Math 6170 C, Lecture on April 1, 2020

Yongchang Zhu

Plan

(1) V. §1. The Number of Rational Points over Finite Fields (Review)

(2). V. §2. The Weil Conjectures.

(3). V. §3. The Endomorphism Ring.

V. § 1. Number of Rational Points (Review)

Let K be a finite field with $|K| = q$, E/K be an elliptic curve given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

All a_i's are in K.

Theorem V 1.1.

Let E/K be an elliptic curves over a finite field F of q elements. Then

$$||E(K)| - q - 1| \leq 2\sqrt{q}.$$

Proof.

$$|E(K)| = |\ker(1-\phi)| = \deg(1-\phi).$$

$\deg : \mathrm{End}(E) \to \mathbb{R}$ is a positive definite quadratic form (Corollary III 6.3), so by Cauchy-Schwartz inequality, we have

$$|\deg(1-\phi) - \deg(1) - \deg(\phi)| \leq 2\sqrt{\deg(1)\deg(\phi)}$$

that is

$$|\,|E(K)| - 1 - q| \leq 2\sqrt{q}.$$

Let K be a finite field with $|K| = q$. Let V be a projective variety. Let K_n be the degree n extension of K, so $|K_n| = q^n$.

Definition. The zeta function of V/K is the power series

$$Z(V/K, T) = \exp\left(\sum_{n=1}^{\infty} |V(K_n)| \frac{T^n}{n}\right)$$

Let $\mathbb{Q}[[T]]$ be the formal power series ring over $\mathbb{Q}$.

The exponential map $\exp : \mathbb{Q}[[T]]T \to \mathbb{Q}[[T]]$ given by

$$\exp(f) = \sum_{k=0}^{\infty} \frac{1}{k!} f^k$$

is well-defined for the following reason:

$f^k = c(k,k)T^k + c(k,k+1)T^{k+1} + \dots$

The coefficient of T^n in $\exp(f)$ has **no** contribution from the terms $\frac{1}{k!}f^k$ with $k > n$.

The coefficient of T^n in $\exp(f)$ = the coefficient of T^n in $\sum_{k=0}^{n} \frac{1}{k!} f^k$.

The formal logarithmic function

$$\log(1+T)=\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n}T^n \in \mathbb{Q}[[T]]T$$

satisfies that

$$\exp(\log(1+T))=1+T$$

It is obvious that $\mathbb{Q}[T] \subset \mathbb{Q}[[T]]$. Certain localization of $\mathbb{Q}[T]$ can also be embedded into $\mathbb{Q}[[T]]$,

$$\{\frac{P(T)}{Q(T)} \mid P(T), Q(T) \in \mathbb{Q}[T], Q(0) \neq 0\}$$

can be embedded as a subring of $\mathbb{Q}[[T]]$.

$Q(T) = a_0 + a_1 T + \cdots + a_n T^n, a_0 \neq 0,$

$$\frac{1}{Q(T)} \mapsto a_0^{-1}(\sum_{k=0}^{\infty} (-a_0^{-1}(a_1 T + \cdots + a_n T^n))^k)$$

We have

$$|\mathbb{P}^N(K_n)| = \frac{q^{n(N+1)} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}$$

This implies

$$Z(\mathbb{P}^N/K, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^N T)}.$$

Theorem V 2.2.

(Weil Conjecture). Let K be a finite field with q elements and V/K a smooth projective variety of dimension n.

(a) Rationality

$$Z(V/K, T) \in \mathbb{Q}(T).$$

(b) Functional Equation. There is an integer ϵ (called the Euler characteristic of V) so that

$$Z(V/K, T) = \pm q^{n\epsilon/2} T^{\epsilon} Z(V/K, T)$$

(to be continued)

Theorem V 2.2. Continued

(c) Riemann hypothesis. There is a factorization

$$Z(V/K, 1/q^n T) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) P_2(T) \cdots P_{2n}(T)}$$

with each $P_i \in \mathbb{Z}[T]$. Further $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$, and for each $1 \leq i \leq 2n-1$, $P_i(T)$ factors (over $\mathbb{C}$) as

$$P_i(T) = \Pi_j (1 - \alpha_{ij} T)$$

with

$$|\alpha_{ij}| = q^{i/2}.$$

Part (a) (b) are motivated by **Lefschetz Fixed Point Theorem.**

Theorem. Let M be a compact complex manifold of dimension n, $f : M \to M$ be a non-constant holomorphic map, and for at each point point $P \in M$, $\mathrm{Jac}(f)|_P$ is non-degenerate. Then

The number of fixed points of f is equal to

$$\sum_{i=0}^{2n} (-1)^i \mathrm{Tr}\, f^*|_{H^*(M,\mathbb{R})}.$$

where $H^*(M, \mathbb{R})$ is the i-th De-Rham cohomology of M.

Suppose we have suitable cohomology theory for projective varieties V over K, say, $H^*(V, \mathbb{Q}_l)$, so that the analog of Lefschetz Fixed Point Theorem holds. Apply it to the morphisms ϕ^n, where $\phi : V \to V$ is the Forbenius morphism ($x \mapsto x^q$).

$$V(K_n) = \text{fixed point set of } \phi^n$$

$$|V(K_n)| = \sum_{i=0}^{2n} (-1)^i \mathrm{Tr}\, (\phi^*)^n|_{H^*(M,\mathbb{Q})}$$

This would imply

$$Z(V/K,T)$$
$$= \frac{\det(1-\phi^* T)|_{H^1(V)} \cdot \det(1-\phi^* T)|_{H^3(V)} \cdots \det(1-\phi^* T)|_{H^{2n-1}(V)}}{\det(1-\phi^* T)|_{H^0(V)} \cdot \det(1-\phi^* T)|_{H^2(V)} \cdots \det(1-\phi^* T)|_{H^{2n}(V)}}$$

$$P_i(T) = \det(1 - T\phi^*)|_{H^i(V)}.$$

The l-adic cohomology theory was developed by Grothendieck (also Artin) and used to prove (a) (b). Deligne proved (c).

For each $\psi \in \mathrm{End}(E)$, $\psi : E[l^n] \to E[l^n]$, we have commutative diagram

$$\begin{array}{ccc} E[l^{n+1}] & \xrightarrow{\psi} & E[l^{n+1}] \\ \downarrow [l] & & \downarrow [l] \\ E[l^n] & \xrightarrow{\psi} & E[l^n] \end{array}$$

This means ψ acts on the Tate module $T_l(E)$, so we have a ring homomorphism

$$\mathrm{End}(E) \to \mathrm{End}(T_l(E)), \quad \psi \mapsto \psi_l$$

Since $T_l(E)$ is a free $\mathbb{Z}_l$-module of rank 2, so each ψ_l can be presented as a 2×2 matrix over $\mathbb{Z}_l$. We can define its determinant and trace:

$$\det(\psi_l), \quad \mathrm{tr}(\psi_l)$$

Proposition V 2.3.

Let $\psi \in \mathrm{End}(E)$. Then

$$\det(\psi_l) = \deg(\psi)$$

and

$$\mathrm{tr}(\psi_l) = 1 + \deg(\psi) - \deg(1 - \psi).$$

Proof. Let v_1, v_2 be a basis for $T_l(E)$, assume the matrix for ψ_l w.r.t. this basis is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Recall we have a non-degenerate, bilinear, skew-symmetric pairing:

$$e : T_l(E) \times T_l(E) \to T_l(\mu) \simeq \mathbb{Z}_l$$

Proof (continued).

$$\begin{aligned} e(v_1, v_2)^{\deg \psi} &= e([\deg \psi] v_1, v_2) \\ &= e(\hat{\psi}_l \psi_l v_1, v_2) \\ &= e(\psi_l v_1, \psi_l v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} \end{aligned}$$

Since $e(\ )$ is non-degenerate and skew-symmetric, so $e(v_1, v_1) = e(v_2, v_2) = 1$ $e(v_1, v_2) \in T_l(\mu)$ is a generator of $\mathbb{Z}_l$-module $T_l(\mu)$. So

$$\deg \psi = ad - bc = \det(\psi_l)$$

Proof (continued).

The second identity follows the identity

$$\mathrm{tr}(A) = 1 + \det(A) - \det(1 - A)$$

for any 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

$$\mathrm{Right} = 1 + ad - bc - ((1-a)(1-d) - bc) = a + d = \mathrm{tr}(A)$$

Let $\phi : E \to E$ be the q-th power Frobenius endomorphism,

$$|E(K)| = \deg(1 - \phi)$$

Similarly,

$$|E(K_n)| = \deg(1 - \phi^n)$$

From Prop. 2.3, the characteristic polynomial of ϕ_l

$$\det(T - \phi_l) = T^2 - \mathrm{tr}(\phi_l)T + \det(\phi_l)$$

is a polynomial with coefficients in $\mathbb{Z}$. Assume we have a factorization over $\mathbb{C}$:

$$\det(T - \phi_l) = (T - \alpha)(T - \beta)$$

We claim α and β are complex conjugate each other. It is enough to prove $\det(T - \phi_l)|_{T=r} \geq 0$ for all real number r.

It is enough to prove $\det(T - \phi_l)|_{T=r} \geq 0$ for all rational number $\frac{m}{n}$.

$$\det(\frac{m}{n} - \phi_l) = \frac{1}{n^2}\det(m - n\phi_l) = \frac{1}{n^2}\deg(m - n\phi_l) \geq 0$$

So we have $|\alpha| = |\beta|$.

$$\alpha\beta = \det(\phi_l) = \deg(\phi) = q.$$

$$\det(T - \phi_l^n) = (T - \alpha^n)(T - \beta^n)$$

Theorem. $|E(K_n)| = 1 - \alpha^n - \beta^n + q^n$.

Proof.

$$|E(K_n)| = \deg(1 - \phi^n) = \det(1 - \phi_l^n) = 1 - \alpha^n - \beta^n + q^n$$

Theorem V 2.4.

Let K be a finite field with $|K| = q$ and E/K an elliptic curve. Then there is an $a \in \mathbb{Z}$ so that

$$Z(E/K, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

Further

$$Z(E/K, \frac{1}{qT}) = Z(E/K, T)$$

and

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$$

with $|\alpha| = |\beta| = \sqrt{q}$.

Proof.

$$\begin{aligned}\log Z(E/K,T) &= \sum_{n=1}^{\infty}|E(K_n)|\frac{T^n}{n}\\ &= \sum_{n=1}^{\infty}(1-\alpha^n-\beta^n+q^n)\frac{T^n}{n}\\ &= -\log(1-T)+\log(1-\alpha T)\\ &\quad+\log(1-\beta T)-\log(1-qT)\end{aligned}$$

Proof (continued).
Hence

$$Z(E/K, T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)}.$$

The remaining part of theorem is straightforward.

The real Riemann hypothesis is about the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

$\zeta(s)$ has zeros at $-2, -4, \ldots$. The RH claims that all the other zeros are in the critical line $\mathrm{re}\, s = \frac{1}{2}$.

We replace T in $Z(E/K, T)$ by $T = q^{-s}$, then $Z(E/K, q^{-s})$ has a functional equation that relates the values at s and $1 - s$, and the zeros are on the line $\mathrm{re}\, s = \frac{1}{2}$.

Theorem V. 3.1. Let K be a perfect field of characteristic p, and E/K be an elliptic curve. Then the following three conditions are equivalent:

(a) $E[p] = 0$

(b) $E[p^r] = 0$ for all $r \geq 1$.

(c) $\mathrm{End}(E)$ is an order in a quaternion algebra.

Definition. E is called to be **supersingular** if the conditions in Theorem hold.

Chapter VI. Elliptic Curves over $\mathbb{C}$.

The elliptic curves over $\mathbb{C}$ are in one-to-one correspondence with compact Riemann surfaces of genus 1 with a marked point.

Every Riemann surface of genus 1 is isomorphic to a quotient $\mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$.

We have analytic tools to study elliptic curves over $\mathbb{C}$.

A **lattice** in $\mathbb{C}$ is a free $\mathbb{Z}$-submodule $\Lambda \subset \mathbb{C}$ of rank two such that a basis of Λ is $\mathbb{R}$-linearly independent.

Example. $\mathbb{Z} + \mathbb{Z}i$ is a lattice.

Example. $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ is **not** a lattice.

A lattice can be written as

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

where ω_1 and ω_2 are $\mathbb{R}$-linear independent.

Definition. An **elliptic function** (relative to the lattice Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ such that

$$f(z+\omega) = f(z)$$

for all $\omega \in \Lambda$ and all $z \in \mathbb{C}$.

To be continued.

End