A "BSD-type" Conjecture of Mazur and Tate

Tony Feng

April 27, 2016

Contents

1 Overview

1.1 Vague form of the conjecture

Let E be an elliptic curve over $\mathbf{Q}$. I am going to describe a conjecture of Mazur and Tate which is in some sense a sequel of their investigation (together with Teitelbaum) of a "p-adic BSD conjecture". However, while this conjecture involves some ideas in the spirit of p-adic L-functions, it is of a completely different nature.

There will be an input integer M (whiich can be composite), which has some constraints coming from E but can be significantly varied even for any given E. We let $K_M := \mathbf{Q}(\mu_M)^+$ and

$$G_M := \mathrm{Gal}(K_M/\mathbf{Q}) \cong (\mathbf{Z}/M)^*/\{\pm 1\}. \tag{1.1}$$

The eventual conjecture will make a prediction of the form

$$[\text{"Mazur-Tate derivative" of } L(E,s) \text{ at } 1] \sim [\text{"discriminant of } E(\mathbf{Q})\text{"}] \tag{1.2}$$

Here the squiggle means equal up to some factors (such as $Ш(E)$.)

Explaining what we mean by the left and right hand sides will take up the rest of the talk, but this vague form highlights the similarity to BSD. However, we should at least say in what ambient object this comparison is taking place. First of all, the

"critical rank" at which the derivative is taken is *not* $\operatorname{rank} E(\mathbf{Q})$; depending on our choice of M it lies in the range

$$\operatorname{rank} E(\mathbf{Q}) \leq r \leq \operatorname{rank} E(\mathbf{Q}) + \#\{\text{places where } E \text{ has split multiplicative reduction}\}.$$

In particular, the conjecture gives information *beyond* the rank. We should remark that the "p-adic BSD conjecture" of Mazur-Tate-Teitelbaum already exhibits this intriguing phenomenon of reaching beyond the usual leading order.

Let $\mathbf{Z}[G_M]$ be the group algebra of G_M and $I \subset \mathbf{Z}[G_M]$ the augmentation ideal. Then the left side of (1.2) lives in I^r/I^{r+1}.

Obviously this mean that the right hand side of (1.2) is also in I^r/I^{r+1}, but we shall see that the discriminant of the pairing is naturally valued in some larger group.

2 The Mazur-Tate Derivative

2.1 General Outline

The "Mazur-Tate derivative" is not a literal derivative, but rather a kind of equivariant derivative. To motivate our construction, we recall that one interpretation of a p-adic L-functions is as an object that interpolates special values of the usual L-functions.

To describe this, we begin by considering the rational group ring $\mathbf{Z}[G_M]$. We seek to interpret an L-function as a "thing" that interpolates L-values:

$$\chi \mapsto L(E \otimes \chi, 1).$$

More precisely, we seek an element $\theta_{E,M} \in \mathbf{Q}[G_M]$ such that for all $\chi \in \widehat{G_M}$,

$$\chi(\theta_{E,M}) \sim L(E \otimes \chi, 1).$$

Why have we put a squiggle above instead of an equality? The value $L(E \otimes \chi, 1)$ can be transcendental, and the left side could only be algebraic. So what we'll actually seek is to interpolate is the "algebraic part" of $L(E \otimes \chi, 1)$.

$$\chi(\theta_{E,M}) \approx \frac{L(E \otimes \chi, 1)}{\Omega_E}$$

where Ω_E is a period making the ratio algebraic. (Ultimately this picture will have to be adjusted a tiny bit.)

We think of this $\theta_{E,M}$ as literally being our L-function. With this in hand, we can make sense of its "derivatives". For instance, we can say that $\theta_{E,M}$ "vanishes to order r" if $\theta_{E,M} \in I^r$, where I is the augmentation ideal of $\mathbf{Q}[G_M]$. You can think of this as the literal order of vanishing of $\theta_{E,M}$ at point of Spec $\mathbf{Q}[G_M]$ represented

by the trivial character. If $\theta_{E,M}$ vanishes to order r, then its "rth derivative" is the value of $\theta_{E,M}$ in I^r/I^{r+1}.

More generally, we can make sense of order of vanishing "at χ" for any character χ of G_M, and speak of its "rth dervative at χ" as the value in I_χ^r/I_χ^{r+1}.

Example 2.1. We will actually work not with the full rational group ring $\mathbf{Q}[G_M]$, but a finitely generated subring R which contains the coefficients of $\theta_{E,M}$.

To get a feeling for what kinds of objects these derivatves are, we consider some special cases. Pretend for now that $R = \mathbf{Z}$. For $r = 0$ we have $I^0/I^1 \cong \mathbf{Z}$. For $r = 1$ we have $I^1/I^2 \cong G_M$, thanks to the long exact sequence of group *homology* associated to $0 \to I \to \mathbf{Z}[G] \to \mathbf{Z} \to 0$:

$$0 = H_1(G, \mathbf{Z}[G]) \to H_1(G, \mathbf{Z}) \to H_0(G, I) \to H_0(G, \mathbf{Z}[G]) = 0$$

2.2 Twisted L-values

We said that we (roughly) wanted our element $\theta_{E,M}$ to interpolate $L(E \otimes \chi, 1)$. The correct result ends up being to take

$$\theta_{E,M} = \frac{1}{2} \sum_{a \mod M} \left[\frac{a}{M}\right]_E \sigma_a$$

where $\sigma_a \in G_M$ corresponds to $\zeta \mapsto \zeta^a$, and $\left[\frac{a}{M}\right]_E$ is the (positive) *modular symbol* associated to E; we will elaborate on this later.

We give a heuristic derivation of the expression to motivate where this comes from. The χ-twisted L-function of E is

$$L(E \otimes \chi, s) = \sum_{n=1}^{\infty} \frac{a_n \chi(n)}{n^s}$$

so we have

$$\begin{aligned}
L(E\otimes\chi,1) &= \sum_{n=1}^{\infty}\frac{a_n\chi(n)}{n}\\
&= \sum_{m \bmod M}\chi(m)\sum_{n\equiv m \bmod M}\frac{a_n}{n}\\
&= \sum_{m \bmod M}\chi(m)\sum_n\frac{a_n}{n}\left(\frac{1}{M}\sum_{a \bmod M}e^{2\pi ia(m-n)/M}\right)\\
&= \sum_{a \bmod M}\left(\frac{1}{M}\sum_{m \bmod M}\chi(m)e^{2\pi iam}\right)\sum_n\frac{a_n}{n}e^{-2\pi ian/M}\\
&= \frac{\tau(\chi)}{M}\sum_{a \bmod M}\overline{\chi}(a)\sum_n a_n\frac{e^{-2\pi ian/M}}{n}\\
&= \frac{\tau(\chi)}{M}\sum_{a \bmod M}\overline{\chi}(a)\sum_n a_n\left(2\pi i\int_{\infty}^{-a/M}e^{2\pi inz}\,dz\right)\\
&= \frac{\tau(\chi)}{M}\sum_{a \bmod M}\overline{\chi}(a)2\pi i\int_{\infty}^{-a/M}f(z)\,dz.
\end{aligned}$$

2.3 Modular symbols

The quantities

$$\int_{\infty}^{-a/M}f(z)\,dz.$$

obtained in the preceding calcluation are examples of *modular symbols*. In the weight 2 case, a modular symbol for the congruence subgroup Γ is simply a map

$$\mathrm{Hom}_{\Gamma}(\mathrm{Div}^0(\mathbf{P}^1(\mathbf{Q})),\mathbf{C})$$

where Γ acts by translation on $\mathrm{Div}^0(\mathbf{P}^1(\mathbf{Q}))$. For our purposes, we can think of a modular symbol as a combinatorial gadget that encodes L-values.

Example 2.2. For $f\in\mathcal{S}_2(\Gamma)$, we get a modular symbol given by

$$[a/M]-[\infty]\mapsto 2\pi i\int_{\infty}^{a/M}f(z)\,dz.$$

However, there are other kinds of modular symbols which don't come from cusp forms. (They are instead related to Eisenstein series.)

Let $E/\mathbf{Q}$ be an elliptic curve of conductor N. Attached to E we have a normalized cusp form f of level N, which induces a modular symbols as above. This is what we see appearing in the expression for $L(E\otimes\chi,1)$.

Now, if we consider the integrals

$$2\pi i \int_{\infty}^{a/M} f(z)\, dz$$

for all a/M in $\mathbf{Q}$ the values that appear will be special: they will form a *lattice* containing with finite index the lattice associated to E by complex uniformization of elliptic curves. (The latter lattice is what you get by integrating only over $\Gamma_0(N)$-equivalent cusps.)

Since E is in particular defined over $\mathbf{R}$, its lattice will have a special shape. It will be either a square lattice, or index 2 inside a square lattice. The usual normalization is to write

$$\Lambda_E = \{a\Omega_E^+ + bi\Omega_E^-\}$$

where either $a \equiv b \pmod 2$ or $a, b \in \mathbf{Z}$ (unrestricted). Here

$$\Omega_E^+ = \frac{1}{2}\int_{E(\mathbf{R})} |\omega|$$

where ω is the Néron form on E (so this is only a half-period when $E(\mathbf{R})$ has one connected component).

Therefore,

$$\int_{\infty}^{a/M} f(z)\, dz = \left[\frac{a}{M}\right]_E^+ \Omega_E^+ + \left[\frac{a}{M}\right]_E^- \Omega_E^- i$$

with $\left[\frac{a}{M}\right]_E^+$ and $\left[\frac{a}{M}\right]_E^-$ rational numbers. (There is some content here, which is that ω pulls back to $f(q)\frac{dq}{q}$ under the modular uniformization.)

Now, recall that in our computation of $L(E\otimes\chi, 1)$ we found a sum of the quantity

$$2\pi i \int_{\infty}^{a/M} f(z)\, dz$$

over all a mod M. We claim that this is real. The reason comes from the observation that $f(-\overline{z}) = \overline{f(z)}$, since $q = e^{2\pi i z}$ has this property and the Fourier expansion of f in q has real coefficients. So

$$\begin{aligned}
\overline{2\pi i \int_{i\infty}^{a/M} f(z)\, dz} &= -2\pi i \int_{i\infty}^{a/M} \overline{f(z)}\, d\overline{z} \\
&= -2\pi i \int_{i\infty}^{a/M} f(-\overline{z})\, d\overline{z} \\
&= -2\pi i \int_{-i\infty}^{a/M} f(-z)\, dz \\
&= 2\pi i \int_{\infty}^{-a/M} f(z)\, dz
\end{aligned}$$

Thanks to this, we can consider only the + part of the modular symbol, so from now one we define

$$\left[\frac{a}{M}\right] := \left[\frac{a}{M}\right]_+.$$

To sumarize, we have found that

$$L(E \otimes \chi, 1) = \frac{\tau(\chi)}{M} \sum_{a \mod M} \overline{\chi}(a) \left[\frac{a}{M}\right]_E \Omega_E^+.$$

Now, Mazur and Tate define the *modular element*

$$\boxed{\theta_{E,M} := \frac{1}{2} \sum_{a \mod M} \sigma_a \left[\frac{a}{M}\right].}$$

It turns out that this is slightly different than the object which interpolates $L(E \otimes \chi, 1)$; this element interpolates $\frac{\tau(\chi) L(E \otimes \overline{\chi}, 1)}{2\Omega_E^+}$.

Conjecture 2.3. *For every χ, the element $\theta_{E,M}$ vanishes to order at least*

$$\dim_{\mathbf{Q}} E(K_M)[\chi] \otimes \mathbf{Q}.$$

3 Height pairings via bi-extensions

We will now describe global pairings on $E(K)$ through the framework of *bi-extensions*. In this section we let A be an elliptic curve and B its dual elliptic curve. Of course $A = B = E$, but we adopt this notation for two reasons. The first is that the discussion can be extended to abelian varieties, and the second is that these will play *asymmetric* roles in the pairings, which we emphasize through this notation.

3.1 Motivation

The point of the bi-extension formalism is to provide a convenient setting for global pairings. The simplest global pairings (e.g. the Néron-Tate height pairing) is simply a sum of local height pairings, but we will consider more complicated types of pairings.

To illustrate the role of the bi-extensions, we'll imagine rephrasing the global pairings without them. Roughly speaking, we want to define a pairing on $A(K) \times B(K)$ where K is some global field. To do so, we consider each completion $A(K_v) \times B(K_v)$ and try to assign a local pairing value. However, to do so we'll have to make some additional choice, so that the value is not well-defined. The ambiguity in this choice is up to some group G_v. But we would find that when we sum up the local pairings, any global ambiguity in the choices cancels out because of a "product rule".

For reasons you can imagine, carrying around "not-well-defined local pairings" is unwieldy. Instead, we're going to replace this notion with a function on the space

of all possible choices, which forms a G_v-torsor over $A(K_v) \times B(K_v)$. Globally, this defines a function on some object bigger than $A(K) \times B(K)$, but then we can clealy talk about it descending.

3.2 Bi-extensions

Let us first discuss bi-extensions at the level of groups. Let A, B, G be three groups. Informally, a bi-extension is a "bilinear form valued in extensions". This is some set E with a G-action, such that for each $a \in A$ the fiber E_a over a has the structure of group making E_a an extension of B of G, and similarly for each $b \in B$. The extensions need to satisfy a bilinearity property:

$$E_{a_1+a_2,b} \cong E_{a_1,b} + E_{a_2,b}$$

where $E_{a_1,b} + E_{a_2,b}$ is the addition of extensions in the sense of groups, and some cocycle and compatibility conditions. Then a bi-extension of group schemes will be defined in the obvious way in terms of the functor of points. That is, an extension of $A \times B$ by G will be a G-torsor E over $A \times B$, which when considered as an A-scheme is an extension of B by G, and when considered as a B-scheme is an extension of A by G.

Example 3.1. The ur-example of a bi-extension is the Poincaré bundle $\mathcal{P}_A$ on $A \times B$ (viewed as a $\mathbf{G}_m$-torsor rather than a line bundle). The general definition is modelled on the properties of this example.

Definition 3.2. Let A, B, G be group schemes. A bi-extension of $A \times B$ by G is a G-torsor E over $A \times B$ with isomorphisms of torsors:

$$\alpha_{a_1,a_2;b} \colon E_{a_1+a_2,b} \xrightarrow{\sim} E_{a_1,b} + E_{a_2,b}$$
$$\beta_{a;b_1,b_2} \colon E_{a,b_1+b_2} \xrightarrow{\sim} E_{a,b_1} + E_{a,b_2}$$

satisfying certain cocycle and compatibility conditions.

Instead of describing these conditions in general, we do it in the special case of $G = \mathbf{G}_m$ where the language become more familiar. If $G = \mathbf{G}_m$, then by the equivalence between $\mathbf{G}_m$-torsors and line bundles we can also think of a bi-extension of $A \times B$ by G as a line bundle L on $A \times B$ with a bilinearity structure

$$\alpha_{a_1,a_2;b} \colon L_{a_1+a_2,b} \cong L_{a_1,b} \otimes L_{a_2,b}$$
$$\beta_{a;b_1,b_2} \colon L_{a,b_1+b_2} \cong L_{a,b_1} \otimes L_{a,b_2}$$

However, there should be some compatibility conditions. For $a_1, a_2, a_3 \in A$ we have several possible isomorphisms

$$L_{a_1+a_2+a_3,b} \cong L_{a_1,b} \otimes L_{a_2,b} \otimes L_{a_3,b}$$

by first combining $a_1 + a_2$ or $a_1 + a_3$ or $a_2 + a_3$; we demand that these should be the same.

Similarly, there two possible isomorphisms

$$L_{a_1+a_2,b_1+b_2} \cong L_{a_1,b_1} \otimes L_{a_1,b_2} \otimes L_{a_2,b_1} \otimes L_{a_2,b_2}$$

depending on whether we first apply α or β; we demand that these agree.

We remark that checking these conditions for abelian varieties amounts to checking that some line bundle on $A \times A \times B \times B$, etc. is trivial; which follows from results sometimes referred to as "rigidity" or the "Theorem of the Cube" or the "Theorem of the Square".

In the case of general G the story is essentially the same; one simply replaces the tensor product with the natural addition for extensions, which is a combination of pushout and pullback along the diagonal.

All of our bi-extensions will be obtained as modifications of the Poincaré bi-extension. We now go on to describe the technical meaning of "modification".

Definition 3.3. A *modification* of a bi-extension $E(K)$ of $A(K) \times B(K)$ by $G(K)$ is a tuple $(E', \alpha\colon P \to A, \beta\colon Q \to B, \rho\colon G(K) \to H)$ where

- $\alpha\colon P \to A(K)$ and $\beta\colon Q \to B(K)$ are group homomorphisms, and
- E' is a bi-extension of $P \times Q$ by H obtained by pushout of $E|_{P\times Q}$ along $\rho\colon G(K) \to H$.

$$\begin{array}{ccc} E|_{P\times Q} & \longrightarrow & P \times Q \\ \downarrow & & \downarrow{\scriptstyle \alpha\times\beta} \\ E & \longrightarrow & A \times B \end{array} \quad \rightsquigarrow E' = (E|_{P\times Q}) \times^{G,\rho} H.$$

3.3 Trivializations of of bi-extensions

We now define a "trivialization" of a modification of a bi-extension, which in the context of height pairings plays the role of the "not-well-defined local height pairing".

Definition 3.4. Keep the notation of Definition 3.3. A *trivialization* of E' is a map $\psi\colon E' \to H$ giving a bilinear splitting of the extensions. In other words, each E'_a is a group extension of $B(K)$ by H, so $\psi|_{E'_a}$ is a group homomorphism $E'_a \to H$; we demand that

$$\psi|_{E'_{a_1+a_2}} = \psi|_{E'_{a_1}} + \psi|_{E'_{a_2}}.$$

By the pushou property, a trivialization may be equivalently thought of as a map $\psi\colon E(K) \to H$ such that

$$\psi((a, b, c)) = \rho(c) + \psi(a, b)$$

and satisfying a similar bilinearity (which is the point of view we will adopt in discussing height pairings).

To reiterate, in the language without bi-extensions we would be describinga trivialization of a ρ-modification as a "pairing on $A(K) \times B(K)$ valued in H which is not quite well-defined." Namely, we declare $\langle a, b \rangle = \psi(e)$ where e lies over (a, b). This is ambiguous up to translating the fiber by some element of $g \in G$, which changes the result by $\rho(g)$.

3.4 Reformulation in terms of symbols

We give a parametrization of elements of $E(K)$ that will be more concrete to work with. Let $\mathrm{Pic}^0(A)$ be the space of divisors on A algebraically equivalent to 0.

We consider the set of triples $\{\mathfrak{a}, D, c\}$ where

1. $\mathfrak{a} = \sum n_x[x]$ is a zero-cycle on $A(K)$ of degree 0, i.e. $\sum n_x = 0$ (implicitly requiring that all but finitely many coefficients vanish.)
2. $D \in \mathrm{Div}^0(A)$ is a divisor (algebraically equivalent to 0) with disjoint support from $\mathfrak{a}$,
3. $c \in K^*$.

We then define a symbol $[\mathfrak{a}, D, c] \in E(K)$. This lies over $(a, b) \in A(K) \times B(K)$, where

$$a = s(\mathfrak{a}) := \sum n_x x \text{ (in the group law of } A(K))$$

and b is the line bundle corresponding to the divisor D. Furthermore, D describes a meromorphic section $\mathcal{O}(D)$ (the function 1) which gives a trivialization f of the fiber (up to scalar). The coordinate in this trivialization is $cf(\mathfrak{a})$, where

$$f(\mathfrak{a}) = \prod f(x)^{n_x}.$$

The scalar ambiguity is killed by the fact that $\mathfrak{a}$ has degree 0.

The properties of the symbol are the following:

1. $[\mathfrak{a}, D, c] = c + [\mathfrak{a}, D, 1]$,
2. $[\mathfrak{a}, D_1, 1] + [\mathfrak{a}, D_2, 1] = [\mathfrak{a}, D_1 + D_2, 1]$,
3. $[\mathfrak{a}_1, D, 1] + [\mathfrak{a}_2, D, 1] = [\mathfrak{a}_1 + \mathfrak{a}_2, D, 1]$,
4. $[\mathfrak{a}, (f), 1] = [\mathfrak{a}, 0, f(\mathfrak{a})]$.

These properties characterize the symbol $[\mathfrak{a}, D, c]$, because the difference of any two such symbols is

$$\delta(\mathfrak{a}, D, c) = [\mathfrak{a}, D, c]_1 - [\mathfrak{a}, D, c]_2 \in K^*$$

which as D varies glues to a map $A \to \mathbf{G}_m$, which is necessarily constant.

A bonus consequence of this is that

$$[\mathfrak{a}_a, D_a, c] = [\mathfrak{a}, D, c]$$

where the subscript a denotes translation by $a \in A(K)$, since this satisfies the same properties.

Reformulation of trivialization. We can now also reformulate the notion of trivializations in terms of these symbols. A trivialization will be a map

$$[\mathfrak{a}, D]_\psi := \psi([\mathfrak{a}, D, 1]).$$

The conditions that this satisfies are

1. $[\mathfrak{a}, D]_\psi$ is bi-additive,
2. $[\mathfrak{a}, (f)]_\psi = \rho(f(\mathfrak{a}))$,
3. $[\mathfrak{a}_a, D_a]_\psi = [\mathfrak{a}, D]_\psi$.

Conversely, any splitting can be obtained from this symbol by

$$\psi([\mathfrak{a}, D, c]) = \rho(c) + [\mathfrak{a}, D]_\psi.$$

3.5 Examples

Let K be a local field and $\mathcal{O} = \mathcal{O}_K$ is its ring of integers. If A is an abelian variety over K, then we denote by $\mathcal{A}$ its Néron model over $\mathcal{O}_K$ and $\mathcal{A}^0$ as its relative connected component. We have a filtration

$$A(K) \supset A^0(K) \supset A^1(K) \supset \dots$$

where $A^i(K)$ corresponds to the subset of $\mathcal{A}^0(\mathcal{O})$

$$A^i(K) \leftrightarrow \ker\left(\mathcal{A}(\mathcal{O}) \to \mathcal{A}(\mathcal{O}/\varpi^i)\right).$$

In the examples we will discuss, the trivialiations exist and are unique by generalities, but instead of proving this we will give explicit "geometric" descriptions of them.

3.5.1 The finite unramified trivialization

Let v be a finite place. We take $P = A(K)$ and $Q = B^0(K)$, and define

$$\psi([\mathfrak{a}, D]) = \deg(\mathfrak{a}' \cdot D')$$

where $\mathfrak{a}'$ and D' are interpreted as divisors on A whose generic fibers are $\mathfrak{a}$ and D, and such that for each component F_i of the special fiber $\mathcal{A}_k$ the degree $D' \cdot F_i = 0$ (this is the meaning of the condition $D \in B^0(K)$).

Proposition 3.5. *The pairing $-\log|\psi[\mathfrak{a}, D]|$ is the Néron-Tate pairing.*

Indeed, the latter is uniquely characterized by bilinearity, symmetry, $\langle \mathfrak{a}, (f)\rangle = \log|f(\mathfrak{a})|$, and a continuity property which we leave as an exercise.

Exercise 3.6. Check it.

3.5.2 The finite tamely ramified trivialization

We define a modification $(A(K), B^1(K), K^*/U^1)$ where

$$U^1 = \{x \in \mathcal{O}^* \colon x \equiv 1 \pmod{\mathfrak{m}_v}\}.$$

The target group is non-canonically isomorphic to$\mathbf{Z} \times \mathbf{F}_v^*$, where we can think of $\mathbf{Z}$ as being the same as in the previous case. The subgroup of K^*/U^1 having valuation 0, namely $\mathcal{O}^*/U^1$, does map isomorphically to $\mathbf{F}_v^*$, and here the $\mathbf{F}_v^*$ component is the canonical splitting of $E(k)$ (which exists by generalities).

This can be described more concretely in term of symbols as follows. For a pair $(\mathfrak{a}, D)$ having $\mathbf{Z}$-value 0 we choose $\mathfrak{a}', D'$ extending to the Néron model, as before. Then $D|_k$ is principal, say $(\overline{f})$ and we define the k^* component to be $\overline{f}(\overline{\mathfrak{a}})$.

3.5.3 The finite split multiplicative trivialization

We use a rigid-analytic uniformization of A and B by rigid-analytic tori. In the setting of elliptic curves that we are considering, the results can be stated in a very elementary manner in the language of Tate's curve, but because of the asymmetric roles of A and B we think it clearer to give the general formulation.

Let X and Y be the character group of the split tori A^0/k and B^0/k. Then we have uniformizations $T_X \twoheadrightarrow A$ and $T_Y \twoheadrightarrow B$ by rigid-analytic tori. We then have an embedding $Y \hookrightarrow T_X = X^* \otimes_{\mathbf{Z}} \mathbf{G}_m$ induced by the duality

$$X \times Y \to K^*$$

which fit into the short exact sequences

$$0 \to Y \to T_X \xrightarrow{\alpha} A \to 0$$

and

$$0 \to X \to T_Y \xrightarrow{\beta} B \to 0.$$

We will show that there is a unique splitting.

Remark 3.7. At the level of rigid analytic spaces, the uniqueness of the splitting follows from

$$\mathrm{Hom}(\mathbf{G}_m, \mathbf{G}_m) = \mathbf{Z}$$

and

$$\mathrm{Hom}(\mathbf{G}_m, \mathbf{Z}) = 0$$

in the rigid analytic category, so

$$\mathrm{Hom}(\mathbf{G}_m, \mathrm{Hom}(\mathbf{G}_m, \mathbf{G}_m)) = 0.$$

To construct the splitting we use theta functions. Recall that $E(K)$ could be represented by symbols $[\mathfrak{a}, D, c]$. We will parametrize $E'(K)$ by symbols $[\mathfrak{a}', \theta, c]$ where

1. $\mathfrak{a}' = \sum n_x[x]$ is a zero-cycle of degree 0 on $T_X(K)$,
2. θ is a meromorphic theta function on $T_X(K)$ such that for each y, the ratio $\frac{\theta(t+y)}{\theta(t)}$ is independent of t, and the divisor of θ is disjoint from $\mathfrak{a}'$.
3. $c \in K^*$.

Given such a datum, how can we get an element of $E'(K)$? We need to specify elements of $T_X(K) \times T_Y(K)$ and $E(K)$ that it lies over.

- We have $s(\mathfrak{a}') := \sum n_x x \in T_X(K)$.
- We have a function $u_\theta(y) := \frac{\theta(y+t)}{\theta(t)} \in T_Y(K) = \mathrm{Hom}(Y, K^*)$,
- We have the symbol $[\alpha(s(\mathfrak{a}')), \alpha \operatorname{Div} \theta, c] \in E(K)$.

There is an implicit claim here that we can arrange $\mathfrak{a}'$ to map to an arbitrary degree 0 zero-cycle on $A(K)$ and D_θ be an arbitrary divisor with disjoint support. We shall see this explicitly in an example soon.

In terms of this, the splitting is

$$\psi([\mathfrak{a}', \theta, c]) = c\theta(\mathfrak{a}').$$

What do we need to check in order to ensure that this is well-defined? First, suppose θ is replaced with another theta function θ' having the same cocycles. Then θ/θ' is invariant under translation, so descends to a meromorphic function on $A(K)$. From the rule

$$[\mathfrak{a}, D + (\phi), c] = [\mathfrak{a}, D, c\phi(\mathfrak{a})]$$

we deduce that

$$[\mathfrak{a}', \theta', c] = [\mathfrak{a}', \theta, c\frac{\theta_1(\mathfrak{a}')}{\theta(\mathfrak{a}')}] \text{ for } u_{\theta_1} = u_\theta.$$

Next suppose that we choose some $\mathfrak{a}''$ with the same sum as $\mathfrak{a}'$ in the group law. Then $\mathfrak{a}'' - \mathfrak{a}'$ is built out of zero-cycles of the form $\mathfrak{a}_t - \mathfrak{a}$, so it suffices to assume that $\mathfrak{a}'' - \mathfrak{a}'_t$. Then

$$[\mathfrak{a}'_t, \theta, c] = [\mathfrak{a}', \theta_{-t}, c] = [\mathfrak{a}', \theta, c\frac{\theta_{-t}(\mathfrak{a}')}{\theta(\mathfrak{a}')}] = [\mathfrak{a}', \theta, c\frac{\theta(\mathfrak{a}'_t)}{\theta(\mathfrak{a}')}].$$

Example 3.8. Write in terms of the usual Tate uniformization $T_X = T_Y = \mathbf{G}_m$ and $q \in K^* = \mathbf{G}_m(K)$ with $|q| < 1$. Then $Y = X = q^{\mathbf{Z}}$.

$$\begin{array}{ccc} E'(K) & \longrightarrow & K^* \times K^* \\ \downarrow & & \downarrow{\scriptstyle (\alpha,\beta)} \\ E(K) & \longrightarrow & A(K) \times B(K) \end{array}$$

The basic theta function, having zeros along $q^{\mathbf{Z}}$, is

$$\theta(t) = (1-t)\prod_{n=1}^{\infty}(1-q^n t)(1-q^n t^{-1}).$$

It is easily checked that

$$\theta(qt) = -t^{-1}q(t).$$

Let $\mathfrak{a}' = \sum m_i[a_i]$ and $\mathfrak{b}' = \sum n_j[b_j]$ be zero-cycles of degree 0 on K^* with images in $A(K) = B(K)$ having disjoint supports (which amounts to saying that no a_i/b_j is a power of q.) Let $\mathfrak{a} = \alpha(\mathfrak{a}')$ and $\mathfrak{b} = \beta(\mathfrak{b}')$. Then set

$$\theta_{\mathfrak{b}'} = \prod_j \theta\left(\frac{t}{b_j}\right)^{n_j}.$$

This has divisor $\beta^*\mathfrak{b}$, and satisfies

$$\theta_{\mathfrak{b}'}(qt) = s(\mathfrak{b}')\theta_{\mathfrak{b}'}(t).$$

Then we have a point $[\mathfrak{a}, \theta_{\mathfrak{b}'}, 1] \in E'(K)$.

So this represents $[\mathfrak{a}, \mathfrak{b}, 1] \in E(K)$ and $s(\mathfrak{a}') \times s(\mathfrak{b}')$ in $K^* \times K^*$. The splitting is then

$$\psi[\mathfrak{a}', \mathfrak{b}', 1] = \prod_{i,j} \theta(\frac{a_i}{b_j})^{m_i n_j}.$$

4 The global height pairing

4.1 The global pairing associated to a family of local trivializations

Let $A = E$ be an elliptic curve over a global field K and B its dual elliptic curve; let E/K be the universal $\mathbf{G}_m$-biextension of $A \times B$.

We are now ready to define the global pairing associated to a family of local trivializations $\delta = (\delta_v)$ consisting of

- $\alpha_v \colon A_v \to A(K_v)$,
- $\beta_v \colon B_v \to B(K_v)$,
- $\rho_v \colon K_v^* \to C_v$,
- $\psi_v \colon E_v \to C_v$

with almost all of them being the finite unramified local trivialization.

We define groups $A_\delta, B_\delta, C_\delta$ and a pairing

$$\langle \cdot, \cdot \rangle_\delta \colon A_\delta \times B_\delta \to C_\delta.$$

Basically each A_v is a modification of $A(K_v)$, and A_δ is obtained by putting these modifications together. The C_δ is basically the product of the local value groups, with a global product formula is enforced.

$$\begin{array}{ccc} A_\delta & \longrightarrow & A(K) \\ \downarrow & & \downarrow \prod i_v \\ \prod A_v & \xrightarrow[\alpha_v]{} & \prod A(K_v) \end{array} \qquad \begin{array}{ccc} B_\delta & \longrightarrow & B(K) \\ \downarrow & & \downarrow \prod i_v \\ \prod B_v & \xrightarrow[\beta_v]{} & \prod B(K_v) \end{array}$$

We can think of an element of A_δ as an element $A(K)$ together with (a_v) such that their images in each $A(K_v)$ agree, and similarly for B_δ. So we have a short exact sequence

$$0 \to \prod \ker \alpha_v \to A_\delta \to A(K) \to \prod \operatorname{coker} \alpha_v \to 0$$

and

$$0 \to \prod \ker \beta_v \to B_\delta \to B(K) \to \prod \operatorname{coker} \beta_v \to 0.$$

The value group C_δ is defined by the pushout diagram

$$\begin{array}{ccc} I = \prod K_v^* & \longrightarrow & \bigoplus C_v \\ \downarrow & & \downarrow \\ I/K^* & \longrightarrow & C_\delta \end{array}$$

so we have a product rule *by definition*

$$K^* \xrightarrow{\sum_v \rho_v \circ i_v} \bigoplus_v C_v \xrightarrow{\theta} C_\delta \to 0.$$

The pairing can then be defined as follows. Let $(P, (a_v)) \in A(K)$ and $(Q, (b_v)) \in B(K)$. Then choose some $e \in E(K)$ lying over (P, Q). Then $i_v(e)$ lives over $(i_v(P), i_v(Q))$ for each v.

$$\begin{array}{ccc} E_v & \longrightarrow & E(K_v) \\ \downarrow & & \downarrow \\ A_v \times B_v & \longrightarrow & A(K_v) \times B(K_v) \end{array}$$

We let $e_v \in E_v$ to be the point lying over $i_v(e)$ and (a_v, b_v). Then we define

$$\langle (P, (a_v)), (Q, (b_v)) \rangle = \theta(\sum_v \psi(e_v)).$$

We need to check that this is well-defined; the ambiguity is up to an element of $c \in K^*$, which is killed by *definition* in our value group C_δ.

4.2 S-pairings

Let S be a finite set of places of K and $S_m \subset S$ be the subset of places where A has split multiplicative reduction. We define a global pairing data δ_S as follows:

1. For archimedean v the $C_v = 0$ and α_v, β_v are identity,
2. For $v \notin S$, the pairing is the unramified one,
3. For $v \in S \setminus S_m$, the pairing is tamely ramified,
4. For $v \in S_m$, the pairing is the split multiplicative trivialization.

This defines a pairing

$$\langle \cdot, \cdot \rangle_S \colon A_S \times B_S \to C_S.$$

The target group C_S is $I/K^* \prod_v U_v$ where

$$U_v = \begin{cases} K_v^* & v \text{ archimedean}, \\ \mathcal{O}_v^* & v \text{ unramified}, \\ \mathcal{O}_v^1 & v \in S - S_m \\ 1 & v \in S_m \end{cases}$$

Note then that A_S and B_S are finitely generated of rank $r = \operatorname{rank} A(K) + \#S_m$.

In our case of interest $K = \mathbf{Q}$, the value group is

$$C_S = \left(\prod_{p \in S - S_m} \mathbf{F}_p^* \times \prod_{p \in S_m} \mathbf{Z}_p^* \right) / \{\pm 1\}.$$

4.3 Discriminant

We begin with a general discussion. If M, N are free $\mathbf{Z}$-modules of rank r then we can discriminant of a pairing

$$\langle \cdot, \cdot \rangle \colon M \times N \to R$$

valued in a commutative ring to be

$$\operatorname{disc} h := \det_{1 \le i,j \le r} h(P_i, Q_j)$$

which is a priori defined up to sign. If M, N are not free, then they have free submodules M' and N' of finite index and we define

$$\operatorname{disc} h = \frac{1}{[M : M'][N : N']} \operatorname{disc} h'$$

as long as the orders of the torsion subgroups are invertible in R (we will force this to be the case).

Definition 4.1. We define $\mathrm{disc}_S(E)$ to be the discriminant of the pairing

$$\langle \cdot, \cdot \rangle_S \colon A_S \times B_S \to R \otimes \mathrm{Sym}^{\bullet}_{\mathbf{Z}} C_S$$

in the above sense, where R is some subring of $\mathbf{Q}$ in which $\#E(K)_{\mathrm{tors}}$ is invertible.

This is well-defined up to sign. However, in the special setting of abelian varieties, one can remove this ambiguity. Given an orientation equivalence class of bases for $A(K) \otimes_{\mathbf{Q}} \mathbf{R}$, one can choose a polarization to get a bases for $B(K) \otimes \mathbf{R}$. But what happens for a difference choice of polarization? The key point is that if $\phi, \phi' \colon A \to B$ are two polarization defined over K then $\det \phi^{-1} \circ \phi'$ is positive.

To check this, it suffices to show that the characteristic polynomial of $\phi^{-1} \circ \phi$ acting on $T_\ell(A) \otimes \mathbf{Q}$ has positive roots. But this characteristic polynomial P has the property that $P(n) = \det(n + \phi^{-1}\phi')$, which by results of Mumford has the desired property.

4.4 Corrected discriminant

It turns out that we need to work not with disc_S but with a "corrected discriminant". The basic idea is to "average" in some way over the T-pairings for all $S_m \subset T \subset S$. It is unclear how to give a conceptual explanation for the need to average in this way. In a simplified setting (where enough things are invertible in our group ring), the corrected discriminant just multiplies by

$$\prod_{p \in S - S_m} (p - 1 - n_p)$$

where $n_p = \#B^0(\mathbf{F}_p)$.

5 Formulation of the conjecture

We now assemble these ingredients into a conjecture. Let $E/\mathbf{Q}$ be an elliptic curve, $A = E$ and $B = \widehat{E} = E$. Let S be a finite set of finite primes, and $S_m \subset S$ be the subset of primes where A has split multiplicative reduction.

For each $p \in S_m$ we choose an integer $e_p \geq 0$, and we set

$$M := \prod_{p \in S - S_m} p \prod_{p \in S_m} p^{e_p}$$

Then we have the modular element $\theta_{E,M} \in \mathbf{Z}[G_M]$. Let R be a subring of $\mathbf{Q}$ in which $\#A(\mathbf{Q})_{\mathrm{tors}}$ is invertible and the modular element is defined. We can consider $\theta_{E,M} \in I^r/I^{r+1}$ where

$$r = \mathrm{rank}\, E(\mathbf{Q}) + \#S_m.$$

Now for the right hand side, we have the S-pairing

$$A_S(K) \times B_S(K) \to C_S = \prod_{p \in S - S_m} \mathbf{F}_p^* \times \prod_{p \in S_m} \mathbf{Z}_p^* / \{\pm 1\}.$$

Then the discriminant

$$\mathrm{disc}_S(A) \in R \otimes \mathrm{Sym}^r C_S.$$

The map $C_S \twoheadrightarrow G_M \cong I/I^2$ induces a map

$$\eta_r \colon \mathrm{Sym}^r C_S \twoheadrightarrow I^r/I^{r+1}.$$

(We choose $C_S \to G_M$ to send $a \in (\mathbf{Z}/M)^*$ to the element σ_a.) Finally, let

$$\phi_{S_m} = \#\,\mathrm{coker}(B(\mathbf{Q}) \to \prod_{p \notin S_m} (B/B^0)(\mathbf{F}_p)).$$

Conjecture 5.1 (Mazur-Tate)**.** *We have*

$$\overline{\theta}_{E,M} = \#Ш(E) \cdot \phi_{S_m} \cdot \eta_r(\mathrm{disc}_S(A)) \in I^r/I^{r+1}.$$