ARITHMETIC OF ELLIPTIC CURVES

WEI ZHANG

NOTES TAKEN BY PAK-HIN LEE

Abstract. Here are the notes I am taking for Wei Zhang's ongoing course on the arithmetic of elliptic curves offered at Columbia University in Fall 2014 (MATH G6761: Topics in Arithmetic Geometry). As the course progresses, these notes will be revised. I recommend that you visit my website from time to time for the most updated version.

Due to my own lack of understanding of the materials, I have inevitably introduced both mathematical and typographical errors in these notes. Please send corrections and comments to phlee@math.columbia.edu.

Contents

Last updated: September 20, 2014.

1. Lecture 1 (September 4, 2014)

The main topic for this course will be the arithmetic of elliptic curves over global fields, by which we include both number fields and function fields. Today we will only sketch the main goals of this class.

There are two parallel sets of statements between number fields $F/\mathbb{Q}$ and function fields $F = k(C)$ (of positive characteristic, i.e. $C \to k$ a finite field of characteristic p). The central problem, as everyone knows, is the Birch–Swinnerton-Dyer conjecture. For an elliptic curve E over a global field F, the Mordell–Weil theorem says that $E(F)$ is a finitely generated abelian group, so

$$E(F) \cong \mathbb{Z}^{r_{\mathrm{MW}}} \oplus \text{finite group}$$

where r_{MW} is called the Mordell–Weil rank. On the other hand, there is the analytic rank. To the elliptic curve we can associate an L-function $L(E/F, s)$, where $s \in \mathbb{C}$. In the case F is a function field (due to Drinfeld), $\mathbb{Q}$ (due to Wiles *et al.*) or a real quadratic field, this L-function comes from the L-function of a modular form. $L(E/F, s)$ is centered at $s = 1$, and we define the analytic rank to be

$$r_{\mathrm{an}}(E/F) = \operatorname{ord}_{s=1} L(E/F, s).$$

Conjecture 1.1 (Birch–Swinnerton-Dyer)**.**

1. *BSD rank:*
$$r_{MW}(E/F) = r_{an}(E/F).$$
2. *BSD refined: the leading coefficient of the L-function can be expressed in terms of $E(F)$ and the Tate–Shafarevich group $Ш(E/F)$.*

The Tate–Shafarevich group is roughly defined as

$$Ш(E/F) = \{C : E\text{-torsor over } F,\ E \times C \to C, \text{ trivial locally everywhere, i.e. } C(F_v) \neq \emptyset \text{ for all places } v \text{ of } F\}.$$

It measures a local-to-global obstruction. $Ш(E/F)$ is a torsion abelian group, so can be decomposed as

$$\bigoplus_{\ell \text{ prime}} Ш(E/F)[\ell^\infty].$$

Conjecture 1.2 (Tate–Shafarevich)**.** *$Ш(E/F)$ is finite.*

The BSD refined conjecture can be thought of as a class number formula.

Remark. If $Ш(E/F)$ is finite, then $\#Ш(E/F)$ is a square.

How much is known? We have the following

Theorem 1.3 (M. Artin–Tate, Milne)**.** *If F is a function field, then*

$$r_{MW}(E/F) \leq r_{an}(E/F).$$

Moreover, the following are equivalent:

1. $r_{MW}(E/F) = r_{an}(E/F)$*;*
2. $Ш(E/F)$ *is finite;*
3. $Ш(E/F)[\ell^\infty]$ *is finite for some prime* ℓ*;*
4. *both BSD rank and BSD refined hold.*

Now we introduce the Selmer group. For $n > 1$ prime to p, consider the exact sequence

$$0 \to E[n](\overline{F}) \to E(\overline{F}) \xrightarrow{n} E(\overline{F}) \to 0.$$

Taking cohomology gives

$$0 \to E(F)/nE(F) \to H^1(F, E[n]).$$

A natural question is how we can characterize the image. We can look at the localizations and get a commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & E(F)/nE(F) \arrow[r] \arrow[d, "\text{diagonal } \Delta"'] & H^1(F, E[n]) \arrow[d, "\prod \mathrm{loc}_v"] \\ & \prod_v E(F_v)/nE(F_v) \arrow[r, "\text{Kummer}"] & \prod_v H^1(F_v, E[n]). \end{tikzcd}$$

But this might not be a Cartesian diagram. We define $\mathrm{Sel}_n(E/F)$ to be the fiber product

$$\begin{tikzcd} \mathrm{Sel}_n(E/F) \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & H^1(F, E[n]) \arrow[d] \\ \prod_v E(F_v)/nE(F_v) \arrow[r] & \prod_v H^1(F_v, E[n]), \end{tikzcd}$$

i.e.

$$\mathrm{Sel}_n(E/F) = \{c \in H^1(F, E[n]) : \mathrm{loc}_v(c) \in E(F_v)/nE(F_v) \text{ for all } v\}.$$

Lemma 1.4. $\mathrm{Sel}_n(E/F)$ *is finite for all* n.

The map $E(F)/nE(F) \to \mathrm{Sel}_n(E/F)$ is injective but in general not bijective, hence $\mathrm{Sel}_n(E/F)$ is only a homological (over-)approximation of $E(F)/nE(F)$. It turns out there is an exact sequence

$$0 \to E(F)/nE(F) \to \mathrm{Sel}_n(E/F) \to Ш(E/F)[n] \to 0.$$

People often say $\mathrm{Sel}_n(E/F)$ is "computable", but only relatively so compared to the other two groups.

Let ℓ be a prime different from p. Replacing n by ℓ^n and taking inductive limit, we get

$$0 \to E(F) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to \mathrm{Sel}_{\ell^\infty}(E/F) \to Ш(E/F)[\ell^\infty] \to 0.$$

Conjecturally the last term is finite. In more detail, we know the first term is $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{r_{\mathrm{MW}}}$, and let the middle term be

$$(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{r_\ell} \oplus \text{finite group}$$

where r_ℓ is called the ℓ^∞-Selmer rank. Certainly we have

$$0 \le r_{\mathrm{MW}} \le r_\ell,$$

with equality if and only if $Ш(E/F)[\ell^\infty]$ is finite.

If F is a function field, it is known that $r_{\mathrm{an}}(E/F) \ge r_\ell(E/F)$. We have equality if the (partial) semisimplicity conjecture holds, which we will discuss later.

Finally, we give some consequences of the BSD conjecture.

Conjecture 1.5 (ℓ-independence)**.** $r_\ell(E/F)$ *is independent of* ℓ.

Remark. There is no known example of an elliptic curve E over a number field F which has rank ≥ 2 and finite $Ш(E/F)$.

Theorem 1.6 (Artin–Swinnerton-Dyer)**.** *Suppose E is an elliptic curve over $F = k(\mathbb{P}^1)$ which is the generic fiber of a $K3$ surface X*

$$\begin{tikzcd} X \arrow[d] & E \arrow[l] \arrow[d] \\ \mathbb{P}^1 & F. \arrow[l] \end{tikzcd}$$

Then BSD holds for E/F. Moreover $r_{MW}(E/F) \leq 22$.

Things certainly look more promising in the function field case! For number fields, we have

Theorem 1.7 (Gross–Zagier, Kolyvagin, S. Zhang)**.** *Let F be a totally real field, and E/F be an elliptic curve parametrized by a Shimura curve (this is known for $F = \mathbb{Q}$). If $r_{an}(E/F) \leq 1$, then BSD rank holds and $\#Ш(E/F) < \infty$.*

Remark. If F is a function field, the same holds but we can obtain more information.

Conjecture 1.8 ($\mathrm{rank}_i(E/F, \ell)$)**.** *If $r_\ell(E/F) = i$, then $r_{MW}(E/F) = i$ and $\#Ш(E/F)[\ell^\infty] < \infty$.*

Note this is a purely algebraic statement and does not involve the L-function. In the function field case, this statement is equivalent to the BSD conjecture, but in the number field case this is weaker.

- For $i = 0$, this conjecture is trivial but already has interesting consequences. In the function field case, this implies the full BSD by the theorem of Tate and Milne. In the case $F = \mathbb{Q}$, we can deduce the BSD using the non-vanishing of L-functions by Kato and Skinner–Urban.
- For $i = 1$, this conjecture is known for function fields but not for number fields.

Here are some applications:

- Assuming $\mathrm{rank}_1(E/\mathbb{Q}, \ell = 2)$, the congruent number problem is "mostly solved".
- Assuming $\mathrm{rank}_1(E/F, \ell = 2)$, Hilbert's tenth problem is answered in the negative for the ring of integers of any number field. This is due to Mazur and Rubin.
- Assuming $\mathrm{rank}_1(E/K, \ell = 3)$ where $K/\mathbb{Q}$ is quadratic, the Hasse principle for diagonal cubic 3-folds can be proved. Given $X = \{\sum_{i=1}^{5} a_i X_i^3 = 0\} \subset \mathbb{P}^4$ where $a_i \in \mathbb{Q}$, if $X(\mathbb{Q}_p) \neq \emptyset$ for all p then $X(\mathbb{Q}) \neq \emptyset$. In fact we only need to prove for E with complex multiplication by $\mathbb{Z}[\sqrt{-3}]$.

What I could prove was

Theorem 1.9 (W. Zhang)**.** $\mathrm{rank}_1(E/\mathbb{Q}, \ell)$ *holds for large, "ordinary" $\ell \geq 5$ with some technical conditions. Moreover, one has ℓ-independence in this case.*

The result of Artin and Swinnerton-Dyer is about elliptic $K3$ surfaces. In the perpendicular direction, we have the function field analogue of Gross–Zagier, Kolyvagin and Zhang. Can one "take fiber product" of these?

Heegner points can be used to construct elements of Ш, so one might be interested in the consequences of Kolyvagin's conjecture in the function field case.

The BSD conjecture for elliptic curves is equivalent to

Theorem 1.10 (Tate, Artin). *Suppose the map $\mathcal{X} \to C/k$ from a smooth surface to a smooth curve (over a finite field k) has generic fiber $X \to F = k(C)$ which is a smooth curve. Then the following are equivalent:*

(1) *BSD for* $\mathrm{Jac}(X/F)$*;*
(2) *Tate conjecture for* $\mathcal{X}/k$*;*
(3) $\#\,\mathrm{Br}(\mathcal{X}) < \infty$.

2. Lecture 2 (September 9, 2014)

We will start with the function field case which is much simpler. If we want to compare results with the number field case, we will give a proof for that. For now we will explain some basic results for the Birch–Swinnerton-Dyer conjecture.

Some references for the arithmetic of elliptic curves over function fields are:

- Douglas Ulmer, IAS/Park City Lecture Notes[1];
- Shou-Wu Zhang, Princeton Lecture Notes[2].

Let me give a simple example where we can really prove the BSD. Let $F = k(C)$ where C is a smooth projective curve over a finite field $k = \mathbb{F}_q$ of characteristic $p \geq 5$. Consider an elliptic curve E/F, i.e. a smooth curve over F which is an abelian variety. E can be parametrized by the equation

$$y^2 = x^3 + ax + b$$

with discriminant

$$\Delta = -16(4a^3 + 27b^2)$$

and j-invariant

$$j = 2^{12}3^3\frac{a^3}{\Delta}.$$

Definition 2.1.

(1) An elliptic curve E/F is constant if $E = E_0 \times F$ where E_0/k is an elliptic curve.
(2) An elliptic curve E$/F$ is isotrivial if there exists a finite extension F'/F such that $E \times_F F'$ is constant.
(3) An elliptic curve is non-constant (*resp.* non-isotrivial) if (1) (*resp.* (2)) does not happen.

Lemma 2.2. *E/F is isotrivial if and only if $j(E) \in k$.*

Note that the j-invariant doesn't care about the base field. We identify $k = k' \cap F$.

Now we will define the L-function of E over $F = k(C)$. The reduction of E at $v \in |C|$ (the set of closed points of C) has a minimal Weierstrass model over the local field F_v (with ring of integers $\mathcal{O}_v$), with three possible kinds of reduction:

- good reduction;
- multiplicative reduction (nodal point);
- additive reduction (cuspidal point).

[1]Available at `http://people.math.gatech.edu/~ulmer/research/papers/2011.pdf`.
[2]Available at `http://web.math.princeton.edu/~shouwu/teaching/RatP.pdf`.

We define the conductor of E/F to be

$$\mathfrak{n} = \sum_{v \in |C|} \delta_v v \in \mathrm{Div}(C)$$

where

$$\delta_v = \begin{cases} 0 & \text{if } E \text{ has good reduction at } v, \\ 1 & \text{if } E \text{ has multiplicative reduction at } v, \\ \geq 2 & \text{if } E \text{ has additive reduction at } v. \end{cases}$$

If $p \geq 5$, δ_v equals 2 in the last case. The degree of $\mathfrak{n}$ is

$$\deg(\mathfrak{n}) = \sum \delta_v \deg(v).$$

Definition 2.3. The L-function of E/F is

$$L(E/F, s) = \prod_{v \in |C|} L(E/F_v, s)$$

for $s \in \mathbb{C}$, where the local L-factor is

$$L(E/F_v, s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$$

where

$$a_v = \#E(k_v) - (q_v + 1).$$

It is instructive to compare this with the zeta function of schemes over finite fields. The zeta function of a smooth projective variety $X/k = \mathbb{F}_q$ is

$$\zeta(T, X) = \prod_{v \in |X|} (1 - T^{\deg(v)})^{-1}$$

where $T = q^{-s}$. Alternatively, this can be defined as

$$\zeta(T, X) = \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{T^n}{n} \right).$$

In case X is a curve, this can be rewritten in terms of cohomology:

$$\zeta(T, X) = \frac{\prod_{i=1}^{2g(X)} (1 - \alpha_i T)}{(1 - T)(1 - qT)}$$

where α_i are the Weil numbers, i.e. eigenvalues of the Frobenius operator acting on the cohomology $H^1(X \times \overline{k}, \mathbb{Q}_\ell)$ for $\ell \neq p$.

Example 2.4 (L-function of a constant elliptic curve)**.** Let E be the constant elliptic curve over $F = k(C)$ obtained by base change from E_0/k. Then

$$\begin{aligned} L(E/F, s) &= \prod_{v \in |C|} L(E/F_v, s) \\ &= \prod_{v \in |C|} (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1} \end{aligned}$$

where $\alpha_v = \#E_0(k_v) - (q_v + 1)$.

We can write

$$\zeta(T, E_0) = \frac{(1-\alpha_1 T)(1-\alpha_2 T)}{(1-T)(1-qT)}$$

where $E_0(\mathbb{F}_{q^n}) = (q^n+1) + (\alpha_1^n + \alpha_2^n)$ and $\alpha_1\alpha_2 = q$. Thus

$$a_v = \alpha_1^n + \alpha_2^n$$

for $n = \deg(v)$, and $q_v = q^n$. Therefore we can factorize to get

$$\begin{aligned} L(E/F, s) &= \prod_{v \in |C|} (1 - \alpha_1^{\deg(v)} q^{-\deg(v)s})^{-1} (1 - \alpha_2^{\deg(v)} q^{-\deg(v)s})^{-1} \\ &= \zeta(\alpha_1 q^{-s}, C)\zeta(\alpha_2 q^{-s}, C). \end{aligned}$$

The zeta function of C is

$$\zeta(T, C) = \frac{\prod_{j=1}^{2g(C)} (1 - \beta_j T)}{(1-T)(1-qT)}$$

where β_j are the Weil numbers. In summary, we have proved that

$$L(E/F, s) = \frac{\prod_{i=1}^{2} \prod_{j=1}^{2g(C)} (1 - \alpha_i \beta_j q^{-s})}{\prod_{i=1}^{2} (1 - \alpha_i q^{-s}) \prod_{i=1}^{2} (1 - \alpha_i q^{1-s})}.$$

The numbers $\{a_i\}$ and $\{\beta_j\}$ are determined by the curves E_0/k and C/k respectively.

This function certainly has meromorphic continuation, with zeros when $q^s = \alpha_i \beta_j$ for some i, j. But $|\alpha_i| = |\beta_j| = \frac{1}{2}$, so this is only possible when $\mathrm{Re}(s) = 1$. $L(E/F, s)$ satisfies a functional equation under $s \mapsto 2 - s$, since $\{q/\beta_k\}$ is the same set as $\{\beta_j\}$. The degree of $L(E/F, s)$ (as a rational function of q^{-s}) is $4g(C) - 4$.

Remark. In general, if E is non-constant, $L(E/F, s)$ is a polynomial of q^{-s} of degree $4g(C) - 4 + \deg(\mathfrak{n})$ where $\mathfrak{n}$ is the conductor of E.

Recall the BSD rank conjecture:

$$\mathrm{ord}_{s=1} L(E/F, s) = \operatorname{rank} E(K).$$

Let us verify this for the constant elliptic curve. From the explicit calculation of the L-function, we have the

Corollary 2.5.

$$\mathrm{ord}_{s=1} L(E/F, s) = \#\{(i,j) : \alpha_i \beta_j = q\} = \#\{(i,j) : \alpha_i = \beta_j\}.$$

What about the Mordell–Weil group? Suppose the constant curve E_0/k is given by $y^2 = x^3 + ax + b$ where $a, b \in k$. Then

$$E_0(k(C)) = \mathrm{Mor}_k(C, E_0)$$

The fact that C is a curve is important: any morphism from an open subset of C extends to all of C. A point of $E_0(k(C))$ is torsion if and only if it corresponds to the constant morphism, i.e.

$$E_0(k(C))_{\mathrm{tor}} \cong E_0(k)$$

Using the Albanese property, we see that there is a surjection

$$E_0(k(C)) = \mathrm{Mor}_k(C, E_0) \twoheadrightarrow \mathrm{Hom}_k(\mathrm{Jac}(C), E_0) = \mathrm{Hom}_k(E_0, \mathrm{Pic}^0(C))$$

with kernel being the torsion. Thus

$$\operatorname{rank} E_0(k(C)) = \operatorname{rank} \operatorname{Hom}_k(\operatorname{Jac}(C), E_0).$$

Recall the Tate module for an abelian variety A/k and $\ell \neq \operatorname{char} k$:

$$T_\ell(A) = \varprojlim_{\ell} A[l^n],$$

which is a $\mathbb{Z}_\ell$-module of rank $2\dim A$, and we set $V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$.

$$\begin{tikzcd} E_0 \arrow[d] & \\ k & C \arrow[l] \end{tikzcd}$$

Thus, to prove the BSD conjecture for a constant elliptic curve, it suffices to show

$$\#\{(i,j) : \alpha_i = \beta_j\} = \operatorname{rank} \operatorname{Hom}(\operatorname{Jac}(C), E_0).$$

Since the Weil numbers are the eigenvalues of Frob acting on $H^1(X \times \overline{k}, \mathbb{Q}_\ell)$, and $\operatorname{Gal}(\overline{k}/k) = \langle \mathrm{Frob} \rangle$, the left hand side is the $\mathbb{Q}_\ell$-dimension of

$$\operatorname{Hom}_{\mathbb{Q}_\ell}(H^1(C \times \overline{k}, \mathbb{Q}_\ell), H^1(E_0 \times \overline{k}, \mathbb{Q}_\ell))^{\operatorname{Gal}(\overline{k}/k)} = \operatorname{Hom}_{\operatorname{Gal}(\overline{k}/k)}(V_\ell(\operatorname{Jac}(C)), V_\ell(E_0)).$$

We have

$$\text{order of } L\text{-function} = \dim_{\mathbb{Q}_\ell} \operatorname{Hom}_{\operatorname{Gal}(\overline{k}/k)}(V_\ell(\operatorname{Jac}(C)), V_\ell(E_0))$$

and

$$\operatorname{rank} E_0(k(C)) = \operatorname{rank}_{\mathbb{Z}} \operatorname{Hom}(\operatorname{Jac}(C), E_0)$$

These are related by the Tate homomorphism conjecture.

Theorem 2.6 (Tate)**.** *If A and B are abelian varieties over a finite field k, and $\ell \neq \operatorname{char} k$ is a prime, then the natural injection*

$$\operatorname{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \hookrightarrow \operatorname{Hom}_{\operatorname{Gal}(\overline{k}/k)}(T_\ell A, T_\ell B)$$

is an isomorphism.

Tate conjectured the same statement for number fields k, which was proved by Faltings. The function field case is also known. In general, the existence of algebraic cycles is very difficult to prove. Surjectivity here comes from the construction of "rational" points of $E_0(k(C))$.

Someone should give a talk on the Tate homomorphism conjecture over finite fields, and I will move on to the non-constant curve case. I will assume some familiarity of the first section of Chapter V of Hartshorne (surfaces and some intersection theory).

3. Lecture 3 (September 11, 2014)

Last time we considered the constant elliptic curve, and reduced everything to Tate's conjecture for abelian varieties over finite fields. Today I will move to the non-constant case, and relate the Tate conjecture with BSD. The reference is:

- Tate, *Conjectures on algebraic cycles in ℓ-adic cohomology* (in Motives, Part 1).

Let me introduce the Tate conjecture.

Let X be a smooth projective variety over k (any field). (Later we will consider k that is finitely generated over its prime field, and for BSD over function field we will further specialize to finite fields k in our class.) For $0 \le j \le \dim X = d$, we define the Chow group to be

$$\mathrm{Ch}^j(X)_{\mathbb{Q}} = \frac{\text{group of algebraic cycles of codimension } j}{\text{rational equivalence}} \otimes \mathbb{Q}.$$

For any Galois extension k'/k, we have

$$\mathrm{Ch}(X_{k'})_{\mathbb{Q}}^{\mathrm{Gal}(k'/k)} = \mathrm{Ch}(X)_{\mathbb{Q}}.$$

In the divisor case, namely $j = 1$, we can consider

$$\mathrm{Ch}^1(X) = \mathrm{Pic}(X) = H^1(X, \mathcal{O}_X^*) = \text{isomorphism classes of line bundles.}$$

We can study algebraic cycles in terms of cohomology. Let $\ell \neq \mathrm{char}\, k$ be a prime, and $\overline{k}$ be a separable closure of k. Consider $\overline{X} = X \times_k \overline{k}$ and the ℓ-adic cohomology group $H^*(\overline{X}, \mathbb{Q}_\ell)$. We can define a cycle class map

$$c_j : \mathrm{Ch}^j(X) \to H^{2j}(\overline{X}, \mathbb{Q}_\ell(j))$$

where $\mathbb{Q}_\ell(j)$ is the Tate twist. In the codimension 1 case $j = 1$, we introduce the Néron–Severi group

$$\mathrm{NS}(X) = \frac{\text{divisors}}{\text{algebraic equivalence}} = \frac{\mathrm{Pic}(X)}{\mathrm{Pic}^0(X)}.$$

We can consider the Picard group as a group scheme $\underline{\mathrm{Pic}}^0 \to \underline{\mathrm{Pic}}$ (abelian varieties). There is an exact sequence

$$0 \to \mathrm{Pic}^0(X)(\overline{k}) \to \mathrm{Pic}(X)(\overline{k}) \to \mathrm{NS}(\overline{X})_G \to 0$$

where $G = \mathrm{Gal}(\overline{k}/k)$. If k is finite, then the injection $\mathrm{NS}(X) \to \mathrm{NS}(\overline{X})^G$ is an isomorphism, because of the exact sequence

$$\mathrm{NS}(X) \to \mathrm{NS}(\overline{X})^G \to H^1(k, \mathrm{Pic}^0(\overline{X})(k)) = 0.$$

As a group, $\mathrm{Pic}^0(X)(\overline{k})$ is divisible. We can consider the Kummer sequence on $\overline{X}$: for $p \nmid n$,

$$0 \to \mu \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 0.$$

We have

$$\begin{tikzcd} \mathrm{Pic}(\overline{X})/n \arrow[r, hook] \arrow[d, equal] & H^2(\overline{X}, \mu_n) \\ \mathrm{NS}(\overline{X})/n \arrow[ur] & \end{tikzcd}$$

Putting n to be ℓ^n and taking inverse limit,

$$\mathrm{NS}(\overline{X}) \otimes \mathbb{Z}_\ell \to H^2(\overline{X}, \mathbb{Z}_\ell(1))$$

where $\mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^n}$. This gives an *ad hoc* definition of cycle class map in terms of divisors.

With these objects, let us now go back to the study of algebraic cycles using cohomology. In fact we don't understand the kernel or the image of c_j! At least there is an upper bound for the image: it has to be Galois invariant. The conjecture of Tate says that

Conjecture 3.1 ($T_j(X)$)**.** *The cycle class map has image satisfying*

$$\mathbb{Q}_\ell\text{-}span\ of\ \mathrm{Im}(c_j) = H^{2j}(\overline{X}, \mathbb{Q}_\ell(1))^G.$$

This conjecture shouldn't be stated alone. For example, we want to know that two cycles that are linearly independent over $\mathbb{Q}$ remain so over $\mathbb{Q}_\ell$. For this we need to introduce more notations.

Let $V_j = H^{2j}(\overline{X}, \mathbb{Q}_\ell(j))$ which is a $\mathbb{Q}_\ell$-vector space, and $A_j = \mathrm{Im}(c_j) \subset V_j$ be the $\mathbb{Q}$-span of cycle classes. A relevant conjecture is

Conjecture 3.2 ($I_j(X)$)**.** *The map*

$$A_j \otimes \mathbb{Q}_\ell \to V_j$$

is injective.

A_j is the Chow group modulo ℓ-adic homological equivalence. We can consider numerical equivalence. For $d = \dim X$, we have a pairing $A_j \times A_{d-j} \to \mathbb{Q}$. We define the numerically trivial cycles to be

$$N_j = \{x \in A_j : (x, A_{d-j}) = 0\}.$$

Another relevant conjecture is

Conjecture 3.3 ($E_j(X)$)**.** *$N_j = 0$, i.e. homological equivalence is equivalent to numerical equivalence.*

Last time we saw that when k is finite (and hence $G = \langle \mathrm{Frob} \rangle$), the order of vanishing of L-function is given by the multiplicities of the eigenvalues of the Frobenius operator. For X/k, the zeta function is

$$\zeta(X, T) = \frac{P_1(T)P_3(T)\cdots P_{2g-1}(T)}{P_0(T)P_2(T)\cdots P_{2g}(T)}$$

where

$$P_{2j}(T) = \det(1 - T\,\mathrm{Frob}\,|H^{2j}(\overline{X}, \mathbb{Q}_\ell)).$$

Then we expect the order of pole to be given by

$$-\mathrm{ord}_{s=j}\,\zeta(X, q^{-s}) = \dim V_j^G.$$

The left hand side is just counting the number of q^{-j} that is equal to the eigenvalues, and is equal to the dimension of the generalized eigenspace $V_{j,(\mathrm{Frob}=1)} = \ker(\mathrm{Frob}-1)^M$ (for some sufficiently large M). The right hand side is $\ker(\mathrm{Frob}-1)$. These two spaces are equal precisely when the operator $\mathrm{Frob}-1$ is semisimple. We overlooked this issue last time!

Conjecture 3.4 ($S_j(X)$)**.** *The identity map induces an isomorphism between the Galois invariants and coinvariants*

$$V_j^G \xrightarrow{\cong} V_{j,G}.$$

Here semisimplicity is only partial. Clearly we can formulate a more general

Conjecture 3.5 ($SS_j(X)$)**.** *V_j is a semisimple G-module.*

Now we study the inter-relationship between the conjectures above.

Fix j. We simplify notations as $N \subset A \subset V = V_j$. We have $N' \subset A' \subset V' = V_{d-j}$ for the complementary dimension. Likewise we have the Conjectures T and T'. Recall the following facts from cohomology.

(1) Poincaré duality: V is dual to V'.
(2) Hard Lefschetz: There is a non-canonical isomorphism $V \xrightarrow{\simeq} V'$, depending on the choice of a hyperplane class.

Lemma 3.6. *Conjectures S and S' are equivalent. The four spaces V^G, V_G, $(V')^G$ and V'_G have the same dimension.*

Proof. This is trivial, since the dual map of $V^G \to V_G$ is precisely $(V')^G \to V'_G$. Hard Lefschetz gives non-canonical isomorphisms $V^G \cong (V')^G$ and $V_G \cong V'_G$, so all four spaces have the same dimension. □

Lemma 3.7.
(1) $E \Rightarrow I$.
(2) $T + E \Rightarrow T' + S$.

Proof. We will prove (2) assuming (1). (Without Conjecture I we don't even know A has finite $\mathbb{Q}$-dimension!)

Consider Tate's commutative diagram

$$\begin{tikzcd} A \otimes \mathbb{Q}_\ell \arrow[r, hook] \arrow[d] & (A' \otimes \mathbb{Q}_\ell)^* \\ V^G = (V'_G)^* \arrow[r] & ((V')^G)^* \arrow[u] \end{tikzcd}$$

By E, the top map is injective. T implies the left map is surjective, hence an isomorphism by I. Thus the bottom map is injective, hence bijective which proves $S' \Leftrightarrow S$. Finally, the right map is injective, which proves T'. □

The point here is that we get Conjecture S as an output.

Fact. E_1 holds (i.e. for divisors).

Hence T_1 implies $T_{d-1} + S_1$.

Theorem 3.8 (Tate)**.** *T_1 for abelian varieties over finite fields holds.*

Remark. If k is finite, then $S(X \times X) \Rightarrow SS(X)$. This can be proved by using Künneth decomposition $H^{2d} = \bigoplus_i H^i \otimes H^{2d-i}$ and Poincaré duality.

Thus Tate's theorem implies full semisimplicity SS for all abelian varieties, in the case of divisors.

Next time we will move to non-constant elliptic curves.

4. Lecture 4 (September 16, 2014)

Let's focus on the Tate conjecture for divisors, which is the case that is relevant to BSD over function fields. Let k be a finite field, and X be a smooth projective variety over k. Set $\overline{X} = X \times_k \overline{k}$ and $G = \mathrm{Gal}(\overline{k}/k)$. The Néron–Severi group $\mathrm{NS}(X)$ is a finitely generated abelian group. We have the inequality

$$\operatorname{rank} \mathrm{NS}(X) \le \operatorname{rank} H^2(\overline{X}, \mathbb{Q}_\ell(1))^G \le -\operatorname{ord}_{s=1} \zeta(X, q^{-s}).$$

The middle term $H^2(\overline{X}, \mathbb{Q}_\ell(1))^G$ is the eigenspace of q. The last term $-\operatorname{ord}_{s=1} \zeta(X, q^{-s})$ is the multiplicity of eigenvalue q, i.e. the rank of the generalized eigenspace of q.

Tate's conjecture T_1 states that the first equality holds. Conjecture S_1 states that the second equality holds.

The middle term corresponds to the Selmer rank. Recall from the first lecture: if E is an elliptic curve over a function field, then

$$r_{\mathrm{MW}} \leq r_\ell \leq \operatorname{ord} L(E,s).$$

The second equality holds if we have partial semisimplicity, from which the ℓ-independence of $r_\ell(E)$ also follows.

Theorem 4.1. *If $r_\ell(E) = 1$ for $\ell \gg 0$, then BSD for $E/k(C)$ holds.*

Today we will explain the proof of the equivalence between these conjectures and the finiteness of Ш. Suppose X is a surface over a finite field k. How can we formulate a BSD for X? For example, do we need the Néron–Tate height?

Conjecture 4.2 (Artin–Tate)**.**

(1) *Rank conjecture:*

$$\operatorname{rank} \mathrm{NS}(X) = \operatorname{rank} H^2(\overline{X}, \mathbb{Q}_\ell(1))^G = -\operatorname{ord}_{s=1} \zeta(X, q^{-s}).$$

(2) *Refined conjecture:*

$$\lim_{s\to 1} \frac{P_2(X, q^{-s})}{(1-q^{1-s})^{\mathrm{rank}}} = \#\operatorname{Br}(X) \cdot \operatorname{Reg}(X) \cdot q^{\alpha(X)}$$

where $\zeta(X,T) = \frac{P_1(T)P_3(T)}{P_0(T)P_2(T)P_4(T)}$, $\operatorname{Br}(X) = H^2(X, \mathbb{G}_m)$, *and* $\operatorname{Reg}(X) = \frac{\det\langle D_i, D_j\rangle}{[\mathrm{NS}(X):\bigoplus \mathbb{Z}D_i]^2}$ *for any basis $\{D_i\}$ of the torsion-free part of* $\mathrm{NS}(X)$.

There is no mention of Néron–Tate height, which is in some sense transcendental. In fact it can be defined using intersection pairing, and $q^{\alpha(X)}$ can be thought of as an intersection number. The Artin–Tate conjecture is somewhat more natural than BSD, and can be generalized to higher dimensions.

Today we will show that

$$\#\operatorname{Br}(X)_{\ell^\infty} < \infty \Rightarrow \text{Artin–Tate rank conjecture}$$

and next time we will show how the rank part implies the refined conjecture. In BSD refined, it is not clear why we believe in the form of the leading term, so the Artin–Tate conjecture provides some explanation. Let us begin with the

Lemma 4.3. *If k is finite, then* $\mathrm{NS}(X) = \mathrm{NS}(\overline{X})^G$ *and* $\mathrm{NS}(X) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong (\mathrm{NS}(\overline{X}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^G$.

Proof. We have the exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Pic}^0(\overline{X}) & \longrightarrow & \mathrm{Pic}(\overline{X}) & \longrightarrow & \mathrm{NS}(\overline{X}) & \longrightarrow & 0. \\ & & \| & & \| & & & & \\ & & \underline{\mathrm{Pic}}^0(X)(\overline{k}) & & \underline{\mathrm{Pic}}(X)(\overline{k}) & & & & \end{array}$$

So we get

$$\mathrm{NS}(X) \hookrightarrow \mathrm{NS}(\overline{X})^G \to H^1(k, \mathrm{Pic}^0(X))$$

where the last term is 0 by Lang's theorem. This is where we need the finiteness of k.

The proof of the second statement is similar. $\square$

Definition 4.4. Let A be an abelian group. The Tate module of A is

$$T_\ell A = \varprojlim A_{\ell^n}$$

where the projective system is given by $A_{\ell^{n+1}} \xrightarrow{\ell} A_{\ell^n}$. Alternatively, this can be defined as

$$T_\ell A = \varprojlim \operatorname{Hom}\left(\frac{1}{\ell^n}\mathbb{Z}/\mathbb{Z}, A\right) = \operatorname{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A) = \operatorname{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A_{\ell^\infty}).$$

The Tate module satisfies the following properties.

(1) If A_{ℓ^∞} is finite, then $T_\ell A = 0$.
(2) $T_\ell A$ is torsion-free. (Proof: Given $\varphi : \mathbb{Q}_\ell/\mathbb{Z}_\ell \to A$ with $\ell^n \varphi = 0$, for any $x \in \mathbb{Q}_\ell/\mathbb{Z}_\ell$ we have $\varphi(x) = \varphi(\ell^n y) = \ell^n \varphi(y) = 0$.)
(3) If $A \cong (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^r$, then $T_\ell A \cong \mathbb{Z}_\ell^r$.

Lemma 4.5. *If $\ell \neq \operatorname{char} k$, then*

$$0 \to \operatorname{NS}(X) \otimes \mathbb{Z}_\ell \to H^2(\overline{X}, \mathbb{Z}_\ell(1))^G \to T_\ell(\operatorname{Br}(X)) \to 0.$$

Proof. For $p \nmid n$, we can consider the Kummer sequence

$$0 \to \mu_n \to \mathbb{G}_m \xrightarrow{(n)} \mathbb{G}_m \to 0.$$

By Kummer theory, we get the short exact sequences

$$0 \to H^1(\overline{X}, \mathbb{G}_m)/n \to H^2(\overline{X}, \mu_n) \to H^2(\overline{X}, \mathbb{G}_m)_n \to 0$$

and

$$0 \to H^1(X, \mathbb{G}_m)/n \to H^2(X, \mu_n) \to H^2(X, \mathbb{G}_m)_n \to 0.$$

To compare the cohomology of X and $\overline{X}$, we use the Hochschild–Serre spectral sequence

$$H^i(k, H^j(\overline{X}, \mu_n)) \Rightarrow H^{i+j}(X, \mu_n).$$

For finite fields k, $G = \operatorname{Gal}(\overline{k}/k)$ has cohomological dimension 1. In fact,

$$H^i(k, M) = \begin{cases} 0 & \text{if } i \neq 0, 1, \\ M^G & \text{if } i = 0, \\ M_G & \text{if } i = 1. \end{cases}$$

The spectral sequence only has two columns, and we deduce that

$$0 \to H^{i-1}(\overline{X}, \mu_n)_G \to H^i(X, \mu_n) \to H^i(\overline{X}, \mu_n)^G \to 0.$$

Taking Galois invariants in the first sequence,

$$0 \to (H^1(\overline{X}, \mathbb{G}_m)/n)^G \to H^2(\overline{X}, \mu_n)^G \to H^2(\overline{X}, \mathbb{G}_m)_n^G$$

which fits into the diagram

$$
\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & (H^0(\overline{X},\mu_n)/n)_G \arrow[d] & H^1(X,\mathbb{G}_m)/n \arrow[r] \arrow[d] & (H^1(\overline{X},\mathbb{G}_m)/n)^G \arrow[d] & \\
0 \arrow[r] & H^1(\overline{X},\mu_n)_G \arrow[r] \arrow[d] & H^2(X,\mu_n) \arrow[r] \arrow[d] & H^2(\overline{X},\mu_n)^G \arrow[r] \arrow[d] & 0 \\
 & (H^1(\overline{X},\mathbb{G}_m)_n)_G \arrow[d] & \mathrm{Br}(X)_n \arrow[d] & H^2(\overline{X},\mathbb{G}_m)_n^G & \\
 & 0 & 0 & &
\end{tikzcd}
$$

We have $(H^0(\overline{X},\mu_n)/n)_G = \overline{k}^\times/n = 0$, so the map $H^1(\overline{X},\mu_n)_G \to H^1(\overline{X},\mathbb{G}_m)_n$ on the left is an isomorphism. Taking projective limit (which is exact on compact groups) for $n=\ell^m$ in the above diagram,

$$
\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & 0 \arrow[d] & \mathrm{Pic}(X)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d] & (\mathrm{NS}(\overline{X})\otimes\mathbb{Z}_\ell)^G \cong \mathrm{NS}(X)\otimes\mathbb{Z}_\ell \arrow[r] \arrow[d, "*"] & 0 \\
0 \arrow[r] & H^1(\overline{X},\mathbb{Z}_\ell(1))_G \arrow[r] \arrow[d, "\cong"] & H^2(X,\mathbb{Z}_\ell(1)) \arrow[r] \arrow[d] & H^2(\overline{X},\mathbb{Z}_\ell(1))^G \arrow[r] & 0 \\
 & (T_\ell(\mathrm{Pic}(\overline{X})))_G & T_\ell(\mathrm{Br}(X)) \arrow[d] & & \\
 & & 0 & &
\end{tikzcd}
$$

Here $T_\ell(\mathrm{Br}(X))$ is torsion-free, and $H^1(\overline{X},\mathbb{Z}_\ell(1))_G$ is finite. Since the weight is 1, we know $H^1(\overline{X},\mathbb{Q}_\ell(1))_G = 0$.

By the snake lemma, we have an exact sequence

$$0 \to (T_\ell(\mathrm{Pic}(\overline{X})))_G \to T_\ell(\mathrm{Br}(X)) \to \mathrm{coker}(*) \to 0.$$

Here $(T_\ell(\mathrm{Pic}(\overline{X})))_G \to T_\ell(\mathrm{Br}(X))$ is a map from a finite group into a torsion-free group, hence must be the zero map. Therefore we have shown

$$\mathrm{coker}(*) = T_\ell(\mathrm{Br}(X)). \qquad \square$$

Theorem 4.6. *Let $\ell \neq \mathrm{char}\, k$. The following are equivalent:*

(1) $\mathrm{Br}(X)_{\ell^\infty}$ *is finite;*

(2) $\mathrm{NS}(X)\otimes\mathbb{Z}_\ell \xrightarrow{\sim} H^2(\overline{X},\mathbb{Z}_\ell(1))^G$*;*

(2') T_1 *holds, i.e.* $\mathrm{NS}(X)\otimes\mathbb{Q}_\ell \xrightarrow{\sim} H^2(\overline{X},\mathbb{Q}_\ell(1))^G$*;*

(3) $\operatorname{rank} \mathrm{NS}(X) = \operatorname{rank} H^2(\overline{X}, \mathbb{Z}_\ell(1)))^G$;
(4) $\operatorname{rank} \mathrm{NS}(X) = -\operatorname{ord}_{s=1} \zeta(X, q^{-s})$.

If any of these holds, then the refined conjecture holds up to ℓ-adic units.

We will treat (4) and the refined conjecture next time.

Corollary 4.7. *If $\# \operatorname{Br}(X)_{\ell^\infty} < \infty$ for some $\ell \neq p$, then $\# \operatorname{Br}(X)_{\text{non-}p\text{-part}} < \infty$.*

Proof. In the equation

$$|\text{leading coefficient}|_\ell = |\operatorname{Br}(X)|_\ell \cdot |\operatorname{Reg}|_\ell,$$

the left hand side is independent of $\ell \neq p$, so $|\operatorname{Br}(X)|_\ell$ is finite for all $\ell \neq p$. □

5. Lecture 5 (September 18, 2014)

Last time we proved the unrefined Artin–Tate conjecture for a surface X over k under the assumption $\# \operatorname{Br}(X)_{\ell^\infty} < \infty$. Recall that for X we have the

- algebraic rank $r_{\mathrm{alg}} = \operatorname{rank} \mathrm{NS}(X)$ (which is the analogue of Mordell–Weil rank in higher dimensions);
- Selmer rank $r_\ell = \operatorname{rank} H^2(\overline{X}, \mathbb{Q}_\ell(1))^G$, where $G = \operatorname{Gal}(\overline{k}/k)$;
- analytic rank $r_{\mathrm{an}} = \operatorname{ord} \zeta(X, q^{-s})$.

They satisfy the inequality

$$r_{\mathrm{alg}} \leq r_\ell \leq r_{\mathrm{an}}$$

The first equality holds if Tate conjecture holds, and is equivalent to $\# \operatorname{Br}(X)_{\ell^\infty} < \infty$ for any one $\ell \nmid p$. The second inequality holds if semisimplicity holds.

By the work of Kato on Iwasawa theory, we have the analogous inequality for number fields

$$r_\ell \leq \text{order of } \ell\text{-adic } L\text{-function}$$

with equality if we have semisimplicity. But we can't say anything about the complex L-functions.

Today we will show how the rank conjecture implies the non-p-part of the refined conjecture using linear algebra. Assume $\# \operatorname{Br}(X)_{\ell^\infty} < \infty$. Then we will prove that

$$\lim_{s \to 1} \frac{P_2(X, q^{-s})}{(1 - q^{1-s})^{r_{\mathrm{alg}}}} \overset{\text{“non-}p\text{-part”}}{=} \# \operatorname{Br}(X) \cdot \operatorname{Reg}(X) \cdot q^{-\alpha(X)},$$

i.e. the two sides differ by a power of p. Here the regulator is defined as

$$\operatorname{Reg}(X) = \frac{\det(D_i, D_j)_{i,j}}{[\mathrm{NS}(X) : \bigoplus \mathbb{Z} D_i]^2}$$

for any choice of basis D_i of the torsion-free part of $\mathrm{NS}(X)$, with the intersection pairing $\mathrm{NS}(X) \times \mathrm{NS}(X) \to \mathbb{Z}$, and $\alpha(X)$ is given by

$$\alpha(X) = h^2(X, \mathcal{O}_X) - (h^1(X, \mathcal{O}_X) - \dim \operatorname{Pic}(X)) = \chi(\mathcal{O}_X) - 1 + \dim \operatorname{Pic}(X).$$

We will be doing linear algebra in the following setting. A map $f : A \to B$ of $\mathbb{Z}_\ell$-modules is called a quasi-isomorphism if its kernel and cokernel are both finite, in which case we define

$$z(f) = \frac{\# \ker(f)}{\# \operatorname{coker}(f)}.$$

This is similar to a Herbrand quotient. It satisfies the following properties.

(1) If $f : A \to B$ and $g : B \to C$ are quasi-isomorphisms, then so is $g \circ f$ and

$$z(g \circ f) = z(g)z(f).$$

(2) If $f : A \to B$ is a quasi-isomorphism of finitely generated $\mathbb{Z}_\ell$-modules with matrix (a_{ij}) on the torsion-free part, then

$$z(f) = \frac{1}{\det(a_{ij})} \cdot \frac{\#A_{\mathrm{tor}}}{\#B_{\mathrm{tor}}}.$$

Proof. We apply (1) to the composition $\begin{tikzcd} A \arrow[r, "f"'] \arrow[rr, bend left, "g"] & B \arrow[r, "f'"'] & B/B_{\mathrm{tor}} \end{tikzcd}$. We have

$$z(g) = \frac{\#\ker(g)}{\#\operatorname{coker}(g)} = \frac{\#A_{\mathrm{tor}}}{\#\operatorname{coker}(g)}$$

and

$$z(f') = \#B_{\mathrm{tor}}.$$

Dividing gives

$$z(f) = \frac{z(g)}{z(f')} = \frac{\#A_{\mathrm{tor}}}{\#B_{\mathrm{tor}}} \frac{1}{\operatorname{coker}(g)}$$

To equate $\operatorname{coker}(g) = B/(B_{\mathrm{tor}} + \operatorname{Im}(f))$ and $\det(a_{ij})$, we note that g factors through the torsion-free part of A. □

(3) Define the dual module of A to be $A^* = \operatorname{Hom}(A, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$. The map $f : A \to B$ is a quasi-isomorphism if and only if its adjoint $f^* : B^* \to A^*$ is a quasi-isomorphism, in which case $z(f)z(f^*) = 1$.

(4) Let A be a finitely generated $\mathbb{Z}_\ell$-module and $\theta : A \to A$. The map $f : \ker(\theta) \to \operatorname{coker}(\theta) = A/\operatorname{Im}(\theta)$ induced by the identity is a quasi-isomorphism if and only if

$$\det(T - \theta \otimes 1) = T^\rho R(T),$$

where $\theta \otimes 1 : A \otimes \mathbb{Q}_l \to A \otimes \mathbb{Q}_l$, $\rho = \operatorname{rank}\ker(\theta)$, and $R(0) \neq 0$, in which case $z(f) = |R(0)|_\ell$.

Proof. $\theta' : \operatorname{Im}(\theta) \to \operatorname{Im}(\theta)$ has characteristic polynomial $\det(T - \theta') = R(T)$. □

Let us return to the refined Artin–Tate conjecture. For the Tate conjecture, we deduced the refined conjecture using hard Lefschetz and Poincaré duality. For surfaces, we don't need hard Lefschetz because it simply gives $H^2 \simeq H^2$! Assume $\#\operatorname{Br}(X)_{\ell^\infty} < \infty$. We have

$$\begin{tikzcd} \mathrm{NS}(X) \otimes \mathbb{Z}_\ell \arrow[r] \arrow[d, "\simeq"] & \operatorname{Hom}(\mathrm{NS}(X), \mathbb{Z}_\ell) & \\ H^2(\overline{X}, \mathbb{Z}_\ell(1))^G \arrow[r] & H^2(\overline{X}, \mathbb{Z}_\ell(1))_G \arrow[r, "\simeq"] & \operatorname{Hom}(H^2(\overline{X}, \mu_{\ell^\infty})^G, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \end{tikzcd}$$

To complete the diagram, recall the following diagram from the last lecture

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & 0 \arrow[d] & \mathrm{Pic}(X)/m \arrow[r] \arrow[d] & (\mathrm{Pic}(\overline{X})/m)^G \arrow[d] & \\
0 \arrow[r] & H^1(\overline{X}, \mu_m)_G \arrow[r] \arrow[d, "\cong"] & H^2(X, \mu_m) \arrow[r] \arrow[d] & H^2(\overline{X}, \mu_m)^G \arrow[r] \arrow[d] & 0 \\
 & (\mathrm{Pic}(\overline{X})_m)_G & \mathrm{Br}(X)_m \arrow[d] & ? & \\
 & & 0 & &
\end{tikzcd}$$

Taking inductive limit (which is exact) for $m = \ell^n$, we get

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & 0 \arrow[r] \arrow[d] & \mathrm{NS}(X) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \arrow[r, "\alpha"] \arrow[d] \arrow[dr, "g"] & (\mathrm{NS}(\overline{X}) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell)^G \arrow[d, "\beta"] & \\
0 \arrow[r] & H^1(\overline{X}, \mu_{\ell^\infty})_G \arrow[r] \arrow[d, "\cong"] & H^2(X, \mu_{\ell^\infty}) \arrow[r] \arrow[d] & H^2(\overline{X}, \mu_{\ell^\infty})^G \arrow[r] \arrow[d] & 0 \\
 & (\mathrm{Pic}(\overline{X})_{\ell^\infty})_G & \mathrm{Br}(X)_{\ell^\infty} \arrow[d] & ? & \\
 & & 0 & &
\end{tikzcd}$$

where the map α becomes injective because tensoring with $\mathbb{Q}_l/\mathbb{Z}_l$ kills all torsion.

The first diagram now becomes

$$\begin{tikzcd}
\mathrm{NS}(X) \otimes \mathbb{Z}_\ell \arrow[r, "e"] \arrow[d, "h"', "\simeq"] & \mathrm{Hom}(\mathrm{NS}(X), \mathbb{Z}_\ell) \arrow[r, "\simeq"] & \mathrm{Hom}(\mathrm{NS}(X) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \\
H^2(\overline{X}, \mathbb{Z}_\ell(1))^G \arrow[r, "f"] & H^2(\overline{X}, \mathbb{Z}_\ell(1))_G \arrow[r, "\simeq"] & \mathrm{Hom}(H^2(\overline{X}, \mu_{\ell^\infty})^G, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \arrow[u, "g^*"']
\end{tikzcd}$$

The labeled maps are all quasi-isomorphisms, with

$$\begin{aligned}
z(e) &= \frac{|\det(D_i, D_j)|_\ell}{|\mathrm{NS}(X)_{l^\infty}|_\ell}, \\
z(h) &= 1, \\
z(f) &= \left| \lim_{s \to 1} \frac{P_2(X, q^{-s})}{(1 - q^{-s})^{\mathrm{rank}\,\mathrm{NS}(X)}} \right|_\ell, \\
z(g^*) &= z(g)^{-1}.
\end{aligned}$$

To compute $z(g)$, let's go back to the diagram

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] & \\
 & 0 \arrow[r] \arrow[d] & \mathrm{NS}(X)\otimes\mathbb{Q}_\ell/\mathbb{Z}_\ell \arrow[r, "\cong"] \arrow[d] \arrow[dr, "g"] & \mathrm{Im}(\alpha) \arrow[r] \arrow[d, "\beta|_{\mathrm{Im}(\alpha)}"] & 0 \\
0 \arrow[r] & H^1(\overline{X}, \mu_{\ell^\infty})_G \arrow[r] \arrow[d, "\cong"] & H^2(X, \mu_{\ell^\infty}) \arrow[r] \arrow[d] & H^2(\overline{X}, \mu_{\ell^\infty})^G \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & (\mathrm{Pic}(\overline{X})_{\ell^\infty})_G \arrow[r] \arrow[d] & \mathrm{Br}(X)_{\ell^\infty} \arrow[r] \arrow[d] & \mathrm{coker}(\beta|_{\mathrm{Im}(\alpha)}) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

where we have replaced the upper-right term $(\mathrm{NS}(\overline{X})\otimes\mathbb{Q}_\ell/\mathbb{Z}_\ell)^G$ by the image of α. The maps on the last row come from the snake lemma. We have the following

Lemma 5.1. $\#(\mathrm{Pic}(\overline{X})_{\ell^\infty})_G = \#\,\mathrm{NS}(X)_{\ell^\infty}$.

Therefore,

$$z(g^*) = z(g)^{-1} = \frac{\#\,\mathrm{NS}(X)_{\ell^\infty}}{\#\,\mathrm{Br}(X)_{\ell^\infty}}.$$

Putting all these together gives the refined conjecture.

For elliptic curves over number fields, we have $r_{\mathrm{alg}} \le r_\ell$ but $r_\ell \le r_{\mathrm{an}}$ is still unknown. We have the following results:

- Gross–Zagier, Kolyvagin: If $r_{\mathrm{an}} \le 1$, then BSD holds.
- Kato, Skinner–Urban, Zhang: If $r_\ell \le 1$ for an "ordinary, large" prime ℓ, then the ℓ-part of BSD holds.
- However, this is still not known: If $r_{\mathrm{alg}} = 0$, then BSD holds. This is equivalent to saying that the vanishing of L-function implies $r_{\mathrm{alg}} \ge 1$.

We have finished our discussion of BSD over function fields. Everything follows from the finiteness of Ш at one prime.