQ ^{n} (x), something like that. FQ to the power of.

And some more. No, no, no So, it is. Yeah, let's use this as an example. Let us first look at an example. So let C be this elliptic curve. $x^{2}{}^{3} - x^{2} - x_{1}{}^{2} = 0$ over the base field K_fq. So, I mean, it is just the affine patch; to make it smooth and projective, you have to introduce x_0 . However, when $x_0 = 1$, this is the affine patch, while $x_0= 0$ will give you the point at ∞.

So, this is an elliptic curve; it is basically $x_1^2 = x_2^3 - x_2$. So, what is the problem with the function field of this? The function field is called big K; it will be this field. So, this is a finite extension of degree 3 / $k(x_1)$, which is essentially the function field of the line. Overall, this is a degree 3 field extension. The problem is that once you fix x1, it gives you a univariate equation in x2 of degree 3.

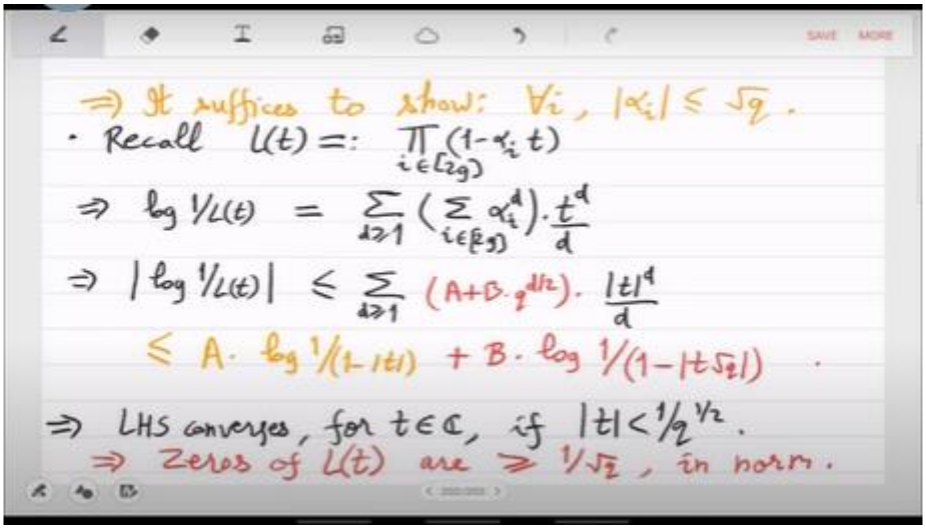
For example, $(x^2)^3 - x^2 - 1$. So, there should be three roots. Now that you have factored this polynomial, it yields only one root. The other two roots are absent. Oh, because when you randomly fix x_1 and x_2 , the polynomial $x_1^3 - x_2 - 1$ is an irreducible polynomial. So, since it is irreducible and the roots are distinct, I mean that they are all conjugate to each other.

So, when you add one root, you do not expect the other two to appear. Sometimes, like $\sqrt{}\, x^{2}$, how do you not know $x^{2} + ?\, x^{2} + x +$ one. So, when you mod out by that, in that case, you will get both roots. However, let us look at $x^3 + x + 1$. So, when you mod out by this, you go to an extension where you obtain one root, but you do not obtain the other two roots. So, you actually have to add a second root that will be of degree 3 times degree 2, resulting in a degree 6 extension; then you will obtain the splitting field.

So, here as well, you generally have to go to a degree 6 extension because the symmetric group of ψ on three elements acts as S_3. So, you have to go to degree 6, and this is only degree 3. So, how do you proceed? Essentially, we want to go beyond this. Which may not be a splitting field / k_ x_1 .

So, over $k(x_1)$, you want to find a splitting field; that is the goal. So, if you go to a splitting field, you obtain the Galois group. We correct this by moving to the splitting field k' . Of $x_2^3 - x_2 - x_1^2$ / kx_1 . So, suppress x_1 as a constant, and it becomes a univariate of degree 3.

Generally, its splitting field will actually have degree 3 times 2 , resulting in degree 6. So, k ‘ / kx1 is three times two. So, that splitting field is now again a transcendence degree 1 field over small k. Therefore, we have expressed the theory in a general form based on a broader theory. So, this is a curve again. Right, because our smooth projective curves are always actually just transverse degree 1 fields, there is a one-to-one correspondence.



$\Rightarrow$ It suffices to show: $\forall i,\ |\alpha_i| \leq \sqrt{q}$.

- Recall $L(t) =: \prod_{i \in [2g]} (1 - \alpha_i t)$

$$\Rightarrow \log 1/L(t) = \sum_{d \geq 1} \Big(\sum_{i \in [2g]} \alpha_i^d \Big) \cdot \frac{t^d}{d}$$

$$\Rightarrow \left| \log 1/L(t) \right| \leq \sum_{d \geq 1} (A + B \cdot q^{d/2}) \cdot \frac{|t|^d}{d}$$

$$\leq A \cdot \log 1/(1-|t|) + B \cdot \log 1/(1-|t\sqrt{q}|) .$$

$\Rightarrow$ LHS converges, for $t \in \mathbb{C}$, if $|t| < 1/q^{1/2}$.

$\Rightarrow$ Zeros of $L(t)$ are $\geq 1/\sqrt{q}$, in norm.

So, we can talk about a curve again; let us call it C ‘. So, C ‘ is a Galois cover of C and the projective line. So, that would be the next reduction, which is of a more fundamental type; it is more geometric. So k' contains k , which contains kx_1 , which contains k , = fq . This is degree 3, and this is degree 2, because you already have one root.

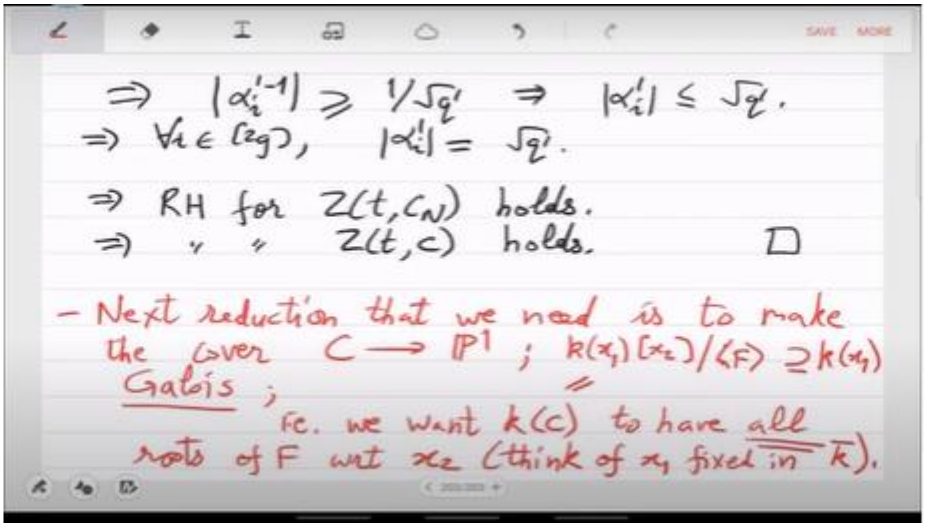
The remaining part is only quadratic; you attach another root, and you get all three roots. So that would be the price to pay. And k' / k is Galois. That is, they are. Yes, I do not want to. No, I don't think I should make this statement.

"Not k times 1 , but is k ‘ over a Galois extension of k ?" Not really correct. It does split, yes, but it only splits a single polynomial. The problem is that the √ x1 may not be present. Yes, that is correct. Yes, I think that is the Galois extension of f .

The function we are using here, which you can call f(x_1, x_2) , is not the problem, I believe. For a Galois extension, don't you need the property that if a polynomial has a root, it must have all its roots? Yes, but a normal and separable extension is called a Galois extension. So, will that property be valid? I think this needs to be checked. If it has one root, then it should have all the other roots.

I think, okay, then I can go back. For now, I can assert that both are Galois. That means they are separable and normal. So, these are the extra properties that are not very important for our Riemann hypothesis proof, but for the proof, you only need this k' that splits the single polynomial f . However, I believe you can also deduce these Galois extension properties. So, returning to the curve, we now have a new curve, which is the curve.

Defined by K ‘, it is a transcendence degree 1 field over small k. This also defines a curve, which is the curve C ‘. This C ‘ arrow C arrow P1 is called the Galois cover of C. Yes, what it is doing—I will discuss this again on Friday—but what it is doing is that on the projective line, if you take a point that fixes x1, then you get 3 x2s, or 3 points in C. Therefore, there are 3 points in C that map to the same point on the line; they are opening up more. So, now when you go to C ‘, C ‘ has two points that map to the same point in C.



$\Rightarrow \quad |\alpha_i'^{-1}| \geqslant 1/\sqrt{q'} \quad \Rightarrow \quad |\alpha_i'| \leq \sqrt{q'}$.

$\Rightarrow \quad \forall i \in [2g], \quad |\alpha_i'| = \sqrt{q'}$.

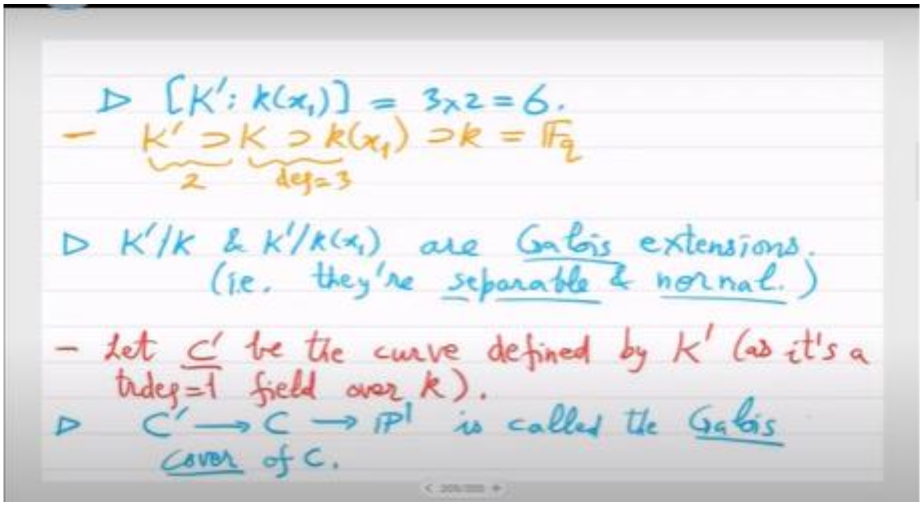
$\Rightarrow$ RH for $Z(t, C_N)$ holds.

$\Rightarrow$ " " $Z(t, C)$ holds. $\square$

- Next reduction that we need is to make the cover $C \longrightarrow \mathbb{P}^1$; $\underset{\shortparallel}{k(x_1)[x_2]/\langle F\rangle} \supseteq k(x_1)$ <u>Galois</u> ; ie. we want $k(C)$ to have <u>all</u> roots of F wrt x_2 (think of x_1 fixed in $\overline{k}$).

No, not exactly; we are not in algebraic closure, so we are in k = f^3 . So, actually, when you fix x2, there is a corresponding point in C. We do not know how many there are; there may be only one point, and that one point will now lead to three.

So, 3 is mapped to 1, and 1 is mapped to 1. This is a generic image. Yes, but those are exceptions. So, we will show that there are very few in number. The generic situation is that 3 maps to 1, which in turn maps to 1. Since we were only getting one point in C, we had to move to a larger curve, which is the Halwa cover. There, we will get all three items. Usually, for standard x2s or x1s, we will get three. Yes, so we will return to this point next.



▷ $[K' : k(x_1)] = 3 \times 2 = 6$.

– $\underbrace{K' \supset K}_{2} \supset \underbrace{ k(x_1)}_{\deg = 3} \supset k = \mathbb{F}_q$

▷ K'/K & $K'/k(x_1)$ are <u>Galois</u> extensions.
(i.e. they're <u>separable</u> & <u>normal</u>.)

– let <u>C'</u> be the curve defined by K' (as it's a trdeg $= 1$ field over k).

▷ $C' \longrightarrow C \longrightarrow \mathbb{P}^1$ is called the <u>Galois cover</u> of C.