Math 7359 (Elliptic Curves and Modular Forms)

Lecture #16 of 24 $\sim$ November 2, 2023

The Hasse Bound and the Weil Conjectures + Tate Modules

- Discussion of the Hasse Bound
- The Weil Conjectures
- The Tate Module

Recall, I

Recall first our results on the m-torsion subgroup of an elliptic curve.

Theorem (The m-Torsion Subgroup)

Let m be a nonzero integer and E be an elliptic curve over k.

9. *If $\mathrm{char}(k)$ does not divide m then the m-torsion subgroup $E[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.*
10. *If $\mathrm{char}(k) = p$, then either $E[p^d] = \{O\}$ for all $d \geq 1$, or $E[p^d]$ is isomorphic to $\mathbb{Z}/p^d\mathbb{Z}$ for all $d \geq 1$.*

Hasse Bound Discussion, I

Recall also our proof of the Hasse bound last time:

Theorem (Points on Elliptic Curves over $\mathbb{F}_q$)

Let $q = p^d$ be a prime power and let $E/\mathbb{F}_q$ be an elliptic curve defined over $\mathbb{F}_q$.

1. *The degree map* $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ *is a positive-definite quadratic form.*
2. *The Frobenius map $\varphi = \mathrm{Frob}_q$ has the property that $1 - \varphi$ is separable.*
3. *(Hasse Bound) The number of points on $E(\mathbb{F}_q)$ satisfies $|\#E(\mathbb{F}_q) - q - 1| \le 2\sqrt{q}$.*

Hasse Bound Discussion, I

Recall also our proof of the Hasse bound last time:

Theorem (Points on Elliptic Curves over $\mathbb{F}_q$)

Let $q = p^d$ be a prime power and let $E/\mathbb{F}_q$ be an elliptic curve defined over $\mathbb{F}_q$.

1. *The degree map $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive-definite quadratic form.*
2. *The Frobenius map $\varphi = \mathrm{Frob}_q$ has the property that $1 - \varphi$ is separable.*
3. *(Hasse Bound) The number of points on $E(\mathbb{F}_q)$ satisfies $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$.*

Exercise: Verify the Hasse bound for $E : y^2 = x^3 + 4x + 1$ over $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{11}$, and $\mathbb{F}_{13}$ (optionally, also over $\mathbb{F}_9$, $\mathbb{F}_{25}$, and $\mathbb{F}_{27}$).

Hasse Bound Discussion, II

We can give some intuition for why we might expect an inequality like the Hasse bound to hold.

- Assuming characteristic not equal to 2 for simplicity, consider a Weierstrass equation $y^2 = p(x)$ for E.

Hasse Bound Discussion, II

We can give some intuition for why we might expect an inequality like the Hasse bound to hold.

- Assuming characteristic not equal to 2 for simplicity, consider a Weierstrass equation $y^2 = p(x)$ for E.
- For each of the q possible finite values of x, there are either 2, 1, or 0 possible values of y, according to whether x is a nonzero square, zero, or a nonsquare.
- Since the squaring map $x \mapsto x^2$ is a homomorphism with kernel $\{\pm 1\}$ in $\mathbb{F}_q$, there are $(q-1)/2$ nonzero squares and $(q-1)/2$ nonsquares, so the expected number of values of y for any given x is equal to 1.
- Since there are q possible x, the expected number of finite points (x, y) is q, so together with the point at ∞, this gives an expected $q + 1$ points on $E(\mathbb{F}_q)$.

Hasse Bound Discussion, III

We can also recast the Hasse bound in terms of a character sum.

- Explicitly, let χ denote the quadratic character on $\mathbb{F}_q$ (it is 0 on 0, 1 on squares, and -1 on nonsquares), and let E have a Weierstrass equation $y^2 = x^3 + Ax + B$.

Hasse Bound Discussion, III

We can also recast the Hasse bound in terms of a character sum.

- Explicitly, let χ denote the quadratic character on $\mathbb{F}_q$ (it is 0 on 0, 1 on squares, and -1 on nonsquares), and let E have a Weierstrass equation $y^2 = x^3 + Ax + B$.
- Then since the number of solutions to $y^2 = c$ is $1 + \chi(c)$, summing over the possible values of x shows that $\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \chi(x^3 + Ax + B)$.
- The Hasse bound then represents the improvement on the character sum estimate $|\sum_{x \in \mathbb{F}_q} \chi(x^3 + Ax + B)|$ from the trivial bound q to the asymptotically far better $2\sqrt{q}$.
- This kind "square-root cancellation" as it is known to analytic number theorists is a fairly typical strong estimate on character sums of this type.

We can also give some statistical motivation for why this estimate on the deviation is somewhat reasonable.

Hasse Bound Discussion, IV

Exercise: Suppose X is the sum of q Bernoulli random variables each of which takes the values 0 and 2 each with probability 1/2. Show that the standard deviation of X is $\sqrt{q}$.

- If we approximate the point-count on E as the sum of q independent coin flips each of which yields 0 or 2 points, then by the exercise above, the standard deviation in the total number of points would be $\sqrt{q}$.
- The Hasse bound thus says our count will always be within 2 standard deviations of its mean $q+1$.
- Of course, this is only a heuristic, since the actual variables themselves are not independent, but it's useful for seeing why the results come out near $\sqrt{q}$.

Zeta Functions, I

Perhaps surprisingly, the error estimate in the Hasse bound is actually tied to much deeper results related to the Riemann hypothesis for algebraic varieties, via the Weil conjectures.

- To explain how, we first define the zeta function of a variety.

Definition

Let q be a prime power and V be a smooth projective variety defined over the field $\mathbb{F}_q$. For each $n \geq 1$, define $a_n = \#V(\mathbb{F}_{q^n})$ to be the number of points of V that lie in the extension field $\mathbb{F}_{q^n}$.

Then the zeta function of V is defined to be the power series

$$\zeta_V(T) = \exp\left[\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right].$$

Zeta Functions, II

Note $\zeta_V(T) = \exp\left[\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right]$ for $a_n = \#V(\mathbb{F}_{q^n})$.

<u>Example</u>: Find the zeta function for $V = \mathbb{P}^1$.

Zeta Functions, II

Note $\zeta_V(T) = \exp\left[\sum_{n=1}^{\infty} a_n \frac{T^n}{n}\right]$ for $a_n = \#V(\mathbb{F}_{q^n})$.

Example: Find the zeta function for $V = \mathbb{P}^1$.

- We have $a_n = q^n + 1$ for each n.
- Thus $\zeta_{\mathbb{P}^1}(T) = \exp(\sum_{n=1}^{\infty} \frac{(qT)^n}{n} + \sum_{n=1}^{\infty} \frac{T^n}{n}) =$ $\exp(-\ln(1-qT) - \ln(1-T)) = \dfrac{1}{(1-qT)(1-T)}$ using the usual series expansion $-\ln(1-T) = \sum_{n=1}^{\infty} \frac{T^n}{n}$.

Zeta Functions, III

Exercise: Find $\zeta_V(T)$ for $V = \mathbb{P}^n$ and for $\mathbb{P}^1 \times \mathbb{P}^1$.

It is not especially clear from this definition why exactly we call

$\zeta_V(T) = \exp\left[\sum_{n=1}^{\infty} \#V(\mathbb{F}_{q^n}) \frac{T^n}{n}\right]$ the the zeta function of V.

Some obvious questions:

Zeta Functions, III

Exercise: Find $\zeta_V(T)$ for $V = \mathbb{P}^n$ and for $\mathbb{P}^1 \times \mathbb{P}^1$.

It is not especially clear from this definition why exactly we call

$\zeta_V(T) = \exp\left[\sum_{n=1}^{\infty} \#V(\mathbb{F}_{q^n})\frac{T^n}{n}\right]$ the the zeta function of V.

Some obvious questions:

- Why does it have an exponential in it?
- What does it have to do with other zeta functions?
- Why divide by n instead of just using $\sum a_n T^n$ like in a normal generating function?

Zeta Functions, IV

Let me try to explain why this actually deserves to be called a zeta function using some motivation for when $V = C$ is a curve:

Proposition (Sum Formula for Zeta Function)

Suppose C is a smooth projective curve defined over $\mathbb{F}_q$ and let b_n be the number of effective divisors $D \geq 0$ of degree n in the divisor group $\mathrm{Div}_{\mathbb{F}_q}(C)$.

Then the zeta function $\zeta_C(T)$ equals $\sum_{n=0}^{\infty} b_n T^n$.

Zeta Functions, IV

Let me try to explain why this actually deserves to be called a zeta function using some motivation for when $V = C$ is a curve:

Proposition (Sum Formula for Zeta Function)

Suppose C is a smooth projective curve defined over $\mathbb{F}_q$ and let b_n be the number of effective divisors $D \geq 0$ of degree n in the divisor group $\mathrm{Div}_{\mathbb{F}_q}(C)$.

Then the zeta function $\zeta_C(T)$ equals $\sum_{n=0}^{\infty} b_n T^n$.

Recall some facts about divisors defined over $\mathbb{F}_q$:

- The degree of a point $P \in C(\overline{\mathbb{F}_q})$ is defined to be the degree of the field extension $\mathbb{F}_q(P)/\mathbb{F}_q$.
- The divisor over $\mathbb{F}_q$ associated to a point P is the sum $\mathrm{div}(P) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}_q(P)/\mathbb{F}_q)} \sigma(P)$, which has degree $\deg(P)$.

Zeta Functions, V

Proposition: $\zeta_C(T)$ equals $\sum_{n=0}^{\infty} b_n T^n$ where b_n is the number of effective divisors of degree n in $\mathrm{Div}_{\mathbb{F}_q}(C)$.

Proof (part 1):

Zeta Functions, V

Proposition: $\zeta_C(T)$ equals $\sum_{n=0}^{\infty} b_n T^n$ where b_n is the number of effective divisors of degree n in $\mathrm{Div}_{\mathbb{F}_q}(C)$.

Proof (part 1):

- Note that any effective divisor $D \geq 0$ in $\mathrm{Div}_{\mathbb{F}_q}(C)$ is of the form $\sum_{P \in C(\overline{\mathbb{F}_q})} n_P \mathrm{div}(P)$ for nonnegative integers n_P, and the degree of this divisor is $\sum_{P \in C(\overline{\mathbb{F}_q})} n_P \deg(P)$.
- So by the usual properties of generating functions, we have $\sum_{n=0}^{\infty} b_n T^n = \prod_{P \in C(\overline{\mathbb{F}_q})} (1 + T^{\deg P} + T^{2\deg P} + \cdots)$ $= \prod_{P \in C(\overline{\mathbb{F}_q})} (1 - T^{\deg P})^{-1}$ as a formal power series.
- Why? Formally multiply out the middle product. Each divisor $\sum_{P \in C(\overline{\mathbb{F}_q})} n_P \mathrm{div}(P)$ of total degree n yields one term T^n.

Zeta Functions, VI

Proof (part 2):

- So we have $\sum_{n=0}^{\infty} b_n T^n = \prod_{P \in C(\overline{\mathbb{F}_q})} (1 - T^{\deg P})^{-1}$.

Zeta Functions, VI

Proof (part 2):

- So we have $\sum_{n=0}^{\infty} b_n T^n = \prod_{P \in C(\overline{\mathbb{F}_q})} (1 - T^{\deg P})^{-1}$.
- Then $\ln[\sum_{n=0}^{\infty} b_n T^n] = -\sum_{P \in C(\overline{\mathbb{F}_q})} \ln(1 - T^{\deg P})$ $= \sum_{P \in C(\overline{\mathbb{F}_q})} \sum_{k=1}^{\infty} \frac{T^{k \deg P}}{k}$, whose coefficient of T^n is the sum $\sum_{P \in C(\overline{\mathbb{F}_q})\,:\,k \deg(P) = n} \frac{1}{k} = \sum_{P \in C(\overline{\mathbb{F}_q})\,:\,\deg(P) | n} \frac{\deg(P)}{n}$.

Zeta Functions, VI

Proof (part 2):

- So we have $\sum_{n=0}^{\infty} b_n T^n = \prod_{P \in C(\overline{\mathbb{F}_q})} (1 - T^{\deg P})^{-1}$.
- Then $\ln[\sum_{n=0}^{\infty} b_n T^n] = -\sum_{P \in C(\overline{\mathbb{F}_q})} \ln(1 - T^{\deg P})$ $= \sum_{P \in C(\overline{\mathbb{F}_q})} \sum_{k=1}^{\infty} \frac{T^{k \deg P}}{k}$, whose coefficient of T^n is the sum $\sum_{P \in C(\overline{\mathbb{F}_q})\,:\,k \deg(P) = n} \frac{1}{k} = \sum_{P \in C(\overline{\mathbb{F}_q})\,:\,\deg(P) | n} \frac{\deg(P)}{n}$.
- When we "glue" all of the $\deg(P)$ Galois-conjugate points $\sigma(P)$ together, this evaluates to $\frac{1}{n} \#\{P \in C(\overline{\mathbb{F}_q}) \ : \ \deg(P) | n\} = \frac{1}{n} \# C(\mathbb{F}_{q^n}) = \frac{a_n}{n}$, where the first equality follows from the fact that an element of $\overline{\mathbb{F}_q}$ lies in $\mathbb{F}_{q^n}$ if and only if its degree divides n.
- Thus, $\ln(\sum_{n=0}^{\infty} b_n T^n) = \sum_{n=0}^{\infty} a_n \frac{T^n}{n}$. Exponentiate.

Zeta Functions, VII

Now we can explain the analogy for why the zeta function is called a zeta function.

- From the sum formula, we have $\zeta_V(T) = \sum_{n=0}^{\infty} b_n T^n = \sum_{D \geq 0} T^{\deg(D)} = \sum_{D \geq 0} \dfrac{1}{N(D)^s}$ where $N(D) = q^{-\deg(D)}$ and $T = q^{-s}$.
- This latter expression is the analogue of the Riemann zeta function's definition $\zeta(s) = \sum_{n \geq 1} \dfrac{1}{n^s}$.

Zeta Functions, VII

Now we can explain the analogy for why the zeta function is called a zeta function.

- From the sum formula, we have $\zeta_V(T) = \sum_{n=0}^{\infty} b_n T^n = \sum_{D \geq 0} T^{\deg(D)} = \sum_{D \geq 0} \dfrac{1}{N(D)^s}$ where $N(D) = q^{-\deg(D)}$ and $T = q^{-s}$.
- This latter expression is the analogue of the Riemann zeta function's definition $\zeta(s) = \sum_{n \geq 1} \dfrac{1}{n^s}$.

The idea is that effective divisors on C are the natural analogue of the positive integers, and that the norm function $N(D)$ gives the proper "size" of a divisor.

- Also, the points in $C(\overline{\mathbb{F}_q})$ are the analogues of the primes showing up in the Euler product $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$, analogous to the Euler product $\zeta_C(T) = \prod_P (1 - q^{-s \deg P})^{-1}$ worked out in the proposition.

The Weil Conjectures, I

Theorem (Weil Conjectures)

Let V be a smooth projective variety of dimension n defined over $\mathbb{F}_q$ with associated zeta function $\zeta_C(T)$. Then:

1. *(Rationality) $\zeta_C(T)$ is a rational function of T. Specifically, $\zeta_C(T) = \prod_{i=0}^{2n} p_i(T)^{(-1)^{i+1}} = \dfrac{p_1(T)p_3(T)\cdots p_{2n-1}(T)}{p_0(T)p_2(T)\cdots p_{2n}(T)}$ for appropriate polynomials $p_i(T) \in 1 + T\mathbb{Z}[T]$, where $p_0(T) = 1 - T$, $p_{2n}(T) = 1 - q^n T$, and $p_i(T) = \prod_j (1 - \alpha_{i,j} T)$ for some $\alpha_{i,j} \in \mathbb{C}$.*
2. *(Functional Equation / Poincaré Duality) The zeta function has a functional equation $\zeta_C(q^{-n}T^{-1}) = \pm q^{nE/2} T^E \zeta_C(T)$, where $E = 2 - 2g$ is the Euler characteristic of V. In particular, the map $\alpha \mapsto q^n/\alpha$ maps the zeroes of p_i to the zeroes of p_{2n-i}.*

The Weil Conjectures, II

Theorem (Weil Conjectures, Continued)

Let V be a smooth projective variety of dimension n defined over $\mathbb{F}_q$ with associated zeta function $\zeta_C(T)$. Then:

3. *(Riemann Hypothesis) With* $\zeta_C(T) = \prod_{i=0}^{2n} p_i(T)^{(-1)^{i+1}} = \dfrac{p_1(T)p_3(T)\cdots p_{2n-1}(T)}{p_0(T)p_2(T)\cdots p_{2n}(T)}$, *for each i, j, the inverse zeroes $\alpha_{i,j}$ of p_i have $|\alpha_{i,j}| = q^{i/2}$. Equivalently, with $T = q^{-s}$, all of the zeroes of $p_k(T)$ lie on the line $\mathrm{Re}(s) = k/2$.*
4. *(Betti Numbers) If V is the reduction modulo $\tilde{p} = \mathrm{char}(\mathbb{F}_q)$ of a smooth variety X defined over an algebraic number field, then the degree of p_i is the ith Betti number of the space $X(\mathbb{C})$ of complex points on X.*

The Weil Conjectures, III

The Weil conjectures have a long history. Here is a brief summary of some of it:

- In the early 1800s, Gauss identified some components of these general results in particular examples for certain curves, in the context of counting points on elliptic curves modulo p.
- In 1924, Artin conjectured the general results for curves and Hasse independently proved the results for elliptic curves.
- In 1949, Weil formulated the general statement of the Weil conjectures (he had previously established Artin's conjectured statements in the case of curves).
- Establishing the Weil conjectures in full took the development of about 20 more years of algebraic geometry machinery: Dwork proved (1) in 1960, while Grothendieck proved (1), (2), and (4) in the 1960s, and Deligne finished (3) in 1973.

The Weil Conjectures, IV

In the specific case $n = 1$ (i.e., for curves), the Weil conjectures read as follows:

1. $\zeta_C(T) = \dfrac{L_C(T)}{(1-T)(1-qT)}$ for some polynomial $L_C(T) = \prod_j (1 - \alpha_j T)$.
2. For $\xi_C(T) = T^{g-1}\zeta_C(T)$, we have $\xi_C(q^{-1}T^{-1}) = \xi_C(T)$.
3. The roots of L_C all have $|\alpha_j| = q^{-1/2}$.
4. The degree of L_C is $2g$.

The Weil Conjectures, IV

In the specific case $n = 1$ (i.e., for curves), the Weil conjectures read as follows:

1. $\zeta_C(T) = \dfrac{L_C(T)}{(1-T)(1-qT)}$ for some polynomial $L_C(T) = \prod_j (1 - \alpha_j T)$.
2. For $\xi_C(T) = T^{g-1}\zeta_C(T)$, we have $\xi_C(q^{-1}T^{-1}) = \xi_C(T)$.
3. The roots of L_C all have $|\alpha_j| = q^{-1/2}$.
4. The degree of L_C is $2g$.

Exercise: Verify the Weil conjectures for $C = \mathbb{P}^1$.

Exercise: Show that for elliptic curves, the Weil conjectures are equivalent to the statement that $\zeta_C(T) = \dfrac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$ where α and β are complex conjugates of absolute value $\sqrt{q}$.

The Weil Conjectures, V

Let's unwind the statement that $\zeta_C(T) = \dfrac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$ where α and β are complex conjugates of absolute value $\sqrt{q}$.

- Suppose for the moment the statement above is true.
- Then $\ln \zeta_C(T)$ $= -\ln(1-T) - \ln(1-qT) + \ln(1-\alpha T) + \ln(1-\beta T)$ $= \sum_{n=1}^{\infty} \dfrac{1^n + q^n - \alpha^n - \beta^n}{n} T^n$, and so we have $\#E(\mathbb{F}_{q^n}) = 1 + q^n - \alpha^n - \beta^n$ for some complex conjugates α and β of absolute value $\sqrt{q}$.

The Weil Conjectures, V

Let's unwind the statement that $\zeta_C(T) = \dfrac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}$ where α and β are complex conjugates of absolute value $\sqrt{q}$.

- Suppose for the moment the statement above is true.
- Then $\ln \zeta_C(T)$ $= -\ln(1-T) - \ln(1-qT) + \ln(1-\alpha T) + \ln(1-\beta T)$ $= \sum_{n=1}^{\infty} \dfrac{1^n + q^n - \alpha^n - \beta^n}{n} T^n$, and so we have $\#E(\mathbb{F}_{q^n}) = 1 + q^n - \alpha^n - \beta^n$ for some complex conjugates α and β of absolute value $\sqrt{q}$.
- Notice that when $n = 1$, this says $\#E(\mathbb{F}_q) = 1 + q - \alpha - \beta$ where α and β are complex conjugates of absolute value $\sqrt{q}$, meaning that $|\#E(\mathbb{F}_q) - q - 1| = 2|\mathrm{Re}(\alpha)| \leq 2\sqrt{q}$: precisely the statement of the Hasse bound!

The Weil Conjectures, VI

So, how could we try to prove the Weil conjectures? As with the proof of the Hasse bound, we need to convert things to a statement about the qth-power Frobenius map φ.

The Weil Conjectures, VI

So, how could we try to prove the Weil conjectures? As with the proof of the Hasse bound, we need to convert things to a statement about the qth-power Frobenius map φ.

- First, we observe that $P \in \overline{\mathbb{F}_q}$ lies in $\mathbb{F}_{q^n}$ if and only if P is fixed by φ^n if and only if $P \in \ker(1 - \varphi^n)$.
- Thus, $\#E(\mathbb{F}_{q^n}) = \#\ker(1 - \varphi^n) = \deg(1 - \varphi^n)$ since $1 - \varphi^n$ is separable by the same argument used in (2) of the Hasse bound proof.
- From properties of duals, we have $[\deg(1 - \varphi^n)] = (\widehat{1 - \varphi^n}) \circ (1 - \varphi^n) = (1 - \hat{\varphi}^n) \circ (1 - \varphi^n)$ $= [1] - \varphi^n - \hat{\varphi}^n + \hat{\varphi}^n \circ \varphi^n = [1] - \varphi^n - \hat{\varphi}^n + [q^n]$.
- This is fairly close to the result we want: we would just need to show that $\varphi^n + \hat{\varphi}^n = [\alpha^n + \beta^n]$ where α and β are complex conjugates of absolute value $\sqrt{q}$.

The Weil Conjectures, VII

So how could we show that $\varphi^n + \hat{\varphi}^n = [\alpha^n + \beta^n]$ where α and β are complex conjugates of absolute value $\sqrt{q}$?

The Weil Conjectures, VII

So how could we show that $\varphi^n + \hat{\varphi}^n = [\alpha^n + \beta^n]$ where α and β are complex conjugates of absolute value $\sqrt{q}$? Let's play a game of "pretend these objects are things we understand better":

- Specifically, let's pretend φ is a linear transformation on a complex vector space and that $\hat{\varphi}$ is its adjoint with respect to an inner product.

The Weil Conjectures, VII

So how could we show that $\varphi^n + \hat{\varphi}^n = [\alpha^n + \beta^n]$ where α and β are complex conjugates of absolute value $\sqrt{q}$? Let's play a game of "pretend these objects are things we understand better":

- Specifically, let's pretend φ is a linear transformation on a complex vector space and that $\hat{\varphi}$ is its adjoint with respect to an inner product.
- Then the sum $\varphi^n + \hat{\varphi}^n$ would represent the trace $\mathrm{tr}(\varphi^n)$ of the linear transformation φ^n, which by basic linear algebra equals the sum of the *n*th powers of the eigenvalues of φ.
- So we would obtain a statement of the desired form if φ had exactly 2 eigenvalues (i.e., if φ were an operator on a 2-dimensional vector space) that were complex conjugates of absolute value $\sqrt{q}$.

Tate Module Preamble, I

Of course, our little game of pretend isn't remotely legitimate. But let's see if we can use the core idea to get close enough to give a real proof.

- Although φ is a linear transformation, it acts on the field $\overline{\mathbb{F}_q}$ of characteristic p.
- In order to make statements about eigenvalues that are complex numbers, we would need to have an action of φ on something in characteristic 0.

Tate Module Preamble, I

Of course, our little game of pretend isn't remotely legitimate. But let's see if we can use the core idea to get close enough to give a real proof.

- Although φ is a linear transformation, it acts on the field $\overline{\mathbb{F}_q}$ of characteristic p.
- In order to make statements about eigenvalues that are complex numbers, we would need to have an action of φ on something in characteristic 0.
- So let's now discuss how to construct an object in characteristic 0 on which φ has a natural 2-dimensional representation.

In fact, for no extra charge, we will construct this object on which Galois automorphisms (like the Frobenius map) and isogenies (like the Frobenius map) both act quite naturally.

Tate Module Preamble, II

So let E be an elliptic curve defined over the field F with algebraic closure k as usual, and let $\sigma \in G = \mathrm{Gal}(k/F)$ be any automorphism in the Galois group.

- Since E is defined over F, σ maps points of E to other points of E, and indeed σ is a group homomorphism from E to E since the addition law of points in F is defined over F as well.

Tate Module Preamble, II

So let E be an elliptic curve defined over the field F with algebraic closure k as usual, and let $\sigma \in G = \mathrm{Gal}(k/F)$ be any automorphism in the Galois group.

- Since E is defined over F, σ maps points of E to other points of E, and indeed σ is a group homomorphism from E to E since the addition law of points in F is defined over F as well.
- For any $P \in E[m]$, we have $[m]\sigma(P) = \sigma([m]P) = \sigma(O) = O$, and so G acts on $E[m]$.
- Since for any integer m not divisible by $p = \mathrm{char}(\mathbb{F}_q)$, the m-torsion subgroup $E[m]$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, this means G has a group action on $(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$, which is to say, we have a representation $G \to \mathrm{Aut}[(\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})] \cong GL_2(\mathbb{Z}/m\mathbb{Z})$.

Tate Module Preamble, III

This is a 2-dimensional representation of the Galois group, which is at least in the right direction for what we want, but we really need a representation in characteristic 0, not characteristic m.

- To do that, we can exploit the fact that we have representations for all integers m, not just individual ones.

Tate Module Preamble, III

This is a 2-dimensional representation of the Galois group, which is at least in the right direction for what we want, but we really need a representation in characteristic 0, not characteristic m.

- To do that, we can exploit the fact that we have representations for all integers m, not just individual ones.
- Since by the Chinese remainder theorem, the action of the representation is completely determined by the action on the prime-power torsion groups, it's enough to instead study the behavior on the l-power torsion subgroups $E[l^d]$ for $l \neq p$, which are isomorphic to $(\mathbb{Z}/l^d\mathbb{Z}) \times (\mathbb{Z}/l^d\mathbb{Z})$.
- We may glue the l-power torsion groups $E[l^d]$ together in a natural way using inverse limits using the fairly simple observation that if P is an l^d-torsion point, then $[l]P$ is an l^{d-1}-torsion point.

Inverse Limits, I

In order to motivate this, let's warm up with a simpler example: constructing the ring $\mathbb{Z}_l$ of l-adic integers.

- Consider the inverse system $\mathbb{Z}/l\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^2\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^3\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^4\mathbb{Z} \xleftarrow{\pi} \cdots$ of rings with projection maps $\pi : \mathbb{Z}/l^{d+1}\mathbb{Z} \to \mathbb{Z}/l^d\mathbb{Z}$ given by the natural projection (i.e., reduction modulo l^d).

Inverse Limits, I

In order to motivate this, let's warm up with a simpler example: constructing the ring $\mathbb{Z}_l$ of l-adic integers.

- Consider the inverse system $\mathbb{Z}/l\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^2\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^3\mathbb{Z} \xleftarrow{\pi} \mathbb{Z}/l^4\mathbb{Z} \xleftarrow{\pi} \cdots$ of rings with projection maps $\pi : \mathbb{Z}/l^{d+1}\mathbb{Z} \to \mathbb{Z}/l^d\mathbb{Z}$ given by the natural projection (i.e., reduction modulo l^d).
- The elements of the inverse limit $\mathbb{Z}_l$ of this system are tuples $(b_1, b_2, b_3, b_4, \dots)$ such that $\pi(b_{d+1}) = b_d$ for each d, which is to say, $b_{d+1} \equiv b_d \pmod{l^d}$.
- If we take the unique representative for each b_i with $0 \leq b_i < l^i$, then we have $b_{d+1} = b_d + a_d l^d$ for some unique integer $a_{d+1} \in \{0, 1, 2, \dots, l-1\}$.
- So we can think of the elements as infinite base-l expansions $a_0 + a_1 l + a_2 l^2 + a_3 l^3 + \cdots$ for appropriate digits $a_i \in \{0, 1, \dots, l-1\}$.

Inverse Limits, II

- Then $\mathbb{Z}_l$ is a ring via componentwise addition and multiplication since the projections π are all ring homomorphisms. (The resulting ring operations are simply that of base-l arithmetic on the resulting digits.)
- In particular, note that $\mathbb{Z}_l$ has characteristic zero.
- Indeed, $\mathbb{Z}_l$ also inherits a metric space topology (the l-adic topology) from the natural l-adic valuation $v_l(\sum a_i l^i)$ given by the minimal power i with $a_i \neq 0$. (Intuitively, two points are close together under this topology when their expansions agree for many terms.)

We also mention that there is another standard way to construct $\mathbb{Z}_l$: namely, as the completion of $\mathbb{Z}$ under the l-adic metric. (See HW4.)

Inverse Limits, III

We may use a very similar inverse limit construction on the torsion groups $E[l^d]$.

- Consider the inverse system $E[l] \overset{[l]}{\leftarrow} E[l^2] \overset{[l]}{\leftarrow} E[l^3] \overset{[l]}{\leftarrow} E[l^4] \overset{[l]}{\leftarrow} \cdots$ of groups whose elements are tuples $(P_1, P_2, P_3, P_4, \dots)$ with $P_d \in E[l^d]$ and where $[l]P_{d+1} = P_d$.

Inverse Limits, III

We may use a very similar inverse limit construction on the torsion groups $E[l^d]$.

- Consider the inverse system $E[l] \overset{[l]}{\leftarrow} E[l^2] \overset{[l]}{\leftarrow} E[l^3] \overset{[l]}{\leftarrow} E[l^4] \overset{[l]}{\leftarrow} \cdots$ of groups whose elements are tuples $(P_1, P_2, P_3, P_4, \dots)$ with $P_d \in E[l^d]$ and where $[l]P_{d+1} = P_d$.
- One may think of these tuples as being obtained by starting with the identity O and then successively choosing inverse images P_1, P_2, P_3, P_4, ... under the multiplication-by-l map.
- Since all of the maps are group homomorphisms, the set of such tuples is a group under componentwise addition: it is the inverse limit $\varprojlim_d E[l^d]$.
- Indeed, since each $E[l^d]$ is a $(\mathbb{Z}/l^d\mathbb{Z})$-module, the inverse limit actually carries a $\mathbb{Z}_l$-module structure, and hence also inherits the l-adic topology.

The Tate Module, I

The inverse limit we just constructed is called the Tate module:

Definition

Let E be an elliptic curve and l be a prime. The l-adic Tate module of E is the $\mathbb{Z}_l$-module $T_l(E) = \varprojlim_d E[l^d]$.

To emphasize, the elements of the Tate module consist of sequences of points $(P_1, P_2, P_3, P_4, \dots)$ such that $lP_{d+1} = P_d$ for each $d \geq 0$, where we think of $P_0 = O$.

The Tate Module, I

The inverse limit we just constructed is called the Tate module:

Definition

Let E be an elliptic curve and l be a prime. The l-adic Tate module of E is the $\mathbb{Z}_l$-module $T_l(E) = \varprojlim_d E[l^d]$.

To emphasize, the elements of the Tate module consist of sequences of points $(P_1, P_2, P_3, P_4, \dots)$ such that $lP_{d+1} = P_d$ for each $d \geq 0$, where we think of $P_0 = O$.

- When $l \neq \mathrm{char}(k)$, when we apply the inverse limit construction starting with generators P and Q of $E[l]$, we obtain topological generators for $T_l(E)$ yielding a group isomorphism $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$.
- When $l = \mathrm{char}(k)$ we instead have $T_l(E) \cong \mathbb{Z}_l$ or 0, according to whether $E[l^d] \cong \mathbb{Z}/l^d\mathbb{Z}$ or 0, respectively.

The Tate Module, II

Now, returning to our discussion, if E is defined over F and $\sigma \in \mathrm{Gal}(k/F)$, then σ acts naturally on the Tate module via $\sigma(P_1, P_2, P_3, \dots) = (\sigma P_1, \sigma P_2, \sigma P_3, \dots)$

The Tate Module, II

Now, returning to our discussion, if E is defined over F and $\sigma \in \mathrm{Gal}(k/F)$, then σ acts naturally on the Tate module via $\sigma(P_1, P_2, P_3, \dots) = (\sigma P_1, \sigma P_2, \sigma P_3, \dots)$

- Since this action is clearly a group action, it yields a representation of $\mathrm{Gal}(k/F)$ on $\mathrm{Aut}[T_l(E)]$.
- In fact, since the Galois group acts continuously on each component $E[l^d]$ of the inverse limit (rather trivially, since it is a profinite group and they are all discrete groups), the Galois action is also continuous.

The Tate Module, III

Definition

Let E be an elliptic curve defined over the field F with algebraic closure k, and let $l \neq \mathrm{char}(k)$ be a prime.

The l-adic Galois representation associated to E is the map $\rho_l : \mathrm{Gal}(k/F) \to \mathrm{Aut}[T_l(E)]$ defined by $\rho_l(\sigma)(P_1, P_2, P_3, \dots) = (\sigma P_1, \sigma P_2, \sigma P_3, \dots)$.

The Tate Module, III

Definition

Let E be an elliptic curve defined over the field F with algebraic closure k, and let $l \neq \mathrm{char}(k)$ be a prime.

The l-adic Galois representation associated to E is the map $\rho_l : \mathrm{Gal}(k/F) \to \mathrm{Aut}[T_l(E)]$ defined by $\rho_l(\sigma)(P_1, P_2, P_3, \dots) = (\sigma P_1, \sigma P_2, \sigma P_3, \dots)$.

- Since $l \neq \mathrm{char}(k)$ we know that $T_l(E)$ is isomorphic to $\mathbb{Z}_l \times \mathbb{Z}_l$, so $\mathrm{Aut}[T_l(E)]$ is isomorphic to $\mathrm{Aut}(\mathbb{Z}_l \times \mathbb{Z}_l) \cong GL_2(\mathbb{Z}_l)$.
- Now, $\mathbb{Z}_l$ is not a field, but it is an integral domain, so it embeds in its field of fractions $\mathbb{Q}_l = \mathbb{Z}_l[l^{-1}]$, and so by embedding $GL_2(\mathbb{Z}_l)$ inside $GL_2(\mathbb{Q}_l)$, we obtain a 2-dimensional representation of $\mathrm{Gal}(k/L)$ over a field of characteristic zero. (At last, progress!)

The Tate Module, IV

Since isogenies also commute with the multiplication-by-l maps, they also act on Tate modules.

- Explicitly, suppose $\varphi : E_1 \to E_2$ is an isogeny. Then since $\varphi \circ [l] = [l] \circ \varphi$, the action of φ induces a natural map of $\mathbb{Z}_l$-modules $\varphi_l : T_l(E_1) \to T_l(E_2)$ via $\varphi_l(P_1, P_2, P_3, \dots) = (\varphi(P_1), \varphi(P_2), \varphi(P_3), \dots)$.
- Since the componentwise action is clearly additive in the isogeny φ, we obtain a group homomorphism $\Psi : \mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(T_l(E_1), T_l(E_2))$.

Exercise: Show that when $E_1 = E = E_2$, the action $\Psi : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$ with $\Psi(\varphi)$ mapping $(P_1, P_2, P_3, \dots) \in T_l(E)$ to $(\varphi(P_1), \varphi(P_2), \varphi(P_3), \dots) \in T_l(E)$ is a ring homomorphism.

The Tate Module, V

Indeed, when $T_l(E_1) \neq 0$, which we know occurs whenever $l \neq \mathrm{char}(k)$, this homomorphism $\Psi : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$ is injective.

The Tate Module, V

Indeed, when $T_l(E_1) \neq 0$, which we know occurs whenever $l \neq \mathrm{char}(k)$, this homomorphism $\Psi : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$ is injective.

- To see this suppose that $\varphi \in \ker(\Psi)$ so that $\varphi(T_l(E_1)) = 0$, which is equivalent to saying that $E[l^d] \in \ker\varphi$ for all d. In particular, $\ker\varphi$ is infinite: but as we showed, nonzero isogenies have a finite kernel, and so we must have $\varphi = 0$.

The Tate Module, V

Indeed, when $T_l(E_1) \neq 0$, which we know occurs whenever $l \neq \mathrm{char}(k)$, this homomorphism $\Psi : \mathrm{End}(E) \to \mathrm{End}(T_l(E))$ is injective.

- To see this suppose that $\varphi \in \ker(\Psi)$ so that $\varphi(T_l(E_1)) = 0$, which is equivalent to saying that $E[l^d] \in \ker \varphi$ for all d. In particular, $\ker \varphi$ is infinite: but as we showed, nonzero isogenies have a finite kernel, and so we must have $\varphi = 0$.

In fact, a much stronger statement is actually true:

Proposition (Isogeny Action on Tate Modules)

The natural map $\mathrm{Hom}(E_1, E_2) \otimes \mathbb{Z}_l \to \mathrm{Hom}(T_l(E_1), T_l(E_2))$ *defined by mapping* $\varphi \otimes 1 \mapsto \varphi_l$ *and then extending* $\mathbb{Z}_l$*-linearly, is injective.*

Summary

We introduced dual isogenies and established many of their properties.

We used dual isogenies to establish the Hasse bound.

Next lecture: The Weil conjectures, the Tate module.