Experimental Evidence on a Refined Conjecture of the BSD type

Francisco X. Portillo-Bobadilla

Universidad Autónoma de la Ciudad de México, Calzada Ermita
Iztapalapa No. 4163, Col. Lomas de Zaragoza, Iztapalapa,
México D.F., C.P. 09620. e-mail: francisco.portillo@uacm.edu.mx

August 8, 2018

Abstract

Let $E/Q$ be an elliptic curve of level $N$ and rank equal to 1. Let $p$ be a prime of ordinary reduction. We experimentally study conjecture 4 of B. Mazur and J. Tate in his article *Refined Conjectures of the Birch and Swinnerton-Dyer Type* [12]. We report the computational evidence.

**Keywords:** Number Theory, Rank 1 Elliptic Curves, $q$-adic Birch and Swinnerton-Dyer Conjecture, Mazur and Tate Conjecture, Experimental mathematics

**2010 Mathematics Subject Classification:** Primary 11Y40, Secondary 11Y35

1 Introduction

B. Mazur and J. Tate in *Refined Conjectures of the Birch and Swinnerton-Dyer Type* postulated a series of conjectures of the BSD-type in terms of finite layers. The goal was to find “functions with adelic type domains of definition and ranges of values” for which the $p$-adic $L$ functions were only a component, as expressed by Yuri Manin [9]. The Mazur and Tate conjecture (MT conjecture) is similar in spirit to the Birch and Swinnerton-Dyer conjecture (BSD conjecture). The conjecture has two assertion:
1. One that relates the rank of the elliptic curve with the order of vanishing of modular elements.

2. The other that gives an explicit formula that relates arithmetic invariants of the curve with the modular element modulo the \( r \)-power of an augmentation ideal. In this formula, we have:

   (a) On the Arithmetic side: invariants like the Tamawaga constant, the order of the torsion group, the order of the Tate-Shafarevich group as exponents of a bi-multiplicative function, called the corrected regulator.

   (b) On the Analytic side: the modular element, defined in terms of modular symbols, and which is an analogue of a Stickelberger element.

In the present work, we show computational evidence only related to the second assertion of the conjecture.

Our goal was to expand the evidence in favor of the conjecture (4) given by B. Mazur and J. Tate in [12]. In particular, they tested the conjecture for the elliptic curves 37A and 43A of rank 1 over sets \( S = \{q\} \), where \( q \) is a single prime of non split multiplicative reduction. They gave a very specific formula on those examples with prime conductor and group of Tate-Shafarevich trivial. We modify their equation so that any elliptic curve of rank 1 can be tested with no restrictions.

The change consist on introducing adequate exponents on each side of the equation, the exponents depend on invariants of BSD type as the mentioned above, and we also introduce a value \( \mu \) which is explained below. Hence, our contribution is to present a very concrete and easy to test conjecture and some computational evidence for it.

## 2 Mazur-Tate Conjecture (General Setting)

Assume \( E \) is an elliptic curve over \( \mathbb{Q} \) with conductor \( N \). Consider a Néron differential \( \omega \) for \( E \). Such \( \omega \) is unique up to sign. Let \( \Lambda_E \) be the Néron lattice (i.e. the lattice generated by the “periods” \( \int_\gamma \omega \in \mathbb{C} \), where \( \gamma \) runs through loops in \( E(\mathbb{C}) \)).

There is a unique pair of positive real numbers \( \Omega_E^+ \) and \( \Omega_E^- \) such that one of the two conditions holds:

1. \( \Lambda_E = \Omega_E^+ \mathbb{Z} + \Omega_E^- i \mathbb{Z} \)

2. \( \Lambda_E \subseteq \Omega_E^+ \mathbb{Z} + \Omega_E^- i \mathbb{Z} \) is the sub-lattice generated by the complex numbers \( a\Omega_E^+ + b\Omega_E^- i \) such that \( a - b \equiv 0 \pmod{2} \).
In the first case, we say that $\Lambda_E$ is rectangular, otherwise $\Lambda_E$ is non-rectangular.

Let $f$ be the modular form associated to $E$, and let $a/b$ be a rational number. We define the modular elements $[a/b]_E^+$ and $[a/b]_E^-$ by:

$$2\pi \int_0^\infty f(a/b + it)dt = \Omega_E^+[a/b]_E^+ + \Omega_E^-[a/b]_E^-i.$$  \hspace{0.5cm} (1)

We will write $[a/b]$ instead of $[a/b]_E^+$, since we will be concerned only with the plus symbols on $E$. The number $[a/b]$ is rational, and if $b$ is prime to the conductor of the curve, the value is an integer [7].

Let $S$ be a finite set of primes, let $S'$ be the subset of $S$ of primes with multiplicative reduction at a fixed elliptic curve $E$. Set

$$M = \prod_{p \in S-S'} p \prod_{p \in S'} p^{e_p}$$  \hspace{0.5cm} (2)

with integers $e_p \geq 0$, and set

$$G_M = (\mathbb{Z}/M\mathbb{Z})^*/(\pm 1)$$  \hspace{0.5cm} (3)

If $a$ is an integer coprime to $M$, let $\sigma_a$ denote its associated element in $G_M$.

Let $R$ be a subring of $\mathbb{Q}$ containing $1/2$ and $1$ over the order of the torsion of $E(\mathbb{Q})$. Define the modular element as

$$\Theta_{E,M} := \frac{1}{2} \sum_{a \text{mod}M} \left[ \frac{a}{M} \right] \cdot \sigma_a \in R[G_M]$$  \hspace{0.5cm} (4)

Let $\epsilon : R[G_M] \rightarrow R$ be the augmentation map, defined by

$$\sum r_i \sigma_a \rightarrow \sum r_i$$  \hspace{0.5cm} (5)

and let $I = \ker(\epsilon)$ its augmentation ideal.

Let $X$ be the Néron model of $E$, let $X(\mathbb{F}_p)$ be fiber of the Néron model of $E$ at $p$, let $X^0(\mathbb{F}_p) = E_{ns}(\mathbb{F}_p)$ be the non-singular points of $E$ modulo $p$ and let $N_p = X(\mathbb{F}_p)/X^0(\mathbb{F}_p)$ be the group of connected components in the fiber.

Define $\phi_S$ as the order of the cokernel of the natural projection:

$$\pi_S : E \rightarrow \prod_{p \notin S'} N_p$$  \hspace{0.5cm} (6)

as $q$ ranges through the set of all primes.

Conjecture 4 in [12] is the following:
Conjecture 2.1. ("Birch-Swinnerton-Dyer type" conjecture.)

Let \( r = \text{rank}(E(\mathbb{Q})) + \#(S') \). The modular element \( \Theta_{E,M} \in R[G_M] \) lies in the \( r \)-th power of the augmentation, \( I^r \subset R[G_M] \), and if \( \tilde{\Theta}_{E,M} \) denotes its image in \( I^r/I^{r+1} \):

\[
\tilde{\Theta}_{E,M} = \#(\mathcal{X}) \cdot \phi_S \cdot \nu_r(\text{Disc}_S(E)) \in I^r/I^{r+1} \tag{7}
\]

In the following pages, we explain the term \( \nu_r(\text{Disc}_S(E)) \).

2.1 Definition of \( \text{Disc}_S(E) \).

2.1.1 Local construction of the regulator

Using the theory of biextensions and splittings, Mazur and Tate introduce local canonical heights and corrected discriminants. We give a brief summary of their work to introduce regulators. For more details, see [11] and [12].

Definition 2.1. If \( A, B \) and \( C \) are abelian groups. A biextension of \( (A,B) \) by \( C \) is an object \( E \) such that for each triple \( (a,b,c) \in A \times B \times C \), we can assign a unique element \( [a,b,c] \in E \) such that \( aE := [a,B,C] \subseteq E \) has a group structure isomorphic to \( B \times C \); and analogously, \( bE := [A,b,C] \) has a group structure isomorphic to \( A \times C \). Also, \( C \) acts freely on \( E \).

Now, let \( \tilde{A}, \tilde{B} \) and \( \tilde{C} \) be other abelian groups. If \( \alpha : \tilde{A} \rightarrow A, \beta : \tilde{B} \rightarrow B \) are injective homomorphisms, and \( \rho : C \rightarrow \tilde{C} \) is a surjective homomorphism, we can obtain a biextension \( \tilde{E} \) given by the pullback of \( E \) by \( \alpha \) and \( \beta \), and the pushout of \( E \) by \( \rho \).

Definition 2.2. Let \( E \) be a biextension of \( (A,B) \) by \( C \), and \( \rho : C \rightarrow \tilde{C} \) a group homomorphism. A \( \rho \)-splitting of \( E \) is a map

\[
\psi : E \rightarrow \tilde{C}
\]

such that

1. \( \psi(\omega \cdot x) = \rho(\omega) \cdot \psi(x) \) for \( x \in E \) and \( w \in C \).
2. \( \psi|_{aE} \) and \( \psi|_{bE} \) are group homomorphisms.

If \( A \) and \( B \) are dual varieties over a field \( K \), we know that there exists a biextension \( E \) of \( (A,B) \) by \( K^* \) that expresses the duality [5]. Denote this biextension by \( E(K) \).

Definition 2.3. A modification \( (\tilde{E}, \alpha, \beta, \rho) \) of \( E(K) \) is a biextension \( \tilde{E} \) obtained by injective homomorphisms \( \alpha : \tilde{A} \rightarrow A(K) \), \( \beta : \tilde{B} \rightarrow B(K) \); and a surjective homomorphism \( \rho : K^* \rightarrow \tilde{C} \).
Definition 2.4. A trivialization $(\alpha, \beta, \rho, \psi)$ of $\mathcal{E}(K)$ is a modification $(\tilde{\mathcal{E}}, \alpha, \beta, \rho)$ of $\mathcal{E}(K)$ and a $\rho$-splitting $\psi$ of $\tilde{\mathcal{E}}$.

Notice that if $\alpha : \tilde{A} \to A(K)$, $\beta : \tilde{B} \to B(K)$ and $\rho : K^* \to C$ are group homomorphism as above, and $(\tilde{\mathcal{E}}, \alpha, \beta, \rho)$ is the associated modification, we have a bi-multiplicative function

$$\langle , \rangle_{\tilde{\mathcal{E}}} : \tilde{A} \times \tilde{B} \to \tilde{C}$$

defined by

$$\langle \tilde{a}, \tilde{b} \rangle_{\tilde{\mathcal{E}}} : = \rho \left( \langle \alpha(\tilde{a}), \beta(\tilde{b}) \rangle_{\mathcal{E}} \right) \quad (\forall \tilde{a} \in \tilde{A} \text{ and } \forall \tilde{b} \in \tilde{B}).$$

Here, $(\ , , )_{\mathcal{E}} : A \times B \to K^*$ is the bilinear pairing that express the duality.

If we define $\tilde{\psi} : \tilde{\mathcal{E}} \to \tilde{C}$ as

$$\tilde{\psi} \left( [\tilde{a}, \tilde{b}, \tilde{c}] \right) : = \tilde{c} : \langle \tilde{a}, \tilde{b} \rangle_{\tilde{\mathcal{E}}},$$

thus $\tilde{\psi}$ is a $\rho$-splitting of $\tilde{\mathcal{E}}$. And therefore, $(\tilde{\mathcal{E}}, \alpha, \beta, \rho)$ is a trivialization of $\mathcal{E}(K)$.

Working over local fields, Mazur and Tate [12] described what they called “the canonical trivilizations”. From now on, we will assume that our local fields are the fields $\mathbb{Q}_p$ for $p$ a prime number, that our global field is $K = \mathbb{Q}$, that $A = E$ is an elliptic curve and $B = E^\vee$ is its dual variety. Also, for each prime $p$, we will consider a system of group homomorphisms:

$$\alpha_p : A_p \to E(\mathbb{Q}_p),$$
$$\beta_p : B_p \to E(\mathbb{Q}_p),$$
$$\rho_p : \mathbb{Q}_p^* \to C_p,$$

where $\alpha_p$ and $\beta_p$ are injective and $\rho_p$ is surjective.

Hence, we will have modifications $(\alpha_p, \beta_p, \rho_p)$ with their corresponding $\rho_p$-splittings. For the purpose of this article, we are interested in the following three trivializations:

a) Néron unramified trivialization. Let $A_p = E(\mathbb{Q}_p)$, $B_p = E^0(\mathbb{Q}_p)$ and $C_p = \mathbb{Q}_p^*/\mathbb{Z}_p^* \simeq \mathbb{Z}$. Here, $E^0(\mathbb{Q}_p)$ denotes the group of points in $E(\mathbb{Z}_p)$ whose reduction modulo $p$ is in the component of zero in the fiber $E(\mathbb{F}_p)$. The homomorphisms $\alpha_p$ and $\beta_p$ are the natural inclusions; $\rho_p : \mathbb{Q}_p^* \to \mathbb{Q}_p^*/\mathbb{Z}_p^*$ is the natural projection. Now, $\psi_p : \mathcal{E}_p \to \mathbb{Q}_p^*/\mathbb{Z}_p^*$ is the only canonical splitting such that $\psi(\mathcal{E}_p(\mathbb{Z}_p)) = 0$.

b) Tamely ramified trivialization. Let $A_p = E(\mathbb{Q}_p)$, $B_p = E^1(\mathbb{Q}_p)$, $C_p = \mathbb{Q}_p^*/p\mathbb{Z}_p^* \simeq \mathbb{F}_p^*$. The maps $\alpha_p$ and $\beta_p$ are the inclusions again and $\rho_p$ is the projection. Now, $E^1(\mathbb{Q}_p)$ are the points in $E(\mathbb{Q}_p)$ whose reduction modulo $p$ is zero in the connected component of zero in the fiber $E(\mathbb{F}_p)$.
c) **Split Multiplicative trivialization.** If \( p \) is a prime of split multiplicative reduction, then \( E(\mathbb{Q}_p) \) is isomorphic to the Tate curve \( E_{q_p} = \mathbb{Q}_p^*/q_p^\mathbb{Z} \), where \( q_p \) is the multiplicative local period. Hence, in this trivialization, we take \( A_p = B_p = \mathbb{Q}_p^* \) and \( C_p = \mathbb{Q}_p^* \). And, \( \beta_p = \alpha_p : \mathbb{Q}_p^* \to \mathbb{Q}_p^*/q_p^\mathbb{Z} \) is the natural parametrization of \( E_{q_p} \), and \( \rho_p : \mathbb{Q}_p^* \to C_p = \mathbb{Q}_p^* \) is the identity.

### 2.1.2 Global Construction of Regulator

For the finite set \( S \) (See section 2.), we will construct extended Mordel groups \( A_S, B_S \) and \( C_S \) as follows:

According to subsection 2.1.1, for each subset of primes \( S \subseteq \wp \), there is a system of homomorphisms

\[
\alpha_p : A_p \to E(\mathbb{Q}_p), \\
\beta_p : B_p \to E(\mathbb{Q}_p), \\
\rho_p : \mathbb{Q}_p^* \to C_p,
\]

with their corresponding trivializations

\[
\psi_p : \tilde{E}_p \to C_p.
\]

The trivialization \( \psi_p \) is determined by the rule:

a) \( \psi_p \) is the Néron unramified trivialization, if \( s \notin S \).

b) \( \psi_p \) is the Tamely ramified trivialization, if \( s \in S - S' \).

c) \( \psi_p \) is the Split Multiplicative trivialization, if \( s \in S' \).

We define \( A_S \) to be the set of pairs \( (P, (a_p)) \) such \( P \in E(\mathbb{Q}) \), \( (a_p) \in \prod_{p \in \wp} A_p \) and \( \alpha_p(a_p) = i_p(P) \) for all prime \( p \), where \( i_p : A(\mathbb{Q}) \to E(\mathbb{Q}_p) \) is the canonical inclusion. We define \( B_S \), similarly.

Now, from the 3 possibilities of local trivializations, we can write \( C_p = \mathbb{Q}_p^*/U_p \), where \( U_p \) could be either \( \mathbb{Z}_p^* \), \( p\mathbb{Z}_p^* \) or \( \{1\} \).

Hence, we have a morphism

\[
\rho := (\rho_p) : \prod_{p \in \wp} \mathbb{Q}_p^* \to \bigoplus_{p \in \wp} (\mathbb{Q}_p^*/U_p).
\]

Now, if we mod out by \( \mathbb{Q}_p^* \) using the natural inclusions \( \mathbb{Q}_p^* \hookrightarrow \mathbb{Q}_p^* \), define:

\[
C_S := \prod_{p \in \wp} \mathbb{Q}_p^*/\mathbb{Q}_p^*(\prod_{p \in \wp} U_p). \tag{8}
\]
Set
\[ \phi : \bigoplus_{p \in \mathcal{P}} C_p \to C_S, \]
the natural map given by coordinates.

For \( a = (P, (a_p)) \in A_S \) and \( b = (Q, (b_p)) \in B_S \), define the bimultiplicative pairing by
\[ \langle a, b \rangle_S := \phi \left( \prod_p \psi_p(x_p) \right) = \prod_p \phi \circ \psi_p(x_p), \tag{9} \]
where \( x_p = [a_p, b_p, k] \in \tilde{E}_p \).

Notice \( A_p = E(\mathbb{Q}_p) \) and \( B_p = E^0(\mathbb{Q}_p) \) for almost all \( p \), and since \( P \in A(\mathbb{Z}_p) \) and \( Q \in B(\mathbb{Z}_p) \) for almost all \( p \), we have that \( \psi_p(x_p) = 1 \) for almost all \( p \).

Hence, the global bi-multiplicative function is computed as a finite product.

In fact, in our example, we have
\[ C_S := \left( \prod_{p \in S - S'} \mathbb{F}_p^* \times \prod_{p \in S'} \mathbb{Z}_p^* \right) / (\pm 1). \tag{10} \]

Now, \( A_S \) and \( B_S \) are finitely generated groups of the same rank:
\[ r = \text{rank}(A(K)) + \#(S') \cdot \dim(A). \]
(Reference: [12].)

Hence, if \( \{P_1, P_2, \ldots, P_r\} \) generates the free part of \( A_S \) and \( \{Q_1, Q_2, \ldots, Q_r\} \) generates the free part of \( B_S \), set
\[ \text{disc}_S = \det_{1 \leq i, j \leq r} \langle P_i, Q_j \rangle. \]

The value \( \text{disc}_S \) is well defined up to sign. But, we can choose an adequate orientation for our purposes.

Now, for our computations, it is useful to work on a subring \( R \subset \mathbb{Q} \) containing the torsion of \( A_S \) and \( B_S \). Hence, we will consider the element
\[ d_S := 1 \otimes \text{disc}_S \in R \otimes \text{Sym}_r(C_S). \]

This discriminant does not work well as the regulator, see the heuristic discussion about it in [12].

Instead, the corrected discriminant is defined as a sum of discriminants \( d_T \) over subsets \( T \subset S \) containing \( S' \).

For any subset \( T \subset S \), we have natural mappings: \( x_{S,T} : A_S \to A_T \), \( y_{S,T} : B_S \to B_T \) and \( z_{T,S} : C_T \to C_S \).
There is also a unique map $\mu_{S,T} : C_S \to C_T$, such that

$$\mu_{S,T} \circ z_{T,S} = \prod_{p \in S - T} (p - 1) \cdot c \text{ for all } c \in C_S$$

Thus, the \textit{corrected discriminant} of $S$ is defined as:

$$\text{Disc}_S(A) = \sum_{S' \subset T \subset S} (-1)^{#(T - S')} \mu_{S,T}(j_T \cdot d_T) \in R \otimes \text{Sym}_r(C_S), \quad (11)$$

where $j_T = (\prod_{p \in S - S'} n_p)/(B_{S'} : B_S)$, $n_p = #B^0(\mathbb{Q}_p)$, and $(B_{S'} : B_S)$ is the index of $B_S$ in $B_{S'}$.

Now, from equation (10) there is a natural surjective homomorphism $C_S \twoheadrightarrow G_M$. And, also a natural identification of $G_M$ with $I^2/I$ (as is described in next section). Thus, we have a natural map $C_S \to I^2/I$, which induces a natural homomorphism:

$$\nu_r : R \otimes \text{Sym}_r(C_S) \to I^{r+1}/I^r \quad (12)$$

Now, we should notice that the formula in Conjecture 2.1 occurs in $I^{r+1}/I^r$, and thus, the analogous of the regulator is $\nu_r(\text{Disc}_S(A))$.

### 3 MT Conjecture (Rank 1, Ordinary and Good Reduction Setting)

#### 3.1 The Analytic Side

In this section, we assume that $E$ has rank 1 and that $S$ has only primes of ordinary reduction. In this context, Conjecture 2.1 in section 2 states that

a) $\Theta_{E,M} \in I$

b) $\tilde{\Theta}_{E,M} = #(\text{III}) \cdot \phi_{S_m} \cdot \nu_r(\text{Disc}_S(E)) \in I/I^2$

Now, assertion a) is equivalent to have $\epsilon(\Theta_{E,M}) = 0$, or equivalently

$$\sum_{a \mod M} \left[ \frac{a}{M} \right] = 0. \quad (13)$$

Hence, we have

$$\Theta_{E,M} = \frac{1}{2} \sum_{a \mod M} \left[ \frac{a}{M} \right] \cdot (\sigma_a - \epsilon) \in R[G_M] \quad (14)$$
where $e$ is the identity on $G_M$.

The Hurewicz Theorem for augmentation ideals gives an isomorphism of abelian groups $G_M \simeq I/I^2$ given by the map $r(g - e) \mapsto g^r$ for $g \in G$ and $r \in \mathbb{Z}$. Hence, we will test assertion b) of the Conjecture directly on the group:

$$G_M = \left( \prod_{p \in S} \mathbb{F}_p^*/\pm 1 \right).$$

Since we cannot compute always square roots in $\mathbb{F}_p^*$, we will test the conjecture for the square of $\tilde{\Theta}_{E,M}$, which is equivalent to eliminate the $\frac{1}{2}$ on $\Theta_{E,M}$. Conjecture 2.1 is additive, but our testing will be multiplicative.

**Definition 3.1.** For $S$ having only primes of good reduction and an elliptic curve $E$ with rank$(E) \geq 1$, we define the following multiplicative modular element:

$$l(S) = \prod_{a \in (\mathbb{Z}/M\mathbb{Z})^*} a^{[a/M]} \pmod{M} \quad (15)$$

with $M = \prod_{p \in S} p$.

The values $[a/M]$ are integers if $\gcd(M,N) = 1$ by 5.4 in [7], so the multiplicative modular element is well defined.

### 3.2 The Arithmetic side

In this section, we also assume that $E$ is an elliptic curve with positive rank. First, assume $p$ is a prime of good reduction and $S = \{p\}$. In this case, we will describe how to compute $\text{Disc}_S(E)$.

An element $x \in \mathcal{E}_p$, can also be described by a triplet $x = [a, D, c]$, where $a = \sum_i n_i(P_i)$ is a zero cycle with $P_i \in E(\mathbb{Q}_p)$, $D = \sum_j m_j(Q_j)$ is a divisor in $E^0(\mathbb{Q}_p)$ algebraically equivalent to zero whose support is disjoint to $a$, and $c \in \mathbb{Q}_p^*$ [12] and [14].

Now, this symbol satisfies the properties:

a) $[a, \text{div}(f), 1] = [a, 0, f(a)]$ for a rational function $f$ defined on $E(\mathbb{Q}_p)$ with $f(a) = \prod_j f(Q_j)^{m_j}$.

b) $[a_R, D_R, c] = [a, D, c]$, where $a_R$ (resp. $D_R$) is obtained from $a$ (resp. $D$) by translating each point by $R$.

Now, since $E$ is an elliptic curve, we identify a point $P \in E$, with the zero cycle $(P) - (O)$. Hence, the discriminant is

$$\text{Disc}_{(p)}(E) = \psi_p([(P) - (O), (O) - (Q_p), 1]) \quad (16)$$
where $P$ is a generator of $E(Q)$, $Q$ is a generator of $E^0(Q)$, and $Q_p = n_p Q$.

Notice that the element $[(P) - (O), (O) - (Q_p), 1]$ is above $E(Q_p) \times E^1(Q_p)$ on the biextension $\mathcal{E}_p$.

Now, the value $\psi_p([a, D, 1])$ coincides with the Néron’s symbol $(D, a)_{vp}$ for the $p$-adic valuation in $\mathbb{Q}_p$. In particular, Theorem 3 in [14] says how to compute $(D, a)_{vp}$ if $D$ is equivalent to $O$.

To compute $\text{Disc}_{(p)}(E)$ is helpful to use property 2) above, translating by a point $P'$. Hence,

$$\text{Disc}_{(p)}(E) = \psi_p([(P + P') - (P'), (P') - (Q_p + P'), 1]) \quad (17)$$

This value is the $g$ function defined by Mazur and Tate in page 747 of [12]: Let $P$, $Q$ and $P'$ be as above. For $p \nmid N$ prime, consider the quantity:

$$g(P, Q, P', P) = \frac{d(P' + P) d(P' + Q_p)}{d(P') d(P' + P + Q_p)} \pmod{p} \quad (18)$$

where $d(T)$ is the square root of the denominator of the $x$-coordinate of a point $T$.

We will consider the square of this $g$ function, just assuming that $d(T)$ is the $x$-coordinate of $T$. This will balance the cancellation of the $\frac{1}{2}$ in $\Theta_{E,M}$, and it is in concordance with definition [3,1].

We summarize the properties of the $g$ function in the following proposition:

**Proposition 3.1.**

1. If $P \in E(Q)$, $Q \in E^0(Q)$, then $g(P, Q, P', p)$ does not depend on $P'$. Moreover, if $P$ is a generator of the free part of $E(Q)$ and $Q$ is a generator of the free part of $E^0(Q)$, then this value depends only on $E$ and $p$.

2. The function

$$\hat{g} : E \times E_0 \to \coprod_{p \mid N} \mathbb{F}_p^*,$$

defined by

$$\hat{g}(P, Q)_p := g(P, Q, P', p) \text{ at the } p \text{ coordinate}$$

is bi-multiplicative.

Now, let $S$ be a finite set of primes having only good reduction at $E$. Set $M = \prod_{p \in S} p, \ n_S = \prod_{p \in S} n_p$ and $Q_S = n_S Q$. If $P$ and $Q$ are generators of the free part of $E$, define

$$g(S) = \frac{d(P' + P) d(P' + Q_S)}{d(P') d(P' + P + Q_S)} \pmod{M} \quad (19)$$
where \(P'\) is a point on \(E\) such than non of the \(d's\) is zero.

Now, if \(M' \mid M\), let

\[
Y_{M',M} : (\mathbb{Z}/M'\mathbb{Z})^* \to (\mathbb{Z}/M\mathbb{Z})^*
\]

be the map defined by \(a \mapsto b^{\phi(M/M')}\), where \(a \in (\mathbb{Z}/M'\mathbb{Z})^*\) and \(b \in (\mathbb{Z}/M\mathbb{Z})^*\) such that \(a \equiv b \pmod{M'}\), and \(\phi\) is the Euler phi.

**Definition 3.2.** The \(G\) function on \(S\) is

\[
G(S) := \prod_{T \subseteq S} Y_{M_T,M} \left( g(P, Q_T, M_T) \right)^{(-1)^{1+\#(T)}}
\]

where \(M_T = \prod_{q \in T} q\), \(n_T = \prod_{p \in T} n_p\) and \(Q_T = n_TQ\).

### 3.3 Multiplicative Equations of Mazur-Tate Conjecture

Assume \(E\) is an elliptic curve of rank 1. Let \(E_0\) be the group of everywhere good reduction points of \(E\).

First, assume \(S\) has only points of ordinary reduction (i.e. \(S' = \emptyset\)). Therefore, \(\phi_S\) is the cokernel of the natural projection:

\[
\pi_S : E \to \prod_{p \in \wp} N_p
\]

where \(p\) ranges through the set of all primes \(\wp\).

The kernel of \(\pi_S\) is \(E_0\). Hence, the induced map

\[
E/E_0 \hookrightarrow \prod_{p \in \wp} N_p
\]

is an injection of finite groups and its cokernel is the cokernel of \(\pi_S\). Hence,

\[
\phi_S = \frac{C}{\#(E/E_0)},
\]

where \(C = \# \left( \prod_{p \in \wp} N_p \right) = \prod_{p \in \wp} c_p\) and \(c_p = |N_p|\) are the Tamagawa numbers.

If \(S' \neq \emptyset\), then we divide by \(C' = \prod_{p \in S'} c_p\), to obtain

\[
\phi_S = \frac{C}{C'\#(E/E_0)}.
\]

Let \(E_{\text{tors}}\) be the group of torsion points of \(E\). If \(u\) is the order of torsion in \(E\) and \(v\) is the order of the torsion in \(E_0\), then we can explicitly compute the order \(\#(E/E_0)\) as \(\frac{uv}{\mu}\), where

\[
\mu = \min \{ j > 0 : jP + R \in E_0 \text{ and } R \in E_{\text{tors}} \}
\]
and $P$ is any generator of the free part of $E$.

Thus, Conjecture 2.1 on its multiplicative form and running over all good reduction points gives:

**Conjecture 3.2.** *(Rank 1 at all Good Reduction Primes.)*

Let $E$ be a curve of rank 1, let $P$ be a generator of $E$ (modulo torsion), and let $Q$ be a generator of $E_0$ (modulo torsion), then:

$$
\hat{l}^{uv} = \hat{g}(P,Q)^{\left|\text{coker}(\phi)\right|} \in \prod_{p \nmid N} \mathbb{F}_p
$$

(25)

where $|\text{III}|$ is the order of the Tate-Shafarevich group and $\hat{l} = \prod_{p \mid N} l(\{p\})$.

Notice that if we exponentiate the above equation by $u/v$, we obtain the equation:

$$
\hat{l}^{u^2} = \hat{g}(P,Q)^{\left|\text{III}\right|/\mu}
$$

(26)

which looks more like the classical BSD.

For a more general $S$, having only good reduction points, the conjecture 2.1 in its multiplicative form becomes:

**Conjecture 3.3.** *(Rank 1 for $S$ having only Good Reduction Primes.)*

Let $E$ be a curve of rank 1 and $S$ having only good reduction primes, then:

$$
l(S)^{uv} = G(S)^{\left|\text{coker}(\phi)\right|} \in G_M
$$

(27)

where $M = \prod_{p \in S} p$ and $|\text{III}|$ is the order of the Tate-Shafarevich group.

In Chapter 4 of [15], we explained how to test Conjecture 3.3 using the individual computations on each prime $p \in S$.

# 4 Testing conjectures 3.2 and 3.3.

On [15], we tested the above conjecture for the first 300 elliptic curves in the Cremona database [3]. All these cases have trivial Tate-Shafarevich group. But, we also tested in [15] for an elliptic curve having a non-trivial Tate-Shafarevich group. The curve was

$$
y^2 + xy + y = x^3 - x^2 - 8587x - 304111
$$

(28)

with conductor $N = 1610$ and $|\text{III}| = 4$.

Those computations were done using the Pari calculator [1] with the help of the script [2], we tested each curve for $p < 300$ and $p \nmid N$. 

12
Now, we enlarge our experimental evidence using SAGE [19]. We test the Conjecture 3.2 on the first 3000 curves elliptic on the Cremona database (already included in SAGE).

We also check the Conjecture 3.2 for more elliptic curves with non-trivial Tate-Shafarevich group. We check on the first 20 elliptic curves with $|\Sha| = 4$ and on the first 7 elliptic curves with $|\Sha| = 9$. We use The L-functions and Modular Forms Database [18] to search for the required elliptic curves to test.

The files with the computing evidence and the scripts are available on

https://github.com/portillofco/MazurTateProject

Note 4.1. Last comment regarding normalization of modular symbols.

We use the usual methods for computing modular symbols and take advantage of the computing power of Pari-gp and Sage. There have been continuous advancement on the methods for computing modular symbols and also in the computing power used on computations, but correct normalization is still a practical issue to be considered during the testing of the conjecture.

The computation of the modular symbols $[a/b]^+$ using only Linear Algebra is alright up to multiplication by a constant. On our first computations [15] using Pari, we determined the constant by a series approximation of the value $[a/b]^+$. Now, Sage computes $[a/b]^+$ correctly in most of the cases, but there are still a few curves when Sage prompts a WARNING MESSAGE.

For example, for the curve 158 in the Cremona Database, we received the following WARNING MESSAGE:

**Warning**: Could not normalize the modular symbols, maybe all further results will be multiplied by -1, 2 or -2.

In such cases, we just verified which of the proposed values works for the conjecture. We must point out that in all the curves tested, one of the suggested values works. We believe that some numerical modular symbols can be used to compute the constant in a direct way [20].

Finally, we mention that we made the computations using a HP Workstation with a Processor Intel Xeon E5-2640v2 with 8 nodes and 48GB of RAM memory.

Acknowledgements

I would like to thank Felipe Voloch for his guidance and advice during the development of this research. I am also very grateful to John Tate for his valuable help and his many explanations regarding the conjecture 4 in [12]. The updating of this article and the new experimental evidence was supported by the project PI2013-38
of the agreement UACM/SECITI/060/2013. I thank also the support of my colleagues Isaías López and Felipe Alfaro during the development of the aforementioned project.

References

[1] K. Belabas and H. Cohen, Program Pari-2/Gp. [http://pari.math.u-bordeaux.fr/]

[2] B. Bernardi and B. Perrin-Riou, W. Stein The program modsym.gp ., [http://modular.fas.harvard.edu/tables/modsym.gp]

[3] J.E. Cremona, Algorithms for modular elliptic curves. Second Edition. Cambridge University Press, Cambridge, 1997.

[4] J.E. Cremona, Elliptic Curve Data. University of Warwick [http://www.warwick.ac.uk/~masgaj/ftp/data/]

[5] A. Grothendieck, Groupes de Monodromie en Géometrie Algébraique. Séminierie de Geométrie Algébraique du Bois Marie, 7 (1967/1969)

[6] S. Lang, Elliptic Functions. Addison-Wesley Publishing Company, Inc., Massachusetts (1973)

[7] Ju. I. Manin, Parabolic points and zeta functions of modular curves. Izv. Akad. Nauk. SSSR. Ser. Mat. 36(1972), 19–64

[8] Ju. I. Manin and M. M. Visik, Values of p-adic Hecke series of quadratic imaginary fields Matematiceskii Sbornik 95(137) (1974) 345–371

[9] Ju. I. Manin, Modular forms and Number Theory Proceedings of the International Congress of Mathematicians", Helsinki, 1978", Aca. Sci Fennica, 177–186

[10] B. Mazur and J. Tate and J. Teitelbaum, On p-adic analogues of the Conjectures of Birch and Swinnerton-Dyer" Invent. Math., 84 (1986) 1–48

[11] B. Mazur and J. Tate, Canonical Height Pairings via Biextensions. Arithmetic and Geometry, Progr. Math. 35(1983), 195–237.

[12] B. Mazur and J. Tate, Refined Conjectures of the Birch and Swinnerton-Dyer Type. Duke Math. J. 54(1987), 711–750.
[13] D. Mumford, *Bi-Extensions of Formal Groups*. In the *Proceedings of the Bombay Colloquium on Algebraic Geometry*, Tata Institute of Fundamental Research Studies in Mathematics 4, London, Oxford University Press 1968

[14] A. Néron, *Quasi-fonctions et Hauteurs sur les Varietes Abeliennes*. Annals of Mathematics, Second Series, Vol. 82, No. 2 (Sep., 1965), pp. 249-331

[15] F.X. Portillo, *Computations on an equation of the Birch and Swinnerton-Dyer type*. Ph.D. dissertation, University of Texas at Austin, 2004.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves* Springer-Verlag, New York. 2nd Edition (2009)

[17] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves* Springer-Verlag, New York. (1994)

[18] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, [http://www.lmfdb.org](http://www.lmfdb.org), 2015, [Online; accessed January 2015]

[19] W. Stein, *SAGE (Software for Algebra and Geometry Experimentation)*, [http://www.sagemath.org/index.html](http://www.sagemath.org/index.html)

[20] C. Wuthrich, *Numerical modular symbols for elliptic curves*, [https://arxiv.org/abs/1608.06423](https://arxiv.org/abs/1608.06423)