Average version of BSD conjecture

XIYU HU

January 11, 2018

We begin with the Weierstrass form of elliptic equation, i.e. look it as an embedding cubic curve in $\mathbb{P}^2$.

Definition 1 (Weierstrass form) *$E \hookrightarrow \mathbb{P}^2$, In general the form is given by,*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

If $charF \neq 2, 3$, then, we have a much more simper form,

$$y^2 = x^3 + ax + b, \Delta := 4a^3 + 27b^2 \neq 0. \tag{2}$$

Remark 2

$$\Delta(E) = \prod_{1 \leq i, \neq j \leq 3} (z_i - z_j)$$

Where $z_i^3 + az_i + b = 0, \forall 1 \leq i \leq 3$.

We have two way to classify the elliptic curve E living in a fix field F.

j-invariant The first one is by the isomorphism in $\bar{F}$. i.e. we say two elliptic curves E_1, E_2 is equivalent iff

$$\exists \rho : \bar{F} \to \bar{F}$$

is a isomorphism such that $\rho(E_1) = E_2$.

Definition 3 (j-invariant) *For a elliptic curve E, we have a j-invariant of E, given by,*

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \tag{3}$$

Why j-invariant is important, because j-invariant is the invariant depend the equivalent class of E under the classify of isomorphism induce by $\bar{F}$.

But in one equivalent class, there also exist a structure, called twist.

Definition 4 (Twist) *For a elliptic curve $E : y^2 = x^3 + ax + b$, all elliptic curve twist with E is given by,*

$$E^{(d)} : y^2 = x^3 + ad^2x + bd^3 \tag{4}$$

So the twist of a given elliptic curve E is given by:

$$H^1(Gal(\bar{F}/F), Aut(E_{\bar{F}})) \tag{5}$$

Remark 5 *Of course a elliptic curve $E : y^2 = x^3 + ax + b$ is the same as $E : y^2 = x^3 + ad^2x + bd^4$, induce by the map $\mathbb{P}^1 \to \mathbb{P}^1, (x, y, 1) \to (x, dy, 1)$.*

But this moduli space induce by the isomorphism of F is not good, morally speaking is because of the abandon of universal property. see [1].

Level n structure We need a extension of the elliptic curve E, this is given by the integral model.

Definition 6 (Integral model) *$s := Spec(\mathcal{O}_F)$, $E \to E_s$. E_s is regular and minimal, the construction of E_s is by the following way, we first construct $\widetilde{E_s}$ and then blow up. $\widetilde{E}_s$ is given by the Weierstrass equation with coefficent in $\mathcal{O}_F$.*

Remark 7 *The existence of integral model need Zorn's lemma.*

Definition 8 (Semistable) *the singularity of the minimal model of E are ordinary double point.*

Remark 9 *Semistable is a crucial property, related to Szpiro's conjecture.*

Definition 10 (Level n structure)

$$\phi : (\mathbb{Z}/n\mathbb{Z})_s^2 \longrightarrow E[N] \tag{6}$$

$P = \phi(1, 0), Q = \phi(o, 1)$ The weil pairing of P, Q is given by a unit in cycomotic fields, i.e. $< P, Q >= \zeta_N \in \mu_N(s)$

What happen if $k = \mathbb{C}$? In this case we have a analytic isomorphism:

$$E(\mathbb{C}) \simeq \mathbb{C}/\Lambda \tag{7}$$

Given by,

$$\mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2 \tag{8}$$

$$z \longrightarrow (\mathfrak{P}(z), \mathfrak{P}'(z), 1) \tag{9}$$

Where $\mathfrak{P}(\mathfrak{z}) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda, \lambda \neq 0} (\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2})$, and the Weierstrass equation E is given by $y^2 = 4x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$. The full n tructure of it is given by $\mathbb{Z} + \mathbb{Z}\lambda$ and the value of P, Q, i.e.

$$P = \frac{1}{N}, Q = \frac{\tau}{N} \tag{10}$$

Where τ is induce by

$$\Gamma(N) := ker(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n\mathbb{Z})) \tag{11}$$

The key point is following:

Theorem 11 *$k = \mathbb{C}$, the moduli of elliptic curves with full level n-structure is identified with*

$$\mu_N^* \times H/\Gamma(N) \tag{12}$$

Now we discuss the Mordell-Weil theorem.

Theorem 12 (Mordell-Weil theorem)

$$E(F) \simeq \mathbb{Z}^r \oplus E(F)_{tor}$$

The proof of the theorem divide into two part:

1. Weak Mordell-Weil theorem, i.e. $\forall m \in \mathbb{N}$, $E(F)/mE(F)$ is finite.
2. There is a quadratic function,

$$\| \cdot \| : E(F) \longrightarrow \mathbb{R} \tag{13}$$

   $\forall c \in \mathbb{R}$, $E(F)_c = \{P \in E(F), \|P\| < c\}$ is finite.

Remark 13 *The proof is following the ideal of infinity descent first found by Fermat. The height is called Faltings height, introduce by Falting. On the other hand, I point out, for elliptic curve E, there is a naive height come from the coefficient of Weierstrass representation, i.e.* $\max\{|4a^3|, |27b^2|\}$.

While the torsion part have a very clear understanding, thanks to the work of Mazur. The rank part of $E(\mathbb{Q})$ is still very unclear, we have the BSD conjecture, which is far from a fully understanding until now.

But to understanding the meaning of the conjecture, we need first constructing the zeta function of elliptic curve, $L(s, E)$.

Local points We consider a local field F_v, and a locally value map $F \to F_\nu$, then we have the short exact sequences,

$$0 \longrightarrow E^0(F_\nu) \longrightarrow E(F_\nu) = E_s(\mathcal{O}_F) \longrightarrow E_s(K_0) \longrightarrow 0 \tag{14}$$

Topologically, we know $E(F_\nu)$ are union of disc indexed by $E_s(k_\nu)$,

$$|E_s(k_\nu)| \sim q_\nu + 1 = \#\mathbb{P}^1(k_\nu)$$

. Define $a_\nu = \#\mathbb{P}^1(k_\nu) - |E_s(k_\nu)|$, then we have Hasse principle:

Theorem 14 (Hasse principle)

$$|a_\nu| \leq 2\sqrt{q_\nu} \tag{15}$$

Remark 15 *I need to point out, the Hasse principle, in my opinion, is just a uncertain principle type of result, there should be a partial differential equation underlying mystery.*

So count the points in $E(F)$ reduce to count points in $H^1(F_\nu, E(m))$, reduce to count the Selmer group $S(E)[m]$. We have a short exact sequences to explain the issue.

$$0 \longrightarrow E(F)/mE(F) \longrightarrow Ш(E)[m] \longrightarrow E(F)/mE(F) \longrightarrow 0 \tag{16}$$

I mention the Goldfold-Szipiro conjecture here.

Conjecture 1 (Goldfold-Szipiro conjecture) $\forall \epsilon > 0$, *there* $\exists C_\epsilon(E)$ *such that:*

$$\#(E) \leq c_\epsilon(E) N_{E/\mathbb{Q}}(N)^{\frac{1}{2}+\epsilon} \tag{17}$$

L-series Now I focus on the construction of $L(s, E)$, there are two different way to construct the L-series, one approach is the Euler product.

$$L(s, E) = \prod_{\nu:bad} (1 - a_\nu q_\nu^{-s})^{-1} \cdot \prod_{\nu:good} (1 - a_\nu q_\nu^{-s} + q_\nu^{1-2s})^{-1} \tag{18}$$

Where $a_\nu = 0, 1$ or -1 when E_s has bad reduction on ν.

The second approach is the Galois presentation, one of the advantage is avoid the integral model. Given l is a fixed prime, we can consider the Tate module:

$$T_l(E) := \varprojlim_{l^n} E[l^n] \tag{19}$$

Then by the transform of different embedding of $F \hookrightarrow \bar{F}$, we know $Gal(\bar{F}/F) \curvearrowright T_l(E)$, decompose it into a lots of orbits, so we can define D_ν, the decomposition group of w(extension of ν to $\bar{F}$). We define I_ν is the inertia group of D_ν.

Then D_ν/I_ν is generated by some Frobenius elements

$$Frob\nu x \equiv x^{q_\nu}(modw), \forall x \in \mathcal{O}_{\bar{Q}} \tag{20}$$

So we can define

$$L_\nu(s, E) = (1 - q_\nu^{-s} Frob_\nu | T_l(E)^{I_\nu})^{-1} \tag{21}$$

And then $L(s, E) = \prod_\nu L_\nu(s, E)$.

Faltings have proved $L_\nu(s, E)$ is the invariant depending the isogenous class in the follwing meaning:

Theorem 16 (Faltings) *$L_\nu(s, E)$ is an isogenous ivariant, i.e. E_1 isogenous to E_2 iff $\forall a.e.\nu$, $L_\nu(s, E_1) = L_\nu(s, E_2)$.*

Conjecture 2 (Modulring conjecture)

$$L(s, E) = L(s - \frac{1}{2}, \pi) \tag{22}$$

Where π come from an automorphic representation for $GL_2(A_F)$.

Now we give the statement of BSD onjecture.

Conjecture 3 (BSD conjecture) *R is the regulator of E, i.e. the volume of fine part of $E(F)$ with respect to the Neron-Tate height pairing. Ω be the volume of $\prod_{v|\infty} F(F_v)$ Then we have,*

1. *$ord_{s=1} L(s, E) = rank E(F)$.*
2. *$|Ш(E)| < \infty$.*
3. *$\lim_{s\to 0} L(s, E)(s-1)^{-rank(E)} = c \cdot \Omega(E) \cdot R(E) \cdot |Ш(E)| \cdot |E(F)_{tor}|^{-2}$*

Here c is an explictly positive integer depending only on E_ν for ν dividing N.

References

[1] Elliptic curves, L-functions, and CM-points, Shou-Wu Zhang 2