Facultad de Ciencias

# On the refined Birch-Swinnerton-Dyer conjecture

## Tesis

entregada a la Universidad de Chile
en cumplimiento parcial de los requisitos
para optar al grado de

Magíster en Ciencias Matemáticas

por
Juan Pablo Llerena Córdova
Enero del 2024

Director de Tesis: Dr. Daniel Barrera Salazar
Co-director de Tesis: Dr. Giancarlo Lucchini Arteche

## Aknoledgments

Let $\mathcal{X}$ be the set of all living creatures that are alive or that have stepped foot, at least once, on this earth. The author would like you to thank the subset $\mathcal{L} \subseteq \mathcal{X}$ which contains, at least, the following elements[1]:

- My family, in no particular order: my dog (Ikita), my brother (Hugo), my mother (Viviana), my Father (Hugo), the cat that lives with the author (gato, yes is called gato), and many more. Special mention to my grandfather (who I bear his name) who passed away during my undergraduate studies.
- My friends that have helped me at some point or another. Especially during the pandemic. For example: Batían, Juan Pablo (Not the author, another Juan Pablo), Carlos[3], Javier, Felipe, Gary, Gabriel, Sergey, Mariano, Guillermo, Daniel, Camilo, Claudio, Ignacio, and many more.
- The professors and the mathematical community that helped the author during this journey in the world of mathematics: Prof. Labra, Prof. Auffarth, Prof. Poblete, Prof. Barrera, Prof. Lucchini, Prof. Pozo, Prof. L Aremas, Prof. M. Arenas, Prof. Reyes, Prof. Castañeda, the cat that lives with the author (yes, again), Prof. Pomareda, Prof. Robledo, H. del Castillo, L. Palacios, R. Tosso (recently found), Prof. Friedman, Prof. Martin, Prof. Grimm, Prof. Herrero, and many more.
- The community of SageMath, and all the people that have worked at some point in the free open-source software. `https://www.sagemath.org/development-map.html`
- Whoever found coffee.

The set $\mathcal{L}$ may contain more elements. Finding all the elements of $\mathcal{L}$ is not an easy task, as the author may forget that some elements exist, or did exist. Nevertheless, we present the following theorem:

**Theorem:** The set $\mathcal{L}$ is finite.

*Proof:* Unfortunately, because of time restrictions, we will not be able to add the proof here. So it will be left as an exercise for the reader.

Finally, we leave the following conjecture, which we were not able to prove:

**Conjecture:** Any element $x \in \mathcal{X} - \mathcal{L}$ will eventually be in $\mathcal{L}$.

*The author is supported by Agencia Nacional de Investigación y Desarrollo-Subdirección de Capital Humano scholarship Magíster Nacional 2021 N° 22221372*

[1] Unfortunately, the author did not take seriously the advice to start writing his thesis early in his masters, so the author is tired and will forget many elements of this set.

## Resumen

Dada una curva elíptica $E/\mathbb{Q}$, la conjetura de Birch-Swinnerton-Dyer predice que el rango de $E$ y el orden de anulación de $L(E,s)$ en $s=1$ son iguales. Más aún, una formulación más fuerte de esta conjetura relaciona el coeficiente líder de $L(E,s)$ en $s=1$ con invariantes aritméticos de $E$. En 1987 Mazur y Tate formularon un análogo refinado a estas conjeturas en un *layer* finito $M$, donde la función $L$ es reemplazada por el elemento de Mazur-Tate $\Theta_M$. Propondremos dos conjeturas similares a las presentadas por Mazur y Tate y presentaremos evidencia numerica soportando estas conjeturas.

## Abstract

Given an elliptic curve $E/\mathbb{Q}$, the Birch-Swinnerton-Dyer conjecture predicts that the rank of $E$ and the vanishing order of $L(E,s)$ at $s=1$ are equal. Furthermore, a stronger formulation of this conjecture relates the leading coefficient of $L(E,s)$ at $s=1$ and arithmetic invariants of $E$. In 1987 Mazur and Tate formulated refined analogs of these conjectures at a finite layer $M$, where the $L$-function is replaced by the Mazur-Tate element $\Theta_M$. We will state two conjectures similar to conjectures presented by Mazur and Tate, and present numerical evidence supporting these conjectures.

# Contents

# Introduction

## History

Since early in the history of mathematics, finding rational solutions to polynomials has been of great interest to mathematicians. Nowadays, a particular family of polynomials, that have captivated the mathematical community, are the elliptic curves over the rationals, which are algebraic objects that can be described in terms of polynomials of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;\ a_i \in \mathbb{Q}.$$

The role that elliptic curves have played in modern mathematics, in particular in modern number theory, can not be downplayed. One example in which elliptic curves were a key tool is the proof of the famous Fermat's last theorem.

**Theorem 0.0.1** (Fermat's last theorem)**.** *If $n > 2$ then the equation*

$$x^n + y^n = z^n$$

*has no non-trivial integer solutions.*

This conjecture was stated around 1637 by P. Fermat and was considered, at the beginning of the 20th century, an unapproachable problem. However, by the work of K Ribet [47], J. Serre [50], G. Frey[20], and others, we know that a way of proving this theorem was to show that every elliptic curve is modular. In other words, if every elliptic curve is modular then Fermat's last theorem would be true.

The statement that every elliptic curve is modular was an open question stated by G. Shimura, Y. Taniyama, and A. Weil, known as the Shimura-Taniyama-Weil conjecture, also considered at the beginning of the 20th century a difficult problem in mathematics. Nevertheless, in 1995 A. Wiles presented a partial proof of the Shimura-Taniyama-Weil conjecture sufficient enough to conclude that Fermat's last theorem is true [59], with a subsequence article with R. Taylor for some correction on the original article [58]. The complete proof of Shimura-Taniyama-Weil, now known as the modularity theorem, was completed in 2001 by the work of C. Breuil, B. Conrad, F. Diamond, and R. Taylor [8]. This is a mere example of the role that elliptic curves have played in modern number theory, which is not an exception and this thesis will focus on one of these mysterious properties of elliptic curves a particular variation of the Birch-Swinnerton-Dyer conjectures.

At the turn of the millennium, the Clay Institute of Mathematics published 7 open problems in different topics in mathematics[9]. These problems were chosen by their importance in their respective areas. One of these problems is the Birch-Swinnerton-Dyer conjecture [60].

Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$. We know from the work of L. Mordell that

$$E(\mathbb{Q}) \cong \mathbb{Z}^{r_E} \times E(\mathbb{Q})_{\mathrm{Tor}},$$

were $r_E$ is called the rank of $E$ and $E(\mathbb{Q})_{\mathrm{Tor}}$ is the torsion part of $E(\mathbb{Q})$.

Also, to the same elliptic curve, we can attach a complex-valued function, called the $L$-function via the Euler product

$$L(E,s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N} (1 - a_p p^{-s})^{-1},$$

where $a_p$ depends on the number of solutions of $E$ modulo $p$, see 1.1.36. Even though this product only converges when $\mathrm{Re}(s) > \frac{3}{2}$, by the modularity theorem, mentioned before, we know that it has an analytic continuation to the whole complex plane.

The modern formulation of the Birch-Swinnerton-Dyer conjecture, as stated by the Clay Institute of Mathematics [60], can be stated as follows.

**Conjecture 0.0.2** (Birch-Swinnerton-Dyer conjecture (*cf.* [60]))**.** Using the same notation as above, we have that

$$r_E = \mathrm{ord}_{s=1} L(E,s).$$

There is an even stronger formulation of this conjecture, describing the leading coefficient of the Taylor series of $L(E,s)$ at $s=1$ by arithmetic invariants of $E$.

**Conjecture 0.0.3** (Strong Birch-Swinnerton-Dyer conjecture)**.** Using the same notation as above and denoting by $\mathcal{P} \subseteq \mathbb{N}$ the set of all prime numbers. Then

$$\frac{L^{(r_E)}(E,1)}{r_E! \cdot \Omega_E^+} = \frac{\#\text{Ш}_E \cdot \prod_{p \in \mathcal{P}} C_{E,p} \cdot \mathrm{Reg}(E)}{(\#E(\mathbb{Q})_{\mathrm{Tor}})^2},$$

where

- $\Omega_E^+$ is the real period of $E$, see 1.2.24.
- $\text{Ш}_E$ is the Tate-Shafarevich group of $E$, see 1.1.28.
- $\mathrm{Reg}(E)$ is the regulator of $E$, see 2.1.5.
- $C_{E,p} = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$ and $E^0(\mathbb{Q}_p)$ denotes the identity component, see 1.1.33.

Only partial results are known for the former conjecture, are very little is known for the latter one.

Our main interest in this thesis is the refined analog of the Birch-Swinnerton-Dyer conjectures stated by B. Mazur and J. Tate in 1987.

## Refined Birch-Swinnerton-Dyer conjectures

Let $E/\mathbb{Q}$ be an elliptic curve. The Mazur-Tate element at layer $M \in \mathbb{N}$ is defined as

$$\Theta_M := \frac{1}{2} \sum_{a \in (\mathbb{Z}/M\mathbb{Z})^*} \lambda(a, M) \cdot [a] \in R\left[(\mathbb{Z}/M\mathbb{Z})^* / \langle -1 \rangle\right],$$

where $\lambda(a, M)$ denotes the modular symbol of $\frac{a}{M} \in \mathbb{Q}$ attached to $E$, see 1.2.26 and $R \subsetneq \mathbb{Q}$ is a subring containing all the modular symbols $\{\lambda(a, M)\}_{a \in (\mathbb{Z}/M\mathbb{Z})^*}$. If we denote by $I$ the augmentation ideal of $R\left[(\mathbb{Z}/M\mathbb{Z})^* / \langle -1 \rangle\right]$, see 2.3.2, we can define the vanishing order of $\Theta_M$ as the $n \in \mathbb{N}_0$ such that $\Theta_M \in I^n$ and $\Theta_M \notin I^{n+1}$, or $\infty$ if $\Theta_M \in I^n$; $\forall n \in \mathbb{N}_0$. Under these hypotheses, in [38] Mazur and Tate conjectured "refined" analogs of the classical Birch-Swinnerton-Dyer conjectures. This thesis will be centered on two of these conjectures.

**Conjecture 0.0.4** ([38, Conjecture 5])**.** Assume that $E(\mathbb{Q})$ is finite and its order is invertible in $R$. Let $S_m \subseteq \mathcal{P}$ be a set containing $r$ prime numbers, such that for each $p \in S_m$, $E$ has split multiplicative reduction at $p$. Also, for each $p \in S_m$, fix a $e_p \geq 0$ and denote by $M := \prod_{p \in S_m} p^{e_p}$. Then $\Theta_M \in I^r$ and

$$\tilde{\Theta}_M \equiv \frac{\#\text{Ш}_E \cdot \prod_{p \in \mathcal{P} - S_m} C_{E,p}}{(\#E(\mathbb{Q}))^2} \prod_{p \in S_m} ([\tilde{q}_{E,p}] - [1]) \in I^r / I^{r+1},$$

where $\tilde{\Theta}_M$ denotes the image of $\Theta_M$ in $I^r/I^{r+1}$, $q_{E,p}$ is the Tate $p$-adic period at the prime $p$ (see 1.1.22) and $\tilde{q}_{E,p} := q_{E,p}/p^{\operatorname{ord}_p(q_{E,p})}$. For a more detailed explanation of how we see $\tilde{q}_{E,p}$ as an element of $I^r/I^{r+1}$ see 2.5.

Using the classical Birch-Swinnerton-Dyer conjecture, we can get a slight reformulation of the previous conjecture.

**Conjecture 0.0.5** ([38, Conjecture 6])**.** Let $E/\mathbb{Q}$ be an elliptic curve. Also, Let $S_m \subseteq \mathcal{P}$ be a set containing $r$ prime numbers, such that for each $p \in S_m$, $E$ has split multiplicative reduction at $p$. For each $p \in S_m$ fix a $e_p \geq 0$ and denote by $M := \prod_{p \in S_m} p^{e_p}$. Furthermore, assume that $\frac{\lambda(0,1)}{2 \prod_{p \in S_m} C_{E,p}}$ is invertible in $R$. Then $\Theta_M \in I^r$ and

$$\tilde{\Theta}_M \equiv \frac{\lambda(0,1)}{2 \prod_{p \in S_m} C_{E,p}} \prod_{p \in S_m} ([\tilde{q}_{E,p}] - [1]) \in I^r / I^{r+1},$$

where, as before, $\tilde{\Theta}_M$ denotes the image of $\Theta_M$ in $I^r/I^{r+1}$, $q_{E,p}$ is the Tate $p$-adic period at the prime $p$ and $\tilde{q}_{E,p} = q_{E,p}/p^{\mathrm{ord}_p(q_{E,p})}$. Furthermore, if $E(\mathbb{Q})$ is not finite, then both sides are 0.

In this thesis, we present numerical calculations supporting a variation of conjecture 0.0.4 and conjecture 0.0.5. But also, present some discrepancies that we found during our calculations.

## Main results

Adding further restrictions, we can get "multiplicative" conjectures similar to conjecture 0.0.4 and conjecture 0.0.5, which are easier to check with SageMath. For the multiplicative conjecture inspired by conjecture 0.0.4.

**Conjecture 0.0.6.** Using the same notation as in 0.0.4, assume that $S_m = \{p\}$ and $M = p$. Then we have that

$$\prod_{0<a<p} a^{D(\#E(\mathbb{Q}))^2 \mathrm{ord}_p(q_{E,p})\lambda(a,p)} \equiv \tilde{q}_{E,p}^{2D(\#Ш_E)(\prod_{p\in\mathcal{P}} C_{E,p})} \in (\mathbb{Z}/p\mathbb{Z})^* / \langle -1 \rangle , \qquad (1)$$

where $D$ is the least common multiple of the denominators of the modular symbols $\{\lambda(a,p)\}_{0<a<p}$. For more detail explanation of how we see $\tilde{q}_{E,p} \in (\mathbb{Z}/p\mathbb{Z})^* / \langle -1 \rangle$ see 2.5.

On the other hand, for the multiplicative conjecture inspired by conjecture 0.0.5 we have.

**Conjecture 0.0.7.** Using the same notation as in 0.0.5, assume that $S_m = \{p\}$ and $M = p$. Then

$$\prod_{0<a<p} a^{D\lambda(a,p)\mathrm{ord}_p(q_{E,p})} \equiv \tilde{q}_{E,p}^{D\lambda(0,1)} \in (\mathbb{Z}/p\mathbb{Z})^* / \langle -1 \rangle \qquad (2)$$

where $D$ is the least common multiple between all the denominators of the modular symbols $\{\lambda(a,p)\}_{0\leq a<p}$. Furthermore, if $E(\mathbb{Q})$ is not finite, then both sides are conjectured to be 1.

With the objective to expand the numerical evidence supporting conjectures similar to conjecture 0.0.4 and conjecture 0.0.5, we implemented a script in SageMath that allowed us to calculate the necessary values and check the multiplicative analogs i.e. conjecture 0.0.6 and conjecture 0.0.7. We obtained around 500.000 pairs $(E, p)$, where $E$ is an elliptic curve and $p$ is a prime for which $E$ has split multiplicative reduction. Adding the restriction that $E(\mathbb{Q})$ is finite these pairs reduce to around 200.000.

Even though the vast majority of pairs $(E, p)$ satisfy conjecture 0.0.7 around 400 (0.08%) pairs $(E, p)$, apparently, do not satisfy conjecture 0.0.7. We did not find any counterexample for 0.0.6. We present our findings in Section 3.

## Other result

In 2001 H. Darmon [13] attached a $p$-adic period $I_\Psi \in \mathbb{Q}_p^*$ to the elliptic curve $E$, which depends on a $\mathbb{Q}$-algebra embedding $\Psi : \mathbb{Q}\times\mathbb{Q} \to M_2(\mathbb{Q})$, with the objective to formulate an analog theory of complex multiplication for the case of real quadratic fields. Even though the definitions of $I_\Psi$ and $q_{E,p}$ are completely different in nature, Darmon proved that these two periods are related by the following theorem

**Theorem 0.0.8** ([13, Theorem 1])**.** *Using the same notation as above*

$$\log_p(I_\Psi) = \frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}\mathrm{ord}_p(I_\Psi), \tag{3}$$

*where* $\log_p$ *is the p-adic logarithm (with* $\log_p(p) = 0$*) and* $\mathrm{ord}_p$ *is the valuation normalized at p such that* $\mathrm{ord}_p(p) = 1$*. In particular, because* $|q_{E,p}| > 1$*, then* $\mathrm{ord}_p(q_{E,p}) \neq 0$*, see 1.1.22.*

Even though $q_{E,p}$ depends on the geometry of $E/\mathbb{Q}_p$ and $I_\Psi$ is purely automorphic, they are still closely related by theorem 0.0.8.

Now, in terms of the natural decomposition

$$\mathbb{Q}_p^* \cong p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p),$$

equation (3) does not detect the projection of $q_{E,p}$ onto $\mu_{p-1}$. With the ever-growing philosophy of "refining" $p$-adic theorems, we were interested in finding a refined analog of equation (3), to be able to detect the projection of $q_{E,p}$ onto $\mu_{p-1}$.

To be able to recover the root of the unity component of $q_{E,p}$ we have to replace $\log_p$ and $\mathrm{ord}_p$ with the functions $\lambda_R$ and $v_R$, respectively, defined as follows. Let $\ell$ a prime number dividing $p-1$ and $n \in \mathbb{N}$ the biggest number such that $\ell^n | p-1$. Also, denote by $R = \mathbb{Z}/\ell^n\mathbb{Z}$ and fix a finite logarithm $\log : (\mathbb{Z}/p\mathbb{Z})^\times \to R$ i.e. a surjective morphism. We define $\lambda_R$ as follows

$$\begin{array}{rcccl} \lambda_R : \mathbb{Q}_p^* & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^* & \longrightarrow & R \\ q & \longrightarrow & \tilde{q} \coloneqq \frac{q}{p^{\mathrm{ord}_p(q)}} \bmod p & \longrightarrow & \log(\tilde{q}) \bmod \ell^n \end{array}$$

and we define $v_R$ as

$$\begin{aligned} v_R : \mathbb{Q}_p^* &\to R \\ q &\mapsto \mathrm{ord}_p(q) \mod \ell^n \end{aligned}$$

**Theorem 0.0.9.** *Let $E/\mathbb{Q}$ be an elliptic curve with conductor p and split multiplicative reduction at p. Also, let $\ell > 3$ be a prime number such that $\ell | p-1$ and is coprime to the modular degree of E. If $\Psi$ is an optimal embedding of conductor* 1*, then:*

$$\lambda_R(I_\Psi) = \frac{\lambda_R(q_{E,p})}{v_R(q_{E,p})} \cdot v_R(I_\Psi).$$

*were $q_{E,p}$ denotes the Tate p-adic period.*

The proof of this theorem was also done during the master studies but is omitted in this thesis. However, it will be published in a subsequent work with Professor Daniel Barrera.

## Thesis structure

The first section of this thesis aims to recall some definitions/Theorems/Propositions necessary for the formulation of the conjectures by B. Mazur and J. Tate in [38]. This section includes Definitions and some properties of elliptic curves, the definition of modular forms for the Hecke subgroups, the relation between modular forms and elliptic curves, and the definition of modular symbols.

The first part of section 2 of this thesis covers some history of the classical Birch-Swinnerton-Dyer conjectures and its $p$-adic analog in the exceptional zero case and also some partial results. We also recall de definition of the Mazur-Tate element and some of the conjectures surrounding it. The last part of this section covers conjecture 0.0.4 and conjecture 0.0.5 and its multiplicative analogs conjecture 0.0.6 and conjecture 0.0.7 respectively, which were the conjectures that we implemented in SageMath.

In the third section of this thesis, we give an overview of some partial results of the refined Birch-Swinnerton-Dyer conjectures. We also explain in more detail our findings with SageMath and some, possible, cases in which conjecture 0.0.7 do not hold.

In Appendix A, we give 100 elliptic curves that, apparently, do not satisfy conjecture 0.0.7. Finally, in Appendix B, we give 4 examples of how we carried the calculations in SageMath for conjecture 0.0.7 or conjecture 0.0.6, two for each conjecture, with a step-by-step explanation of how we use CoCalc's page which has a section to use SageMath online, to calculate the necessary values used in conjecture 0.0.7 and conjecture 0.0.6.

# Chapter 1

# Preliminaries

## Notation

Unless stated otherwise, we fix the following notation:

1. We will denote the set of natural numbers by $\mathbb{N} \coloneqq \{1, 2, 3, ...\}$ and the set of cardinal numbers by $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$.
2. The letter $K$ will always denote a perfect field, and for any field $K$ fix an algebraic closure $\overline{K}$.
3. We will denote the absolute Galois group of $K$ by $\mathrm{Gal}_K \coloneqq \mathrm{Gal}(\overline{K}/K)$.
4. We will denote by $\mathbb{Q}_p$ the set of $p$-adic numbers, by $\mathbb{Z}_p$ the set of $p$-adic integers, and by $\mathbb{C}_p$ the $p$-adic complex numbers i.e. the completation of the algebraic clousure of $\mathbb{Q}_p$. We will also denote by $v_p$ the $p$-adic valuation of $\mathbb{C}_p$ with the convention $v_p(p) = 1$ and by $\log_p : \mathbb{C}_p^* \to \mathbb{C}_p$ the $p$-adic logarithm with $\log_p(p) = 0$.
5. If $G$ is a group, then $G_{\mathrm{Tor}}$ denotes the torsion of the group, and by $G[n]$ the $n$-torsion of $G$.
6. We will denote by $\mathcal{P} \subseteq \mathbb{N}$ the set of all prime numbers.

*In this section we recall some necessary preliminaries and fix notation for the rest of the thesis. The main references are, [53] and [52], and [17]. For our purposes, we will not state every definition/proposition/lemma/theorem in its full generality, this will make some cleaner statements for our purposes.*

## 1.1 Elliptic curves

### 1.1.1 Definitions and basic properties

**Definition 1.1.1.** An elliptic curve $E$ over a field $K$ is a smooth projective curve of genus 1 defined over $K$, with a point $O_E \in E(K)$. If such is the case, we will denote the elliptic curve $E$ over the field $K$ as $E/K$.

Given an elliptic curve $E/K$, we can use the Riemann-Roch theorem to prove that $E$ is defined by a degree 3 polynomial.

**Proposition 1.1.2** ([53, Chapter III, Proposition 3.1])**.** Let $E/K$ be an elliptic curve. There exists a curve $\tilde{E} \subseteq \mathbb{P}^2(K)$ given by an equation of the form:

$$\tilde{E} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3;\ a_i \in K$$

such that $\tilde{E} \cong E$ as $K$-varieties. If we consider the non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$ we get an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;\ a_i \in K$$

We will refer to the previous equation as a **Weierstrass equation** of $E$.

Let $E/K$ be an elliptic curve with a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;\ a_i \in K. \tag{1.1}$$

We define the following quantities:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, & b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_4^2 + 4a_6, & b_8 &= a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_4^2, \\ c_4 &= b_2^2 - 24b_4. \end{aligned} \tag{1.2}$$

**Definition 1.1.3.** Let $E/K$ be an elliptic curve. We define the **Discriminant** of $E$ as

$$\Delta_E \coloneqq -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{1.3}$$

and the $j$**-invariant** of $E$ as

$$j_E = \frac{c_4^3}{\Delta_E},$$

where $b_i$ and $c_4$ are defined as in (1.2).

**Proposition 1.1.4.** If $E/K$ is an elliptic curve, then $\Delta_E \neq 0$.

*Proof.* The proof can be found in [53, Chapter III, Proposition 1.4]. However, there is a typo in Proposition 1.4.a.i) it should be "*It is nonsingular if and only if* $\Delta \neq 0$", as one can see in the proof. □

The latter proposition allows us to conclude that the $j$-invariant is always well-defined.

**Remark 1.1.5.** Given an elliptic curve $E/\mathbb{Q}$ with a Weierstrass equation as in (1.1), we can consider the substitution

$$(x, y) \mapsto \left( \frac{x - 3(a_1^2 + a_4)}{36}, \frac{y - a_1x - a_3}{216} \right),$$

to get an equation of the form

$$y^2 = x^3 + ax + b; \tag{1.4}$$

for some $a, b \in \mathbb{Q}$ and discriminant $\Delta_E = 16(a^3 + 27b^2) \neq 0$. We will refer to equation (1.4) as a **simplified Weierstrass equation** of $E$. Reciprocally, if $a, b \in \mathbb{Q}$ with $-16(a^3 + 27b^2) \neq 0$, then the equation

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

will determine an elliptic curve over $\mathbb{Q}$. For the proof of this see [53, Chapter III, Proposition 1.4] and [53, Chapter III, Proposition 3.1].

Finally, we will define a binary operation $\oplus$ on $E(K)$.

**Definition 1.1.6** ([53, Chapter III, Composition Law 2.1])**.** Let $E/K$ be an elliptic curve and $P, Q \in E(K)$. Let $L$ be the line through $P$ and $Q$ (if $P = Q$ let $L$ be the tangent line to $E(K)$ at P), and let $R$ be the third point of intersection of $L$ with $E(K)$. Let $L'$ be a line through $R$ and $O_E$. Then $L'$ intersects $E(K)$ at $R$, $O_E$, and a third point $C$. We define the binary operation on $E(K)$ as $P \oplus Q = C$, with $P, Q$ and $C$ as previously described.

For a more detailed construction of the binary operation and the fact that it is well-defined, which is a consequence of Bézout Theorem [24, Chapter I, Theorem 7.8], see [53, Chapter III.2].

**Proposition 1.1.7** ([53, Chapter III, Proposition 2.2])**.** Let $E/K$ be an elliptic curve. Then $(E(K), \oplus)$ is an abelian group with identity $O_E$.

**Definition 1.1.8.** Let $E_1/K$ and $E_2/K$ be two elliptic curves. A morphism of $K$-varieties $\phi : E_1 \to E_2$ such that $\phi(O_{E_1}) = O_{E_2}$ is called an $K$-**isogeny**.

### 1.1.2 Reduction of an elliptic curve

Let $p$ be a prime number. We have that $\mathbb{Z}_p$ has $\mathbb{Q}_p$ as its field of fractions and has $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ as its residue field.

**Definition 1.1.9.** An **Integral Weierstrass equation** of $E/\mathbb{Q}_p$, is an equation of the form

$$\tilde{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;\ a_i \in \mathbb{Z}_p, \tag{1.5}$$

such that $\tilde{E} \cong E$ as $\mathbb{Q}_p$-varieties. Furthermore, if $\text{ord}_p(\Delta_{\tilde{E}})$ is minimal with respect to all integral Weierstrass equations we say that (1.5) is a **Minimal Weierstrass equation**

**Proposition 1.1.10** ([53, Chapter VII, Proposition 1.3])**.** Every elliptic curve $E/\mathbb{Q}_p$ has a minimal Weierstrass equation.

Now, if we consider $E/\mathbb{Q}_p$ with a minimal Weierstrass equation as in (1.5), we can use the natural projection $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ and obtain an equation

$$\overline{E} : y^2 + \overline{a}_1 xy + \overline{a}_3 y = x^3 + \overline{a}_2 x^2 + \overline{a}_4 x + \overline{a}_6; \quad a_i \mapsto \overline{a}_i \in \mathbb{F}_p. \tag{1.6}$$

However, $\overline{E}$ will not always be an elliptic curve defined over $\mathbb{F}_p$, it may lose the smoothness property.

**Proposition 1.1.11** ([53, Chapter III, Proposition 1.4])**.** The curve $\overline{E}$ defined in (1.6) has at most one singular point.

**Definition 1.1.12.** Let $E/\mathbb{Q}_p$ be an elliptic curve with a minimal Weierstrass equation as in (1.5), and denote by $\overline{E}$ the curve defined by (1.6):

1. If $\overline{E}$ is an elliptic curve, then we say that $E$ has good reduction.
2. If $\overline{E}$ has a cusp, then we say that $E$ has additive reduction.
3. If $\overline{E}$ has a node, then we say that $E$ has multiplicative reduction. Furthermore, there are two types of multiplicative reduction:
   (a) If the slopes of the two tangents on the node are defined over $\mathbb{F}_p$, then we say that $E$ has split multiplicative reduction.
   (b) If the slopes of the two tangents on the node are not defined over $\mathbb{F}_p$, then we say that $E$ has non-split multiplicative reduction.

As $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to a $p$-adic absolute value, we define the reduction of an elliptic curve $E/\mathbb{Q}$ at a prime $p$ as follows.

**Definition 1.1.13.** Let $E/\mathbb{Q}$ be an elliptic curve and $p$ a prime number.

1. We say that $E$ has good reduction at $p$ if and only if $E$ has good reduction viewed in $\mathbb{Q}_p$.
2. We say that $E$ has additive reduction at $p$ if and only if $E$ has additive reduction viewed in $\mathbb{Q}_p$.
3. We say that $E$ has multiplicative reduction at $p$ if and only if $E$ has multiplicative reduction viewed in $\mathbb{Q}_p$.
4. We say that $E$ has split multiplicative reduction at $p$ if and only if $E$ has split multiplicative reduction viewed in $\mathbb{Q}_p$.
5. We say that $E$ has non-split multiplicative reduction at $p$ if and only if $E$ has non-split multiplicative reduction viewed in $\mathbb{Q}_p$.

A way of encoding the behavior of the reduction of an elliptic curve $E/\mathbb{Q}$ with respect to all primes is with the conductor of $E$.

**Definition 1.1.14.** Let $E/\mathbb{Q}$ be an elliptic curve. We define the **conductor** of $E$ as

$$N_E := \prod_{p \in \mathcal{P}} p^{f_p}$$

where

$$f_p = \begin{cases} 0 & p \text{ has good reduction} \\ 1 & p \text{ has multiplicative reduction} \\ 2+\delta_p & p \text{ has additive reduction} \end{cases}$$

Where $\delta_p$ depends on the Tate module $T_p(E)$ of $E$[1].In particular, if $p \neq 2, 3$, then $\delta_p = 0$.

In the case of elliptic curves $E/\mathbb{Q}$, there exists Weierstrass equations that is minimal with respect to all primes $p$, this is known as a global minimal Weierstrass equation.

**Definition 1.1.15.** An **Integral Weierstrass equation** for $E/\mathbb{Q}$ is a Weierstrass equation

$$\tilde{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6;\ a_i \in \mathbb{Z} \tag{1.7}$$

such that $\tilde{E} \cong E$ has $\mathbb{Q}$-varieties. Furthermore, if an integral Weierstrass equation is a minimal Weierstrass equation for all $p \in \mathcal{P}$ as in definition 1.1.9, we say that (1.7) is a **Global minimal Weierstrass equation**.

**Proposition 1.1.16** ([53, Chapter VIII, Corollary 8.3])**.** Every elliptic curve $E/\mathbb{Q}$ has a global minimal Weierstrass equation.

Finally, we define the following objects.

**Definition 1.1.17.** By a **lattice** of $\mathbb{C}$, we mean a rank 2 $\mathbb{Z}$-module $\Lambda$ such that $\mathbb{R}\Lambda = \mathbb{C}$. By fixing a basis, we have that any lattice can be described as a $\mathbb{Z}$-lattice $\Lambda = \langle \omega_1, \omega_2 \rangle$ where $\omega_1, \omega_2 \in \mathbb{C}^*$ and $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$.

**Definition 1.1.18.** Let $E/\mathbb{Q}$ be an elliptic curve with Weierstrass equation:

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6;\ a_i \in \mathbb{Q}. \tag{1.8}$$

We define the **Invarient differential** as

$$\omega_E := \frac{dx}{2y + a_1 + a_3}$$

and the **Period lattice** as

$$\Lambda_E := \left\{ \int_{[\gamma]} \omega_E;\ [\gamma] \in H_1(E(\mathbb{C}), \mathbb{Z}) \right\}. \tag{1.9}$$

[1] The Tate module is defined as $T_p(E) := \lim_{\leftarrow} E(\overline{\mathbb{Q}})[p^n]$, for the definition of $\delta_p$ see [52, Chapter IV, §10]

If the equation (1.8) is a global minimal Weierstrass equation, then the invariant differential and period lattice are called the **Néron differential** and the **Néron Lattice**, respectively.

**Proposition 1.1.19** ([53, Chapter VI, Proposition 5.2])**.** Let $E/\mathbb{Q}$ be an elliptic curve. The set (1.9) is a lattice of $\mathbb{C}$.

### 1.1.3 Uniformization of elliptic curves

**Proposition 1.1.20** (Complex Uniformization)**.** Given an elliptic curve $E/\mathbb{C}$, there exists a lattice $\Lambda \subseteq \mathbb{C}$ and a isomorphism of groups

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C}). \tag{1.10}$$

Furthermore, for all elliptic curve $E/\mathbb{C}$ there exists a $\tau \in \mathbb{C}$ with $\mathrm{Im}(\tau) > 0$ such that $E(\mathbb{C}) \cong \mathbb{C}/\left\langle 1, \tau \right\rangle$. Reciprocally, given any lattice $\Lambda \subseteq \mathbb{C}$, there exists an elliptic curve $E/\mathbb{C}$ such that $\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$.

*Proof.* For the proof of the first statement see [53][Chapter VI, Proposition 3.6], for the proof of the second statement see [53][Chapter VI, Corollary 5.1], and for the last statement see [40, Chapter 3, §3]. □

Now, if we consider the $\mathbb{C}_p$ points of $E$, we could try to replicate the uniformization as in (1.10). Unfortunately, there does not exist an isomorphism of the form

$$\mathbb{C}_p/\Lambda \xrightarrow{\sim} E(\mathbb{C}_p)$$

where $\Lambda$ is a discrete subgroup of $\mathbb{C}_p$. Because $\mathbb{C}_p$ does not have non-trivial discrete subgroup.

**Proposition 1.1.21.** Let $H \leq \mathbb{C}_p$ be a non-trivial additive subgroup. Then $H$ has an accumulation point.

*Proof.* If $H \leq \mathbb{C}_p$ is a non-trivial subgroup, we will prove that 0 is an accumulation point. Consider any element different from the identity $x \in H$, and the sequence $\{p^n x\}_{n \in \mathbb{N}}$. We can see that $p^n x \neq 0, \forall n \in \mathbb{N}$ and that

$$\mathrm{ord}_p(p^n x) = n + \mathrm{ord}_p(x) \xrightarrow{n \to \infty} \infty$$

Therefore, $\{p^n x\}$ converges to 0 and $H$ has an accumulation point. □

Nevertheless, we can use the last affirmation of proposition 1.1.20 to make the following observation. Let $E/\mathbb{C}$ be an elliptic curve, by proposition 1.1.20 we know that there exists a $\tau \in \mathbb{C}$ with $\mathrm{Im}(\tau) > 0$, such that

$$E(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}/\left\langle 1, \tau \right\rangle$$

If we now consider the function $f : \mathbb{C} \to \mathbb{C}^*;\ z \mapsto e^{2\pi i z}$, we can see that $f(0) = 1$. Therefore, we have the following isomorphisms

$$E(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}/\langle 1, \tau\rangle \xrightarrow{\sim} \mathbb{C}^*/q_\tau^{\mathbb{Z}}$$

where $q_\tau = e^{2\pi i\tau}$. We can conclude that

$$E(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}^*/q_\tau^{\mathbb{Z}}. \tag{1.11}$$

Even though an isomorphism of the form (1.10) did not hold in the non-Archimedean case, under certain conditions, an isomorphism analogous to (1.11) does hold in the non-Archimedean case.

**Theorem 1.1.22** (Tate uniformization[2])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. If $E$ has multiplicative reduction at $p$, then the exists a unique $q_{E,p} \in \mathbb{Q}_p^*$ with $|q_{E,p}| < 1$ such that there is a group isomorphism*

$$\mathbb{C}_p^*/q_{E,p}^{\mathbb{Z}} \cong E(\mathbb{C}_p).$$

*The isomorphism is defined over $\mathbb{Q}_p$, if and only if $E$ has split multiplicative reduction at $p$.*

*Proof.* For a proof that does not use the theory of rigid analytic geometry, see [52, Chapter V, Theorem 5.3] □

We will refer to the $p$-adic number $q_{E,p}$ in the previous theorem as the Tate $p$-adic period.

The Tate $p$-adic period of an elliptic curve is a number of great interest. For example, by its role in the $p$-adic Birch-Swinnerton-Dyer conjectures (See 2.2) and the refined Birch-Swinnerton-Dyer conjectures (See 2.5). A way of studying the Tate $p$-adic period is by considering the natural decomposition

$$\mathbb{Q}_p^* \cong p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p).$$

and studying the projection of $q_{E,p}$ into the different components. The valuation of $q_{E,p}$ can be described in terms of the $j$-invariant.

**Proposition 1.1.23** ([39][Pag. 28])**.** Let $E/\mathbb{Q}$ be an elliptic curve with multiplicative reduction at $p$. Then

$$\mathrm{ord}_p(q_{E,p}) = -\mathrm{ord}_p(j_E).$$

On the other hand, the projection of $q_{E,p}$ into the group $1 + p\mathbb{Z}_p$ has been studied in [22], [13], and others. Finally, the projection of $q_{E,p}$ into the group $\mu_{p-1}$ has not been studied as much as the later and former projection, but some works are [16] and [21].

[2] This is normally cited [57][Theorem 5], but for the first published proof see [48]. However, Roquette's proof is in the language of *Rigid Analytic Geometry.*

### 1.1.4 Rational points of an elliptic curve

The last group structure of interest is the set of rational points of an elliptic curve $E/\mathbb{Q}$. By the work of Mordell, we know a description of the abstract group structure of the rational points of the elliptic curves.

**Theorem 1.1.24** ([41])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. There exists a $r_E \in \mathbb{N}_0$ such that*

$$E(\mathbb{Q}) \cong \mathbb{Z}^{r_E} \times E(\mathbb{Q})_{\mathrm{Tor}}.$$

**Definition 1.1.25.** Let $E/\mathbb{Q}$ be an elliptic curve. The number $r_E \in \mathbb{N}_0$ in theorem 1.1.24 is called the **rank** of $E$.

This theorem lets us understand the abstract group structure of $E(\mathbb{Q})$ by its torsion and free part.

The torsion part has been studied and classified by the work of B. Mazur.

**Theorem 1.1.26** ([36][Chapter III, Theorem 5.1])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\mathrm{Tor}}$ is isomorphic to one of the following groups*

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} \ &; n \leq 10 \text{ or } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \ &; m \leq 4. \end{aligned}$$

Furthermore, by the work of T. Nagell and É Lutz, we can determine the torsion points of $E(\mathbb{Q})$.

**Theorem 1.1.27** ([35][42])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with simplified Weierstrass equation*[3]

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

*with discriminant $\Delta_E = -16(4a^3 + 27b^2) \neq 0$. If $P(x, y) \in E(\mathbb{Q})_{\mathrm{Tor}}$ different from the identity, then*

- *$x, y \in \mathbb{Z}$,*
- *either $y = 0$ else $y^2 | D$.*

These two theorems can be used to find the torsion group of any elliptic curve. This calculation can be done even by hand, as shown in [53, Chapter VIII, Example 7.4].

So, to be able to completely determine the abstract group structure of $E(\mathbb{Q})$ the only remaining part is to understand the free part of $E(\mathbb{Q})$. Unfortunately, this is not an easy task. For example, if we consider $r_E$ as $E/\mathbb{Q}$ varies through all the elliptic curves, it is not known if $r_E$ is bounded. At the moment of writing, the highest rank for an elliptic curve $E/\mathbb{Q}$ is known to be at least 28 found by N. Elkies, see the introduction of [26].

[3] As per remark 1.1.5 this equation will always exists.

### 1.1.5 Arithmetic invariants

As mentioned in the introduction, an elliptic curve $E/\mathbb{Q}$ has interesting and mysterious arithmetic properties. We have already seen one, the rank of $E$. There are other arithmetic invariants [4] attached to an elliptic curve. But, as is in the case of the rank of $E$, some of them are not very well understood.

If we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ for all primes $p \in \mathcal{P}$, we get an embedding of the corresponding Galois groups $\mathrm{Gal}_{\mathbb{Q}_p} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}$. Using Galois cohomology, we get a morphism

$$H^1(\mathrm{Gal}_{\mathbb{Q}}, E(\overline{\mathbb{Q}})) \to \prod_{p\in\mathcal{P}} H^1(\mathrm{Gal}_{\mathbb{Q}_p}, E(\overline{\mathbb{Q}}_p)).$$

The kernel of this morphism is known as the Tate-Shafarevich group[5].

**Definition 1.1.28.** Let $E/\mathbb{Q}$ be an elliptic curve. The **Tate-Shafarevich** is the group defined as

$$Ш_E := \ker\left(H^1(\mathrm{Gal}_{\mathbb{Q}}, E(\overline{\mathbb{Q}})) \to \prod_{p\in\mathcal{P}} H^1(\mathrm{Gal}_{\mathbb{Q}_p}, E(\overline{\mathbb{Q}}_p))\right).$$

Some results are known about the group structure of $Ш_E$, due to the work of B. Gross, D. Zagier, V. Kolyvagin, and J. Cassels. The work of Cassels allows us to conclude the following.

**Theorem 1.1.29** ([10],[56])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. If $Ш_E$ is finite, then $\#Ш_E$ is a perfect square.*

The hypothesis that $Ш_E$ is finite, in the previous theorem, is not known if it's superfluous. The statement that $Ш_E$ is finite is, in fact, a conjecture.

**Conjecture 1.1.30.** If $E/\mathbb{Q}$ is an elliptic curve, then $Ш_E$ is a finite group.

In some cases, it is known that $Ш_E$ is finite (See 2.1.6), but the general case remains open. Another fact about $Ш_E$ is that its finiteness is related to the calculation of the rank of an elliptic curve.

**Proposition 1.1.31.** [6] Let $E/\mathbb{Q}$ be an elliptic curve. If $Ш_E$ is finite, then there is a known algorithm to calculate the rank of $E$.

**Remark 1.1.32.** At the moment of writing, there is no known algorithm to compute the rank of an arbitrary elliptic curve (see the introduction of [54]). The fact that $Ш_E$ might be infinite is an obstruction to the well-known descent method to calculate the rank. Because, if $Ш_E$ is not finite, then the descent method may not halt.

[4] By *Arithmetic invariant* we mean a number or group attached to $E$ that is invariant under isomorphism defined over $\mathbb{Q}$

[5] For a more detailed construction of the Tate-Shafarevich group see [53][Chapter X, Section 4].

[6] See the preceding discussion of [53, Chapter X, Conjecture 4.3].

The last arithmetic invariant that we will define is the Tamagawa number.

**Definition 1.1.33.** Let $E/\mathbb{Q}$ be an elliptic curve. We define the **Tamagawa number** of $E$ as

$$C_E \coloneqq \prod_{p \text{ prime}} C_{E,p}$$

where $C_{E,p} \coloneqq \#(E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p))$ and $E^0(\mathbb{Q}_p)$ denotes the identity component.

In the case when the elliptic curve $E$ has split multiplicative reduction at a prime $p$, we have the following characterization of $C_{E,p}$ due to the work of A. Néron and K. Kodaira.

**Theorem 1.1.34** ([43], [27])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at $p$. Then*

$$C_{E,p} = \operatorname{ord}_p(q_{E,p}),$$

*where $q_{E,p}$ is the Tate $p$-adic period, defined in 1.1.22.*

**Remark 1.1.35.** By the work of J. Tate, we have an algorithm to calculate the Tamagawa number of any elliptic curve, see [55]

### 1.1.6 Hasse-Weil $L$-function of $E$

We define a complex-valued function attached to $E/\mathbb{Q}$.

**Definition 1.1.36.** Let $E/\mathbb{Q}$ by an elliptic curve with a global minimal Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \; a_i \in \mathbb{Z}.$$

The **Hasse-Weil $L$-function** of $E$, or simply **$L$-function** of $E$, is a complex-valued function defined as a Euler product

$$L(E,s) = \prod_{p \nmid N_E} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p | N_E} (1 - a_p p^{-s})^{-1}, \tag{1.12}$$

where $a_p \coloneqq p + 1 - \#\tilde{E}(\mathbb{F}_p)$, where $\tilde{E}$ denotes the reduction of $E$ modulo $p$.

**Proposition 1.1.37** ([17, 8.8])**.** Let $E/\mathbb{Q}$ be an elliptic curve. The Hasse-Weil $L$-function of $E$ has a series expansion of the form

$$L(E,s) = \sum_{n\mathbb{N}} \frac{a_n}{n^s}$$

for some $a_n \in \mathbb{Z}$; for example if $n = p$, then $a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p)$ as in definition 1.1.36. For the general description of $a_n$ see [17, 8.8].

**Proposition 1.1.38** ([53, C.16])**.** Let $E/\mathbb{Q}$ be an elliptic curve. The $L$-function of $E$ converges if $\operatorname{Re}(s) > 3/2$.

Even though the product (1.12) does not converge on the whole complex plane, by the modularity theorem, we will be able to conclude that the $L$-function has an analytic continuation to the whole complex plane. There is also a twisted version of the $L$-function.

**Definition 1.1.39.** Let $E/\mathbb{Q}$ be an elliptic curve and $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ Dirichlet character i.e. a group homomorphism. Let

$$L(E, s) = \sum_{n\in\mathbb{N}} \frac{a_n}{n^s},$$

be the series of the $L$-function attached to $E$ as in 1.1.37. We define the **twisted $L$ function of $E$ by $\chi$** as

$$L(E, \chi, s) = \sum_{n\in\mathbb{N}} \frac{a_n\chi(n)}{n^s}.$$

## 1.2 Modular forms

### 1.2.1 Definitions and basic properties

We will denote the **upper half plane** as

$$\mathcal{H} = \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\},$$

and the **extended upper half plane** as $\mathcal{H}^* := \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

**Definition 1.2.1.** Let $N \in \mathbb{N}$. We define the **modular group** as

$$\mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z});\ ad - bc = 1 \right\},$$

and the **Hecke subgroup at level $N$** as

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z});\ c \equiv 0 \mod N \right\}.$$

In particular $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.

Let $N \in \mathbb{N}$, we have a natural action of $\Gamma_0(N)$ on $\mathcal{H}$ and $\mathbb{P}^1(\mathbb{Q})$, by Möbious transformation i.e. if $\gamma \in \Gamma_0(N)$ then its action is defined as

$$z \mapsto \frac{az + b}{cz + d};\ \ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ z \in \mathcal{H}^*,$$

with the convention that $\frac{a\infty+b}{c\infty+d} = \frac{a}{c}$.

**Proposition 1.2.2.** We have that $\mathcal{H}$ has a natural structure of Riemann surface, and the action of $\Gamma_0(N)$ is totally discontinuous. This induces a structure of Riemann surface on the quotient $\Gamma_0(N) \setminus \mathcal{H}$.

*Proof.* Because $\mathcal{H}$ is a connected open subset of $\mathbb{C}$, it has a natural structure of Riemann surface, see [40, Example 1.21] and [40, 1.15]. For the proof the action of $\Gamma_0(N)$ in $\mathcal{H}$ is totally discontinuous, see [17, Proposition 2.1.1]. Finally, for the structure of Riemann structure of $\Gamma_0(N) \setminus \mathcal{H}$ which comes from the quotient topology, see [40, Proposition 3.3] □

**Definition 1.2.3.** Let $N \in \mathbb{N}$. We define the **open modular curve of level** $N$ as $Y_0(N) = \Gamma_0(N) \setminus \mathcal{H}$ and the **modular curve at level** $N$ as $X_0(N) \coloneqq \Gamma_0(N) \setminus \mathcal{H}^*$.

**Proposition 1.2.4.** The modular curve $X_0(N)$ is a compact Riemann surface. This allows us to identify $X_0(N)$ with a smooth projective curve over $\mathbb{C}$. Furthermore, the curve $X_0(N)$ is defined over $\mathbb{Q}$.

*Proof.* The fact that $X_0(N)$ is a compact Riemann surface can be seen in [17, Proposition], for the fact that it is a smooth projective curve defined over $\mathbb{Q}$ see [17, section 7.7]. □

**Definition 1.2.5.** Let $k, N \in \mathbb{N}$. A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is a **modular form of weight** $k$ for $\Gamma_0(N)$ if

- $f(\gamma z) = (cz + d)^k f(z)$ for any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.
- Define $f[\gamma]_k \coloneqq (cz + d)^{-k} f(\gamma z)$. Then $f[\gamma]_k$ is holomorphic at $\infty$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ i.e. the Fourier expansion has no negative powers:

$$f(z) = \sum_{n \in \mathbb{N}_0} a_n^{\gamma} q^n; \; q = e^{2\pi i z} \tag{1.13}$$

Moreover, we have the additional distinctions

- If in the Fourier expansion (1.13) we have that $a_0^{\gamma} = 0; \; \forall \gamma \in \Gamma_0(N)$, then we say that $f$ is a **cusp form of weight** $k$ for $\Gamma_0(N)$.
- If $f$ is a cusp form of weight $k$ and in the Fourier expansion (1.13) we have that $a_1 = 1$, then we say that the cusp for is **normalized**.
- If all the $a_n$ in Fourier expansion (1.13) are rational numbers we say that $f$ is **rational**.

We will denote the space of cusp forms of weight $k$ with respect to $\Gamma_0(N)$ by $S_k(\Gamma_0(N))$ and the rational cusp form of weight $k$ by $S_k(\Gamma_0(N))_{\mathbb{Q}}$, which are, in fact, complex vector spaces

**Definition 1.2.6.** Let $N \in \mathbb{N}$. The **Fricke involution** on $S_2(\Gamma_0(N))$ is defined as

$$\begin{aligned} w_N : S_2(\Gamma_0(N)) &\to S_2(\Gamma_0(N)) \\ f(z) &\mapsto \frac{1}{Nz^2} f\left(\frac{-1}{Nz}\right) \end{aligned}$$

**Proposition 1.2.7** ([17, 5.10])**.** The Fricke involution is an involution on $S_2(\Gamma_0(N))$, with eigenvalues ±1.

As is in the case of elliptic curves, we can also define a $L$-function for a modular form and, in some cases, these two $L$ functions will be equal.

**Definition 1.2.8.** Let $f \in S_2(\Gamma_0(N))$ be a cusp form. We define the $L$-**function** of $f$ as:

$$L(f,s) = \sum_{n \in \mathbb{N}} \frac{a_n}{n^s}$$

where $f(z) = \sum_{n \in \mathbb{N}} a_n q^n$ it the Fourier expansion at $\infty$.

**Proposition 1.2.9** ([17, 5.10])**.** Let $f \in S_2(\Gamma_0(N))$ be a cusp form. The $L$-function of $f$ converges if $\mathrm{Re}(s) > 2$.

Now, unlike the analytic continuation of the $L$-function of an elliptic curve $E/\mathbb{Q}$, the proof of the fact that the $L$-function of a modular form has an analytic continuation can be seen in textbooks of modular forms [17].

**Theorem 1.2.10** ([17, 5.10], Hecke)**.** *Let $f \in S_2(\Gamma_0(N))$ be an eigenvector of the Fricke involution $w_N$. The $L$-function attach to $f$ has an analytic continuation to $\mathbb{C}$ by the function*

$$\Lambda(f,s) = N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(f,s),$$

*where $\Gamma(s)$ denotes the gamma function and $-\epsilon$ is the eigenvalue of $f$ with respect to the Ficke involution $w_N$. Furthermore, the function $\Lambda(f,s)$ satisfies the following functional equation*

$$\Lambda(f,s) = \epsilon\Lambda(f,2-s).$$

**Proposition 1.2.11.** Let $f \in S_2(\Gamma_0(N))$ be a normalized cusp form. The set

$$\Lambda_f := \left\{ \int_{[\gamma]} f(z)dz;\ [\gamma] \in H_1(X_0(N), \mathbb{Z}) \right\}$$

is a lattice of $\mathbb{C}$.

**Corollary 1.2.12.** Consider a normalized weight 2 cusp form $f \in S_2(\Gamma_0(N))$. There exists an elliptic curve $E_f/\mathbb{C}$ such that

$$\mathbb{C}/\Lambda_f \cong E_f(\mathbb{C}).$$

*Proof.* This comes from the latter proposition and proposition 1.1.20. □

### 1.2.2 Connection between elliptic curves and modular forms

In this subsection, we will mention a very deep result in mathematics, which is a relation between new forms of weight 2 and elliptic curves. We can summarize this relation as follows. There is a one-to-one correspondence between:

$$\{\text{weight 2 normalized rational newforms}\} \leftrightarrow \{\text{optimal elliptic curves over } \mathbb{Q}\}$$

The proof of this statement is a result spanning years and it culminated with the work by C. Breuil, B. Conrad, F. Diamond, R. Taylor, and A. Wiles. They prove, what is now known as, the full modularity theorem in 2001.

**Proposition 1.2.13.** Let $f \in S_2(\Gamma_0(N))$ be a cusp form and a $M \in \mathbb{N}$. The function

$$g(z) := f(Mz)$$

is a cusp form of weight 2 of $\Gamma_0(NM)$.

A consequence of this proposition is that given a cusp form $f \in S_2(\Gamma_0(N))$, this cusp form could be of the form $g(Mz) \in S_2(d)$ where $Md = N$. So, the cusp form $f$ "comes" from a lower level. In some sense, it is an "old" cusp form and a "new" cusp form would be those that do not "come" from a lower level.

**Definition 1.2.14.** Let $N \in \mathbb{N}$. The space spanned in $S_2(\Gamma_0(N))$ by the set

$$\{g(Mz) \in S_2(\Gamma_0(N)); N = Md,\ g \in S_2(d)\}$$

is called the **space of old forms**, denoted by $S_2(\Gamma_0(N))^{\text{old}}$. The complement of $S_2(\Gamma_0(N))^{\text{old}}$, with respect to the Petersson inner product[7], is called the **space of new forms** and denoted by $S_2(\Gamma_0(N))^{\text{new}}$, or $S_2(\Gamma_0(N))^{\text{new}}_{\mathbb{Q}}$ if all its coefficients are rational.

By corollary 1.2.12 we can attach to any weight 2 normalized cusp form an elliptic curve $E_f$ as follows:

$$E_f(\mathbb{C}) \cong \mathbb{C}/\Lambda_f. \tag{1.14}$$

However, if $f$ also is a rational new form, then $E_f$ will be defined over $\mathbb{Q}$ and we can recover arithmetic information about the elliptic curve $E_f$. This is summarized in the following proposition

**Theorem 1.2.15** (Eichler-Shimura [18][51]). *Let $f \in S_2(\Gamma_0(N))^{\text{new}}_{\mathbb{Q}}$ is normalized and $E_f$ is the elliptic curve in 1.14. Then*

- *The elliptic curve $E_f$ is defined over $\mathbb{Q}$ and has conductor $N$.*
- *Let $p$ is prime number. If $p|N$, and $f|w_p = \epsilon_p f$, then $E_f$ has split multiplicative reduction if $\epsilon_p = 1$ and has non split multiplicative reduction if $\epsilon_p = -1$.*

[7] For our purposes, we will not define the Petersson inner product. For its definition see, [17, 5]

- *The elliptic curve $E_f$ is an optimal quotient of the Jacobian of $X_0(N)$.*
- *There exists a constant $c_{E_f} \in \mathbb{Q}$ such that*

$$2\pi i c_{E_f} f dz = \phi^*(\omega_{E_f}), \tag{1.15}$$

*where $\omega_{E_f}$ is the Néron differential attached to $E_f$, defined in 1.1.18.*

- *The L-function of $E_f$ and the L-function of $f$ are equal*

$$L(E_f, s) = L(f, s)$$

**Definition 1.2.16.** An elliptic curve that can be constructed using the previous theorem, is called an **optimal elliptic curve**.

**Proposition 1.2.17.** For every optimal elliptic curve $E$ there exists a complex uniformization $X_0(N) \to E$. The minimal degree on any surjective morphism $\phi : X_0(N) \to E$ is called the **modular degree** $\deg(\phi)$.

**Definition 1.2.18.** The absolute value of $c_{E_f}$ defined in 1.2.15 is called the **Manin constant** of $E_f$.

Though not explicitly mentioned, Y. Manin conjectured that the Manin constant is always 1.

**Conjecture 1.2.19.** If $E$ is an optimal elliptic curve, then $|c_E| = 1$.

**Remark 1.2.20.** This conjecture remains open. For an account of some general results regarding the Manin constant see [3]

Now, with theorem 1.2.15 we have a way to assign any rational cusp 2 new form an elliptic curve over $\mathbb{Q}$ and obtain arithmetic properties of the elliptic curve. The modularity theorem guarantees that any elliptic curve is isogenous to an optimal elliptic curve over $\mathbb{Q}$.

**Theorem 1.2.21** ([17, Theorem 8.8.4])**.** *For any elliptic curve $E/\mathbb{Q}$, there exists an optimal elliptic curve $E_f/\mathbb{Q}$ that is $\mathbb{Q}$-isogenous to $E$. So there exists a rational new form of weight two $f$ such that $E_f$ is $\mathbb{Q}$-isogenus to $E$.*

*Proof.* This is a consequence, or a different formulation depending on the author, of the Modularity theorem [17, Theorem 8.8.4]. The proof is due to the work of Wiles [59], Taylow-Wiles [58], and Breuil-Conrad-Diamond-Taylor [8]. □

Multiple statements receive the name modularity theorem. The more conventional one is the following, which is a consequence of 1.2.21.

**Theorem 1.2.22.** *Let $E/\mathbb{Q}$ be an elliptic curve. There exists a complex parametrization $\phi : X_0(N) \to E(\mathbb{C})$.*

### 1.2.3 Modular symbols

Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$, $\omega$ the Néron differential, $\Lambda$ the Néron lattice, and $f_E$ the weight 2 new form attached to $E$.

The lattice $\Lambda$ has two possible structures, depending on the discriminant of $E$.

**Proposition 1.2.23** ([11, Chapter II])**.** There exists unique positive real number $\Omega_E^{\pm} \in \mathbb{R}$ such that

- If $\Delta_E > 0$, then
$$\Lambda = \Omega_E^+\mathbb{Z} + \Omega_E^-\mathbb{Z}i.$$
- If $\Delta_E < 0$, then
$$\Lambda \subsetneq \Omega_E^+\mathbb{Z} + \Omega_E^-\mathbb{Z}i.$$
and $\Lambda$ is the sublattice consisting of the complex numbers $a \cdot \Omega_E^+ + b\Omega_E^- i$ such that $a \equiv 2 \mod 2$.

  The former case is called the **rectangular** case. While the latter case is called the **non-rectangular** case.

**Definition 1.2.24.** We define the **real period** of $E$ as the value $\Omega_E^+ \in \mathbb{R}$ from proposition 1.2.23.

By the work of Y. Manin and V. Drinfeld, we have the following theorem.

**Theorem 1.2.25** ([29, Chapter IV. §2])**.** *There exists* $\lambda^{\pm}(a,b) \in \mathbb{Q}$ *such that*

$$2\pi i \int_{\infty}^{\frac{a}{b}} f_E(z)dz = \lambda^+(a,b)\Omega_E^+ + \lambda^-(a,b)\Omega_E^- i$$

**Definition 1.2.26.** Let $E/\mathbb{Q}$ be an elliptic curve. Given $\frac{a}{b} \in \mathbb{Q}$, we define the modular symbol:

$$\lambda(a,b)_E \coloneqq \lambda^+(a,b),$$

where $\lambda(a,b)^+ \in \mathbb{Q}$ is defined in 1.2.25. Note that $\lambda(a,b)$ depends on the elliptic curve $E/\mathbb{Q}$. Nevertheless, we will omit the subscript $E$ i.e. $\lambda(a,b) \coloneqq \lambda(a,b)_E$, if the elliptic curve is implicitly clear.

**Proposition 1.2.27.** Let $\frac{a}{b} \in \mathbb{Q}$. The modular symbol satisfies the following identities

$$\lambda(a,b) = \lambda(-a,b), \tag{1.16}$$
$$\lambda(a,b) = \lambda(a+b,b). \tag{1.17}$$

*Proof.* Proof of (1.16): From [11, 2.1.3] we have that $f_E^*(z) := \overline{f_E(z^*)}$, where $z^* = -\overline{z}$, is a holomorphic function and if $f_E$ has a Fourier expansion $f_E(z) = \sum_{n\in\mathbb{N}} a_n q^n$, then $f_E^*(z) = \sum_{n\in\mathbb{N}} \overline{a}_n q^n$. On one side we have that

$$\begin{aligned} &= \overline{2\pi i \int_{i\infty}^{\frac{a}{b}} f_E(z)dz} \\ &= \overline{\lambda^+(a,b)\Omega_E^+ + \lambda^-(a,b)i\Omega_E^-} = \lambda^+(a,b)\Omega_E^+ - \lambda^-(a,b)\Omega_E^- i \end{aligned}$$

We can consider the following path of integration $\frac{a}{b} + iy$; $y \in [\infty, 0]$. So $dz = idy$ and

$$\begin{aligned} \overline{2\pi i \int_{i\infty}^{\frac{a}{b}} f_E(z)dz} &= \overline{2\pi i \int_{\infty}^{0} f_E\left(\frac{a}{b} + iy\right) i\, dy} \\ &= 2\pi i \int_{\infty}^{0} \overline{f_E\left(\frac{a}{b} + iy\right) i}\, dy \\ &= 2\pi i \int_{\infty}^{0} f_E^*\left(-\left(\overline{\frac{a}{b} + iy}\right)\right) i\, dy \\ &= 2\pi i \int_{\infty}^{0} f_E^*\left(\frac{-a}{b} + iy\right) i\, dy = 2\pi i \int_{i\infty}^{\frac{-a}{b}} f_E(z)dz \end{aligned}$$

We know that $f_E$ has rational coefficients, so

$$f_E^*(z) = \sum_{n\in\mathbb{N}} \overline{a}_n q^n = \sum_{n\in\mathbb{N}} a_n q^n = f_E(z)$$

We can conclude that,

$$2\pi i \int_{i\infty}^{\frac{-a}{b}} f_E(z)dz = 2\pi \int_{0}^{\infty} f_E^*\left(\frac{-a}{b} + iy\right) dy = \overline{2\pi i \int_{i\infty}^{\frac{a}{b}} f_E(z)dz} = \lambda^+(a,b)\Omega_E^+ - \lambda^-(a,b)\Omega_E^- i$$

Therefore $\lambda(a,b) = \lambda(-a,b)$. Proof of (1.17): We know that given a matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$

$$f_E(z) = (cz+d)^{-2} f_E(\gamma z)$$

In particular, if we consider the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$, then $cz + d = 1$. So

$$2\pi i \int_{i\infty}^{\frac{a}{b}} f_E(z)dz = 2\pi i \int_{i\infty}^{\frac{a}{b}} f_E(\gamma z)dz = 2\pi i \int_{i\infty}^{\frac{a}{b}} f_E(z+1)dz$$

If we make the following change of variable $w = z + 1$, we obtain

$$2\pi i \int_{i\infty}^{\frac{a}{b}} f_E(z)dz = 2\pi i \int_{i\infty}^{\frac{a}{b}} f_E(z+1)dz = 2\pi i \int_{i\infty}^{\frac{a+b}{b}} f_E(w)dw$$

□

# Chapter 2

# The BSD conjectures and its variations

## 2.1 Classical Birch-Swinnerton-Dyer conjectures

At the turn of the millennium, the Clay Institute of Mathematics selected 7 open conjectures in Mathematics, now known as the Millennium Prize Problems. The Clay Institute of Mathematics awards 1 million USD, to anyone who proves or disproves one of any of these conjectures. These problems are really profound in each of their areas. One of them is the Birch-Swinnerton-Dyer conjecture.

In 1960 B. Birch and P, Swinnerton-Dyer in [6], using numerical evidence, formulated the following conjecture

**Conjecture 2.1.1** ([6, Pag. 80, (1.5)])**.** Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$r_E \neq 0 \iff L(E,1) = 0.$$

**Remark 2.1.2.** We will use the abbreviation BSD for "Birch-Swinnerton-Dyer".

The current formulation, as stated by the Clay Institute of Mathematics [59], was formulated by A. Wiles.

**Conjecture 2.1.3** ([59])**.** Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$r_E = \mathrm{ord}_{s=1} L(E,s). \tag{2.1}$$

There is an even stronger version of the BSD conjectures, though we have to make the following assumption that will be kept for the rest of the thesis.

**Assumption 2.1.4.** If $E/\mathbb{Q}$ is an elliptic curve, then $Ш_E$ is finite.

**Conjecture 2.1.5** (Strong BSD conjecture)**.** Let $E/\mathbb{Q}$ be an elliptic curve. Using the same notation as in the previous section, we have that

$$\frac{L^{(r_E)}(E,1)}{r_E!\Omega_E^+} = \frac{\#\text{Ш}_E \cdot \text{Reg}(E)C_E}{(\#E(\mathbb{Q})_{\text{Tor}})^2},$$

where $\text{Reg}(E)$ is the regulator term, which depends on the free part of $E(\mathbb{Q})$ and the *Néron-Tate height*[1], which we will not define for the purposes of this thesis.

The main results regarding conjecture 2.1.3 is due to the work of B. Gross, D. Zagier, and V. Kolyvagin, which state the following

**Theorem 2.1.6** ([23] [28])**.** *Let $E/\mathbb{Q}$ be an elliptic curve. If* $\text{ord}_{s=1}L(E,s) \in \{0,1\}$ *then:*

1. *The identity* (2.1) *holds.*
2. *The group* $\text{Ш}_E$ *is finite.*

The proof of Kolyvagin relies on so-called "euler systems" and "heegner points", the former are certain classes of cohomology that allow one to relate arithmetic and analytic objects, while the former comes from the modular parametrization.

**Remark 2.1.7.** Finally, we want to mention that all these conjectures are for elliptic curves defined over $\mathbb{Q}$. There are generalizations of the BSD conjectures for the case of abelian varieties over an arbitrary number field [25, Conjecture F.4.1.6]. Furthermore, there is the generalizations for motives known as the Block-Kato conjectures [7].

## 2.2 $p$-adic BSD conjectures

There is a $p$-adic analog of the BSD conjectures stated by B. Mazur, J. Tate, and J. Teitelbaum in [39]. As stated in the introduction of their article [39, Pag. 1], after the $p$-adic analog of the $L$-function of an elliptic curve was defined, and the $p$-adic analogs to the theory of canonical height were developed, Mazur, Tate, and Teitelbaum embarked on the project of formulating a $p$-adic analog of the BSD conjectures. These conjectures depend on a certain $p$-adic analog of the $L$-function, the $p$-adic $L$-function $L_p(E,\cdot) : \mathbb{Z}_p \to \mathbb{Q}_p$ its construction can be seen in [39], [37], [4].

As is in the classical case, we consider an elliptic curve $E/\mathbb{Q}$ and we want to study the value of $L_p(E,s)$ at $s = 1$.

For our purposes, we will only state these conjectures when the elliptic curve $E/\mathbb{Q}$ has split multiplicative reduction at $p$. For a general account see [39].

[1] For the precise definition see [53, pag. 253] and for the complete construction [53, VIII.9]

**Conjecture 2.2.1** ([39, BSD($p$)-exceptional case])**.** Let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at $p$. Then

1. $L_p^{(k)}(E,1) = 0;\ \forall k < r_E + 1$.
2. $$L_p^{(r_E+1)}(E,1) = \frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})} \frac{\#\text{Ш}_E \cdot R_p^{\mathrm{Sch}}(E) C_E}{\#(E(\mathbb{Q})_{\mathrm{Tor}})^2}, \tag{2.2}$$

   where $q_{E,p}$ is the Tate $p$-adic period and $R_p^{\mathrm{Sch}}(E)$ is the $p$-adic regulator[2]. The ratio $\frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})}$ is called the ***L*-invariant** of $E$, which is a reason of the interest in the Tate $p$-adic period $q_{E,p}$.

**Remark 2.2.2.** These conjectures are known as the exceptional case, the reason being that when $p$ is a split multiplicative prime the $p$-adic $L$-function has a trivial 0 i.e. $L_p(E,1) = 0$, even if $L(E,1) \neq 0$.

We can see the similarities between the classical BSD conjectures and their $p$-adic version. Furthermore, we can rewrite (2.2) and relate it to the classical $L$-function.

**Conjecture 2.2.3.** Let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at $p$. Then

$$L_p^{(1)}(E,1) = \frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})} \frac{L(E,1)}{\Omega_E^+}$$

This conjecturem was, mostly, proven by R. Greenberg and G. Stevens in 1993 [22].

**Theorem 2.2.4** ([22, Theorem 0.3])**.** *Let $p \geq 5$ be a prime and $E$ be an elliptic curve with split multiplicative reduction at $p$. Then*

$$L_p^{(1)}(E,1) = \frac{\log_p(q_{E,p})}{\mathrm{ord}_p(q_{E,p})} \frac{L(E,1)}{\Omega_E^+}$$

**Remark 2.2.5.** It should be noted that Greenberg and Stevens prove a more general result. Not only do they prove that the identity holds for elliptic curves, but they also prove that the theorem holds for any new form of weight 2 which is split multiplicative at $p$ [22, Theorem 7.1].

## 2.3 Refined BSD conjectures

There is also a lesser-known variation of the BSD conjectures, which are the "refined" analogs stated by B. Mazur and J. Tate in 1987 [38]. The refined BSD

[2] For our purposes we will note use $R_p^{\mathrm{Sch}(E)}$, so we will not define it. For a detailed construction see [39, Pag. 35]

conjectures[3] are the main topic in this thesis. In particular, we are interested in [38, Conjecture 5] and [38, Conjecture 6]. So, we will omit some sections of the article [38] which are not necessary to state these conjectures.

We will use the same notation and conventions as in Section 1.

Fix an elliptic curve $E/\mathbb{Q}$ for the rest of the section. Given $M \in \mathbb{N}$, we denote by

$$G_M \coloneqq (\mathbb{Z}/M\mathbb{Z})^* \,/\, \langle -1 \rangle \,.$$

Also, we will denote by $\mathbb{Q}(\mu_M)^+$ the largest totally real field contained in $\mathbb{Q}(\mu_M)$, where $\mu_M$ denotes a primitive $M$-root of unity.

**Definition 2.3.1** (Mazur-Tate element at layer $M$)**.** [4] The Mazur-Tate element of $E$ at layer $M$ is defined as

$$\Theta_{E,M} \coloneqq \frac{1}{2} \sum_{a \in (\mathbb{Z}/M\mathbb{Z})^*} \lambda(a,M)[a] \in R\left[G_M\right]. \tag{2.3}$$

where $R \subsetneq \mathbb{Q}$ is a subring that contains $\{\lambda(a,M)\}_{a\in(\mathbb{Z}/M\mathbb{Z})^*}$, which by 1.2.25 we now that such a $R$ exists, and $[a]$ denotes the element in $G_M$ attached to $a$. We will denote $\Theta_{E,M}$ by $\Theta_M$ if the elliptic curve causes no confusion.

As for the classical and $p$-adic $L$-functions, we can define the vanishing order and the leading coefficient of $\Theta_M$, which depends on the augmentation ideal.

**Definition 2.3.2.** Let $R \subseteq \mathbb{Q}$ be a ring, $G$ an abelian group, and $R[G]$ the group ring. We consider the following ring morphism,

$$\begin{aligned} \phi : R[G] &\to R \\ \sum_{g\in G} a_g[g] &\mapsto \sum_{g\in G} a_g. \end{aligned}$$

We define the **Augmentation ideal** as

$$I \coloneqq \ker(\phi).$$

**Definition 2.3.3.** The vanishing order of $\Theta_M$ at layer $M$ is defined as

$$\operatorname{ord}(\Theta_M) \coloneqq \begin{cases} r & \text{if } \Theta_M \in I^r \text{ and } \Theta_M \notin I^{r+1}, \\ \infty & \text{if } \Theta_M \in I^n, \forall n \in \mathbb{N}. \end{cases}$$

We will state some properties of the augmentation ideal.

[3] In the literature, these conjectures can also be called the Mazur-Tate conjectures or Refined conjectures of BSD type

[4] In the literature, the Mazur-Tate element can also be referred to as a Stickelberger element.

**Lemma 2.3.4.** Let $G$ be an abelian group, $\mathbb{Z}[G]$ the group algebra, and $I$ the augmentation ideal. The augmented ideal is a free $\mathbb{Z}$-module, and $\{[g]-[e]\}_{g\in G-\{e\}}$ is a $\mathbb{Z}$-basis.

*Proof.* Let $\sum_{g\in G} a_g[g] \in I, a_g \in \mathbb{Z}$, this implies that

$$\sum_{g\in G} a_g = 0$$

Therefore

$$\sum_{g\in G} a_g[g] = \sum_{g\in G} a_g[g] - \sum_{g\in G} a_g[e] = \sum_{g\in G} a_g([g]-[e]).$$

The fact that $I$ is a free $\mathbb{Z}$-module is due to $\mathbb{Z}[G]$ being a free $\mathbb{Z}$-module, and a submodule of a free module is free. □

**Proposition 2.3.5.** Using the same notation as in the previous lemma, the groups $I/I^2$ and $G$ are isomorphic.

*Proof.* Consider the function

$$\begin{aligned} \rho : G &\to I/I^2 \\ g &\mapsto [g]-[e]+I^2 \end{aligned}$$

we can see that $[g]-[e] \in I, \forall g \in G$ so $\rho$ is well defined. Now we will show that $\rho$ is a morphism. Let's consider $a, b \in G$. We have that

$$\rho(a)+\rho(b)+I^2 = [a]-[e]+[b]-[e]+I^2$$

But, we have that $([a]-[e])([b]-[e]) \in I^2$. Therefore

$$[a]-[e]+[b]-[e]+I^2 = [a]-[e]+[b]-[e]+([a]-[e])([b]-[e])+I^2 = [ab]-[e]+I^2 = \rho(ab)+I^2$$

We can conclude that $\rho$ is a morphism. To show that $\rho$ is an isomorphism, we will prove that the function

$$\begin{aligned} \sigma : I/I^2 &\to G \\ \sum_{a\in G} r_a\left([a]-[e]\right)+I^2 &\mapsto \prod_{a\in G} a^{r_a} \end{aligned}$$

is the inverse of $\rho$. Using 2.3.4 we can see that a generating set of $I^2$ is $\{([a]-[e])([b]-[e])\}_{a,b\in G}$. Therefore, it is sufficient to prove that for all the elements of the form $([g]-[e])([h]-[e])+I^2$, we have that $\sigma\left(([g]-[e])([h]-[e])+I^2\right)=e$ to show that $\sigma$ is well defined.

So, let $([g]-[e])([h]-[e])+I^2 \in I/I^2$, we can see that

$$([g]-[e])([h]-[e])+I^2 = ([gh]-[e])-([g]-[e])-([h]-[e])+I^2.$$

Therefore

$$\sigma\left(([g]-[e])([h]-[e])+I^2\right)=\sigma\left(([gh]-[e])-([g]-[e])-([h]-[e])+I^2\right)=ghg^{-1}h^{-1}=e.$$

We can conclude that $\sigma$ is well-defined.

To prove the fact that $\sigma$ is a homomorphism, consider $\sum_{a\in G} r_a\left([a]-[e]\right)+I^2, \sum_{a\in G} r'_a\left([a]-[e]\right)+I^2 \in I/I^2$, we have that

$$\begin{aligned}
&\sigma\left(\sum_{a\in G} r_a\left([a]-[e]+I^2\right)+\sum_{a\in G} r'_a\left([a]-[e]\right)+I^2\right)\\
&=\sigma\left(\sum_{a\in G}(r_a+r'_a)\left([a]-[e]\right)+I^2\right)\\
&=\prod_{a\in G} a^{r_a+r'_a}=\left(\prod_{a\in G} a^{r_a}\right)\left(\prod_{a\in G} a^{r'_a}\right)\\
&=\sigma\left(\sum_{a\in G} r_a\left([a]-[e]\right)+I^2\right)+\sigma\left(\sum_{a\in G} r'_a\left([a]-[e]\right)+I^2\right)
\end{aligned}$$

We can conclude that $\sigma$ is a morphism.

Lastly, we have to prove that prove that $\sigma$ is the inverse of $\rho$. Let $g\in G$, we can see that

$$\sigma\circ\rho(g)=\rho([g]-[e]+I^2)=g$$

Reciprocally, let $x=\sum_{a\in G} r_a([a]-[e])+I^2\in I/I^2$, we have that,

$$\sigma\circ\rho\left(\sum_{a\in G} r_a([a]-[e])+I^2\right)=\rho\left(\prod_{a\in G} a^{r_a}\right)=\sum_{a\in G}\rho\left(a^{r_a}\right)=\sum_{a\in G} r_a([a]-[e]).$$

We can conclude that $I/I^2$ is isomorphic to $G$. □

## 2.4 Relation between Mazur-Tate element and the classical BSD conjecture

Consider a group homomorphism $\chi : G_M \to \mathbb{C}^*$, and let $R \subsetneq \mathbb{Q}$ be a ring that contains all the coefficients of $\Theta_M$.

By $R_\chi \subseteq \overline{\mathbb{Q}}$ we mean the $R$-algebra generated by $\operatorname{Im}(\chi)$. Consider the morphism

$$\begin{aligned}
\tilde{\chi} : R_\chi[G_M] &\to R_\chi\\
\sum_{g\in G_M} r_g[g] &\mapsto \sum_{g\in G_M} r_g\chi(g)
\end{aligned}$$

We define the augmentation ideal at $\chi$ as $I_\chi \coloneqq \ker(\tilde{\chi})$.

**Definition 2.4.1.** The vanishing order of $\Theta_M$ at $\chi$ is defined as

$$\operatorname{ord}_\chi(\Theta_M) = \begin{cases} r & \text{if } \Theta_M \in I_\chi^r \text{ and } \Theta_M \notin I_\chi^r, \\ \infty & \text{if } \Theta_M \in I_\chi^n, \forall n \in \mathbb{N}. \end{cases}$$

Also, if $r = \operatorname{ord}_\chi(\Theta_M) < \infty$, then the leading coefficient of $\Theta_M$ at $\chi$ is the image of $\Theta_M$ in $I_\chi^r / I_\chi^{r+1}$.

We have two conjectures relating the vanishing order of $\Theta_M$ at $\chi$ and the classical BSD conjecture.

**Proposition 2.4.2** ([38, pag. 716])**.** Let $M \in \mathbb{N}$. Then

$$\begin{aligned} \sigma : G_M &\to \operatorname{Gal}(\mathbb{Q}(\mu_M)^+/\mathbb{Q}) \\ a &\mapsto \sigma_a. \end{aligned}$$

This allow us to identify $G_M$ with $\operatorname{Gal}(\mathbb{Q}(\mu_M)^+/\mathbb{Q})$.

**Definition 2.4.3.** The $\chi$-part of the Mordell-Weil of $E$ is the complex vector subspace $V_\chi \subseteq E(\mathbb{Q}(\mu_M)^+) \otimes \mathbb{C}$ generated by all $v$ such that; given $a \in \mathbb{Z}$ with $(a, M) = 1$

$$\sigma_a \cdot v = \chi(a) \cdot v$$

where we use the identification by proposition 2.4.2.

**Conjecture 2.4.4** ([38, Conjecture 1])**.** Using the same notation as before, we have that

$$\operatorname{ord}_\chi(\Theta_M) \geq \dim_{\mathbb{C}}(V_\chi).$$

There is also a conjecture relating the vanishing order of $\Theta_M$ at $\chi$ and the $L$-function of $E$ twisted by $\chi$ (defined as in 1.1.39).

**Conjecture 2.4.5** ([38, Conjecture 2])**.** Using the same notation as before, we have that

$$\operatorname{ord}_\chi(\Theta_M) \geq \operatorname{ord}_{s=1} L(E, \chi, s)$$

## 2.5 Conjectures

Let $E/\mathbb{Q}$ be an elliptic with conductor $N$, $S \subseteq \mathcal{P}$, and fix the notation $\tau_E := \#E(\mathbb{Q})_{\mathrm{Tor}}$. Also, let $S_m \subseteq S$ be the subset of primes $p$ such that $E$ has split multiplicative reduction $p$ and if $q_{E,p}$ it the Tate $p$-adic period at $p$, then we will denote by $\tilde{q}_{E,p} := q_{E,p}/p^{\operatorname{ord}_p(q_{E,p})} \in \mathbb{Z}_p^*$. Set

$$C_S := \left( \prod_{p \in S \setminus S_m} \mathbb{F}_p^* \times \prod_{p \in S_m} \mathbb{Z}_p^* \right) / \langle -1 \rangle .$$

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

$$M := \prod_{p \in S \setminus S_m} p \prod_{p \in S_m} p^{e_p} \tag{2.4}$$

We can see that we have a natural projection from $C_S \to G_M$.

$$r := r_E + \#S_m$$

and

$$\phi_{S_m} = \#\text{coker}\left( E(\mathbb{Q}) \to \prod_{p \in \mathcal{P} - S_m} (E(\mathbb{Q}_p)/E^0(\mathbb{Q}_p)) \right),$$

where $E^0(\mathbb{Q}_p)$ denotes the identity component.

**Conjecture 2.5.1** ([38, conjecture 4])**.** Let $R \subsetneq \mathbb{Q}$ a subring that contains all the denominators of $\Theta_M$. Then

1. We have that $\text{ord}(\Theta_M) \geq r$.
2. If we denote by $\tilde{\Theta}_M$ the image of $\Theta_M$ in $I^r/I^{r+1}$, then

$$\tilde{\Theta}_M \equiv \#\text{Ш}_E \phi_{S_m} \eta_r \left(\text{Disc}_S(E)\right) \in I^r/I^{r+1}$$

where $\eta_r : R \otimes \text{Sym}_\text{r}(\text{C}_\text{S}) \to I^r/I^{r+1}$ and $\text{Disc}_S(E) \in R \otimes \text{Sym}_\text{r}(\text{C}_\text{S})$ is the corrected discriminant [5]

An interesting aspect of this conjecture is that in contrast to the classical BSD conjectures the order of vanishing of $\Theta_M$ does not depend only on the rank of $E$, it also depends on the cardinality of $S_m$. Similarly to the $p$-adic $L$-function 2.2.2, if $\#S_m > 0$ then it is conjectured that $\Theta_M$ has "trivial zeros", one for each prime of split multiplicative reduction.

If we focus on the case when $r_E = 0$ and $S = S_m$ [38, (2.9) Pag. 742], we get that

$$\eta_r \left(\text{Disc}_S(E)\right) \equiv \prod_{p \in S_m} ([\tilde{q}_{E,p}] - [1]) \in I^r/I^{r+1}.$$

So, a particular case of conjecture 2.5.1 is the following.

**Conjecture 2.5.2** ([38, conjecture 5])**.** Assume that $r_E = 0$, $S = S_m$, and $\tau_E^{-1} \in R$. Then

1. We have that $\text{ord}(\Theta_M) \geq r$.
2. If we denote by $\tilde{\Theta}_M$ the image of $\Theta_M$ in $I^r/I^{r+1}$, then

$$\tilde{\Theta}_M \equiv \prod_{p \in S_m} ([\tilde{q}_{E,p}] - [1]) \frac{\#\text{Ш}_E \prod_{p \in \mathcal{P} - S_m} C_{E,p}}{\tau_E^2} \in I^r/I^{r+1}. \tag{2.5}$$

[5] For the statement of the conjectures of interest its not necessary the construction. For a detailed construction, see [38, Chapter 2]

**Remark 2.5.3.** We can formulate a "multiplicative" conjecture similar to conjecture 2.5.2, which will be easier to implement in SageMath. Consider the case when $S = S_m = \{p\}$ and $M = p$. Also, denote by $\tilde{\Theta}_p$ the image of $\Theta_p$ in $I/I^2$. We can multiply both sides of (2.5) by $\mathrm{ord}_p(q_{E,p})$, which is equal to $C_{E,p}$ by Theorem 1.1.33, and rearranging the equation we get

$$\tau_E^2 \cdot \mathrm{ord}_p(q_{E,p}) \cdot \tilde{\Theta}_p = ([\tilde{q}_{E,p}] - [1]) \cdot \#\text{Ш}_E \cdot C_E \in I/I^2$$

Now, denote by $D$ the least common multiple between all the denominators of the modular symbols $\{\lambda(a,p)\}_{0<a<p}$. By multiplying both sides of the equation by $2D$[6] we guarantee that both sides of the equation are integers.

$$D\tau^2 \mathrm{ord}_p(q_{E,p}) \left( \sum_{0<a<p} \lambda(a,p)\sigma_a \right) = ([\tilde{q}_{E,p}] - [1]) \cdot 2D \cdot \#\text{Ш}_E \cdot C_E \in I/I^2 \quad (2.6)$$

Finally, we can see that equation (2.6) is well defined if $R = \mathbb{Z}$, which may not be for equation 2.5. So, if we consider $R = \mathbb{Z}$ we can use the isomorphism $I/I^2 \xrightarrow{\sim} G_M$, defined in 2.3.5, to get the following "multiplicative" conjecture similar to conjecture 2.5.2.

**Conjecture 2.5.4.** Using the same notation as in 2.5.2. Assume that $r_E = 0$, $S = S_m = \{p\}$, and $M = p$. Then:

1. We have that $\mathrm{ord}(\Theta_p) \geq 1$.
2. We have the following equality

$$\prod_{0<a<p} a^{D\cdot\tau_E^2\cdot\mathrm{ord}_p(q_{E,p})\lambda(a,p)} \equiv \tilde{q}_{E,p}^{2D\cdot(\#\text{Ш}_E)\cdot C_E} \in (\mathbb{Z}/p\mathbb{Z})^* / \langle -1 \rangle . \quad (2.7)$$

Returning to the general, before the remark 2.5.3, the classical BSD conjecture predicts that if $r_E = 0$ then

$$\frac{\lambda(0,1)}{2} = \frac{\#\text{Ш}_E \cdot C_E}{\tau_E^2} \iff \frac{\lambda(0,1)}{2\prod_{p\in S_m} C_{E,p}} = \frac{\#\text{Ш} \cdot \prod_{p\in\mathcal{P}-S_m} C_{E,p}}{\tau_E^2}$$

Using this, we can rewrite conjecture 2.5.2 to get the following formulation

**Conjecture 2.5.5** ([38, conjecture 6])**.** Assume that $\lambda(0,1)/(2\prod_{p\in S_m} C_{E,p})$ is invertible in $R$ and $S = S_m$.

1. We have that $\mathrm{ord}(\Theta_M) \geq r$.
2. If we denote by $\tilde{\Theta}_M$ the image of $\Theta_M$ in $I^r/I^{r+1}$, then

$$\tilde{\Theta}_M = \prod_{p\in S_m} ([\tilde{q}_{E,p}] - [1]) \frac{\lambda(0,1)}{2\prod_{p\in S_m} C_{E,p}} \in I^r/I^{r+1}. \quad (2.8)$$

[6] The factor 2 comes from the fact that $\Theta_p$ has a $\frac{1}{2}$ multiplying all the modular symbols

If $E(\mathbb{Q})$ is not finite, then both sides are conjecturally 0.

We can use the same procedure that we used to get conjecture 2.5.4 from conjecture 2.5.2 to get a "multiplicative" conjecture similar to conjecture 2.5.5.

**Conjecture 2.5.6.** Assume that $S = S_m = \{p\}$ and $M = p$. Then

1. We have that $\operatorname{ord}(\Theta_p) \geq 1$.
2. We have the following identity:

$$\prod_{0<a<p} a^{D\lambda(a,p)\operatorname{ord}_p(q_{E,p})} = \tilde{q}_{E,p}^{D\lambda(0,1)} \in (\mathbb{Z}/p\mathbb{Z})^* \,/\, \langle -1 \rangle \tag{2.9}$$

where $D$ is the least common multiple between all the denominators of the modular symbols $\{\lambda(a,p)\}_{0\leq a<p}$. If $E(\mathbb{Q})$ is not finite, then both sides are conjecturally 1.

**Remark 2.5.7.** The reason to consider these two variation of conjecture 2.5.2 and conjecture 2.5.5, is that there are easier to implement in SageMath.

**Remark 2.5.8.** We want to mention that there are two conjectures that we did not mention here.

1. There is the so-called "Main weak conjecture", which relates the Mazur-Tate element with the *Fitting ideal* of the *Integral Selmer group.* For the precise statement see [38, "Main weak conjecture", Pag. 720].
2. Mazur and Tate also conjecture a quadratic congruence relations between certain modular symbols. For the precise statement see [38, Conjecture 7, Pag. 746]

# Chapter 3

# Progress on the refined BSD conjectures

In comparison with the classical BSD conjectures and its $p$-adic analog, not much work has been done regarding the refined BSD conjectures. Moreover, most of the focus has been in regard to the vanishing order of the Mazur-Tate element, not much work has been done regarding conjecture 2.5.2 or conjecture 2.5.5.

We will mention some important results regarding the Mazur-Tate element and the conjectures surrounding it.

## 3.1 Vanishing order

We will use the same notation as in the previous section. One aspect of the refined BSD conjectures is proving that

$$\operatorname{ord}(\Theta_M) \geq r_E + \#S_m.$$

We can see that the vanishing order of $\Theta_M$ depends on two factors the rank of the elliptic curve and the cardinality of $S_m$. This has not been fully proven, though there is some progress towards it, mainly by the work of K. Ota, F. Bergunde, and L. Gehrmann. Ota's work studies the relation between $\operatorname{ord}(\Theta_M)$ and $r_E$ in the case when $\#S_m = 0$. On the other hand, F. Bergunde and L. Gehrmann study the relation between $\operatorname{ord}(\Theta_M)$ and $\#S_m$, in the case when $r_E = 0$. We will first mention the work of Ota.

Ota's result does involve some hypothesis, which he considers "mild". Mainly, the restriction is in terms of which elements on $R$ are invertible.

**Definition 3.1.1** ([44, Pag. 496])**.** Let $E/\mathbb{Q}$ be an elliptic curve with conductor $N$, which does not have complex multiplication i.e. $\mathbb{Z} \cong \operatorname{End}(E)$ as groups. A prime number $p$ is admissible if

- $p$ does not divide
$$\#E(\mathbb{F}_p)6N\prod_{\ell|N}[E(\mathbb{Q}_\ell):E_0(\mathbb{Q}_\ell)]$$
where $\ell$ is a prime and $E_0(\mathbb{Q}_\ell)$ denotes the group of points of $E(\mathbb{Q}_\ell)$ with non-singular reduction, see [53, Pag. 188].
- The Galois representation $\mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$ is surjective, where $T_p(E)$ denotes the Tate module[1].
- $p \geq r_E$.

The main theorem of Ota's article [44] is the following.

**Theorem 3.1.2** ([44, Theorem 1.2])**.** *Let $E/\mathbb{Q}$ be an elliptic curve and $R \subseteq \mathbb{Q}$ a subring such that every prime that is not admissible for $E$ is invertible in $R$. Let $M$ be a product of square-free primes $\ell \nmid N_E$, such that for each prime $p$ that is not invertible in $R$, the module $E(\mathbb{F}_\ell)[p]$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or $\{0\}$. Then $\Theta_M \in R[G_M]$ and*
$$\mathrm{ord}(\Theta_M) \geq r_E.$$

We can see that under some hypotheses, Ota proves that, if $\#S_m = 0$, then the vanishing order of $\Theta_M$ is at least $r_E$. However, Ota's result does not guarantee that $\mathrm{ord}(\Theta_M) = r_E$. Furthermore, as he mentions [44, Remark 2.5.i)], there are some cases where $\mathrm{ord}(\Theta_M) > r_E$.

As mentioned before, in [5] Gehrmann and Bergunde consider an elliptic curve of rank 0 and $\#S_m > 0$.

**Theorem 3.1.3** ([5])**.** *Let $E$ be an elliptic curve of rank 0. Also, let $R \subsetneq \mathbb{Q}$ be a subring that contains the modular symbols $\lambda(a,b)$ for all $\frac{a}{b} \in \mathbb{Q}$ and $S_m \subseteq \mathcal{P}$ a set of primes numbers, such that for each $p \in S_m$ $E$ has split multiplicative reduction at $p$. Then*
$$\mathrm{ord}(\Theta_M) \geq \#S_m,$$
*where $M = \prod_{p\in S_m} p$.*

Therefore, if the rank of $E$ is 0 and $\#S_m = r$, then the Mazur-Tate element has order at least $r$.

The is no result regarding the case when $r_E > 0$ and $\#S_m > 0$.

## 3.2 The leading coefficient of the Mazur-Tate element

The major work regarding the leading coefficient of the Mazur-Tate element has been done by E. de Shalit in the particular case when the conductor of the elliptic

[1] For the Galois representation attached to $T_p$ see [53, Chapter III.7]

curve is a prime number $p$. In a series of articles [15], [16], and [14], de Shalit replicates the techniques of Greenberg and Stevens [22] in the refined setting, which allows him to conclude the following theorem.

**Theorem 3.2.1** ([16, Theorem 0.3])**.** *Let $E$ be an elliptic curve of conductor $p$. Also, let $\ell \geq 5$ be a prime number such that $\ell | p-1$. If $\ell$ is coprime to the modular degree of $E$ and $\tilde{q}_{E,p} = q_{E,p}/p^{\mathrm{ord}_p(q_{E,p})}$ then*

$$\prod_{0<a<p} a^{\lambda(a,p)\mathrm{ord}_p(q_{E,p})} = \tilde{q}_{E,p}^{\lambda(0,1)}$$

*in the $\ell$-Sylow component of the natural decomposition of $(\mathbb{Z}/p\mathbb{Z})^*$ in its $\ell$-Sylow subgroups.*

Another work regarding the leading coefficient of the Mazur-Tate element was done by F. Portillo-Bobadilla in his PhD thesis [46][2] and also in a subsequent article [45]. In [46] Portillo-Bobadilla studies similar conjectures stated in [38]. However, Portillo-Bobadilla has some limitations regarding the calculation of the modular symbols of the elliptic curves as we will mention in the next subsection.

## 3.3 Numerical evidence

As hinted above, a big limitation of numerical evidence for evidence is the calculation of the necessary modular symbols used to define the Mazur-Tate element. For example, in Portillo-Bobadilla's PhD thesis, he was unable to calculate the modular symbols of an elliptic curve of conductor 1610, due to computational limitations [46, Chapter 5].

However, since the last article of Portillo-Bobadilla, optimization has been done to the algorithms for calculating modular symbols. There are three methods with implementation in SageMath, we will mention only two of them:

- The Eclib package implementation, which was written by J. Cremona. Cremona's way of calculating modular symbols is known to be exact because it depends on the fact that one can reduce the problem to solving a system of equations [11].

  However, this method is sometimes slow and also has a hard limit. Because, as the conductor gets larger the Random Access Memory needed also grows, so after a certain point it is impossible to continue.

- The other way was developed by C. Wutrich in [61]. Wutrich's algorithm uses numerical approximations to integrate the integral and bounds on the denominators to get, in some cases, a faster way of calculating method modular symbols. However, there are also some limitations to this implementation, especially in the case when the conductor of $E$ is not square-free, see [61, Introduction].

[2] F. Portillo-Bobadilla did his PhD thesis under the supervision of F. Voloch.

We have calculated the modular symbols necessary to check conjecture 2.5.4 and 2.5.6 of 503301 pairs of the form $(E,p)$ where $E/\mathbb{Q}$ is an elliptic curve with split multiplicative reduction at $p$. This was done with an Intel i5-8300H, with 32 GB of RAM, in Manjaro 6.1.55-1, and SageMath version 10.1. All the necessary calculations were done over several days and saved in various text files. We will refer to all the pairs $(E,p)$ calculated as "database".

Afterward, we wrote a script to check conjecture 2.5.6 and 2.5.4 with the database that we calculated. We found the following results:

1. With respect to conjecture 2.5.6, of all the 503301 pairs $(E,p)$, the script outputted 393 elliptic curves that, apparently, do not satisfy conjecture 2.5.6. A random sample of 10 pairs $(E,p)$ was checked using CoCalc's implementation of SageMath, and we found the same results. This was to guarantee that it was not a flaw in our script. In Appendix A, we give the first 100 examples of elliptic curves that, apparently, do not satisfy 2.5.6.
2. With respect to conjecture 2.5.4, of all the 206110 pairs $(E,p)$ with $r_E = 0$, we did not find any counterexample for this conjecture.

In Appendix B we give 4 examples of how we carried out calculations using CoCalc's implementation of SageMath. For the full code and implementation see [30].

**Remark 3.3.1.** Unfortunately, we were unable to check a large number of elliptic curves using a different program, we encountered some issues with the "old" program *modsymb.gp*[3] written in PARI/GP, which was used in Portillo-Bobadilla's thesis. We were only able to test the elliptic curve $11.a3$ and it did match the calculation by SageMath. Also, we have to remark that there may be a miscalculation with some arithmetic invariants. For more information see `https://www.lmfdb.org/EllipticCurve/Q/Reliability`. Therefore, we have to take caution in some cases, due to the possible flaws that may be presented in Lmfdb and also from our implementation of conjecture 2.5.4 and conjecture 2.5.6 in SageMath.

## 3.4 Conjectures

After finding a possible flaw in conjecture 2.5.6 we checked if an analog of de Shalit theorem [16, Theorem 0.3] holds for arbitrary conductors, under the same hypothesis.

**Conjecture 3.4.1.** Let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at $p$, $\ell \geq 5$ a prime number with $\ell | p-1$ and $\ell$ coprime to the modular degree of $E$. Then

$$\prod_{0<a<p} a^{D\cdot \mathrm{ord}_p(q_{E,p})\lambda(a,p)} \equiv \tilde{q}_{E,p}^{D\cdot\lambda(0,1)}$$

[3] The latest update that we were able to find was an updated made in 2002 written by L. Wetherell *et al.* [19]

where $D$ is the least common multiple of denominators of $\{\lambda(p,a)\}_{0\leq a<p}$ and the equality holds in the $\ell$-Sylow component of the natural decomposition of $(\mathbb{Z}/p\mathbb{Z})^*$ in its $\ell$-Sylow subgroups.

This equation does hold for all the elliptic curves in our database.

Therefore, conjecture 3.4.1 and conjecture 2.5.4 do appear to hold, though further calculations are needed.

# Appendix A

Let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at a prime $p$, $q_{E,p}$ the Tate $p$-adic period (see 1.1.22), and $\lambda(a,b)$ the modular symbols of $E$ with the $+$ sign (see 1.2.26). Also, let $\tilde{q}_{E,p} = q_{E,p}/p^{\mathrm{ord}_p(q_{E,p})}$

This Appendix contains a table of 100 elliptic curves that, apparently, do not satisfy conjecture 2.5.6 i.e. the equation

$$\prod_{0<a<p} a^{D\lambda(a,p)\mathrm{ord}_p(q_{E,p})} \equiv \tilde{q}_{E,p}^{D\lambda(0,1)} \in (\mathbb{Z}/p\mathbb{Z})^* \, / \, \langle -1 \rangle \tag{3.1}$$

where $D$ is the least common multiple of the denominators of the modular symbols $\{\lambda(a,p)\}_{0\leq a<p}$.

**Remark 3.4.2.** We want to note that this is the equation that Mazur and Tate tested, minus the factor $D$, in their original article [38] equation (*) pag. 746. However, there is a missing factor of $\mathrm{ord}_p(q_{E,p})$, in the exponent of the left-hand side of the aforementioned equation, as pointed out by de Shalit in [16, pag. 254].

For the full list of elliptic curves that, apparently, do not satisfy conjecture 2.5.6 see [30], which also contains the code used and an explanation of how it works.

- Label: Every elliptic curve has a unique label indexed in the `http://lmfdb.org` web page. The first sequence of numbers in each label is the conductor of the elliptic curve i.e. an elliptic curve with label 1890.$k$3 has conductor 1890. The terms after the point do not enter into effect for our purposes.
- Prime: This is the prime for which $E$ has split multiplicative reduction and the layer of the Mazur-Tate element i.e. $M = p$.
- Left side: It is the left side of the equation (3.1), i.e.

$$\prod_{0<a<p} a^{D\lambda(a,p)\mathrm{ord}_p(q_{E,p})}$$

- Right side: It is the right side of the equation (3.1), i.e.

$$\tilde{q}_{E,p}^{D\lambda(0,1)}$$

- Rank: Is the $\mathbb{Z}$-rank of the $E(\mathbb{Q})$ i.e. $r_E$.
- $q_{E,p}$: The $p$-adic expansion of the Tate $p$-adic period. Because we only need the order and the leading coefficient, we only express the first factor of the expansion.
- mod deg: Given a minimal modular parametrization $\phi : X_0(N) \to E(\mathbb{C})$. The modular degree is $\deg(\phi)$.

| Label | Prime | Left side | Right side | rank | $q_{E,p}$ | mod deg |
|---|---|---|---|---|---|---|
| 11.a3 | 11 | 1 | 9 | 0 | $8 \cdot 11^1 + O(11^2)$ | 5 |
| 14.a5 | 7 | 1 | 3 | 0 | $3 \cdot 7^1 + O(7^2)$ | 3 |
| 14.a4 | 7 | 1 | 2 | 0 | $2 \cdot 7^2 + O(7^3)$ | 6 |
| 15.a4 | 5 | 1 | 3 | 0 | $3 \cdot 5^1 + O(5^2)$ | 4 |
| 15.a7 | 5 | 1 | 2 | 0 | $2 \cdot 5^1 + O(5^2)$ | 4 |
| 19.a3 | 19 | 1 | 7 | 0 | $8 \cdot 19^1 + O(19^2)$ | 3 |
| 26.a3 | 13 | 12 | 4 | 0 | $11 \cdot 13^1 + O(13^2)$ | 6 |
| 35.a2 | 7 | 1 | 4 | 0 | $2 \cdot 7^1 + O(7^2)$ | 6 |
| 37.b3 | 37 | 1 | 26 | 0 | $10 \cdot 37^1 + O(37^2)$ | 6 |
| 38.a2 | 19 | 1 | 11 | 0 | $7 \cdot 19^1 + O(19^2)$ | 18 |
| 77.b1 | 7 | 1 | 4 | 0 | $3 \cdot 7^2 + O(7^3)$ | 60 |
| 126.b2 | 7 | 2 | 1 | 0 | $6 \cdot 7^1 + O(7^2)$ | 72 |
| 126.b1 | 7 | 4 | 1 | 0 | $1 \cdot 7^2 + O(7^3)$ | 144 |
| 130.b4 | 5 | 1 | 3 | 0 | $3 \cdot 5^1 + O(5^2)$ | 8 |
| 130.b4 | 13 | 9 | 6 | 0 | $6 \cdot 13^1 + O(13^2)$ | 8 |
| 158.b3 | 79 | 62 | 4 | 0 | $9 \cdot 79^1 + O(79^2)$ | 120 |
| 182.d3 | 7 | 4 | 1 | 0 | $1 \cdot 7^1 + O(7^2)$ | 12 |
| 189.c1 | 7 | 1 | 4 | 0 | $5 \cdot 7^1 + O(7^2)$ | 36 |
| 195.a6 | 5 | 1 | 3 | 0 | $3 \cdot 5^1 + O(5^2)$ | 24 |
| 195.a6 | 13 | 3 | 2 | 0 | $2 \cdot 13^1 + O(13^2)$ | 24 |
| 234.e1 | 13 | 4 | 12 | 0 | $8 \cdot 13^1 + O(13^2)$ | 180 |
| 278.a1 | 139 | 80 | 35 | 0 | $114 \cdot 139^1 + O(139^2)$ | 816 |
| 315.b1 | 7 | 4 | 1 | 0 | $1 \cdot 7^1 + O(7^2)$ | 180 |
| 326.a3 | 163 | 53 | 140 | 0 | $125 \cdot 163^1 + O(163^2)$ | 612 |
| 370.a1 | 37 | 1 | 10 | 0 | $11 \cdot 37^1 + O(37^2)$ | 324 |
| 378.e3 | 7 | 4 | 1 | 0 | $1 \cdot 7^1 + O(7^2)$ | 36 |
| 378.d1 | 7 | 1 | 2 | 0 | $4 \cdot 7^1 + O(7^2)$ | 108 |
| 378.g3 | 7 | 4 | 2 | 0 | $2 \cdot 7^1 + O(7^2)$ | 216 |
| 434.d2 | 7 | 1 | 2 | 0 | $4 \cdot 7^1 + O(7^2)$ | 48 |
| 434.d2 | 31 | 1 | 5 | 0 | $6 \cdot 31^1 + O(31^2)$ | 48 |
| 485.a3 | 97 | 85 | 65 | 0 | $68 \cdot 97^1 + O(97^2)$ | 420 |
| 546.d3 | 7 | 2 | 1 | 0 | $6 \cdot 7^1 + O(7^2)$ | 216 |
| 550.j1 | 11 | 9 | 1 | 0 | $1 \cdot 11^1 + O(11^2)$ | 1200 |
| 651.b3 | 7 | 1 | 2 | 0 | $3 \cdot 7^1 + O(7^2)$ | 96 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 651.b3 | 31 | 4 | 20 | 0 | $19 \cdot 31^1 + O(31^2)$ | 96 |
| 693.b3 | 7 | 4 | 1 | 0 | $6 \cdot 7^2 + O(7^3)$ | 1800 |
| 702.a1 | 13 | 1 | 9 | 0 | $6 \cdot 13^2 + O(13^3)$ | 3240 |
| 702.m2 | 13 | 4 | 10 | 0 | $6 \cdot 13^1 + O(13^2)$ | 216 |
| 702.p3 | 13 | 3 | 1 | 0 | $5 \cdot 13^2 + O(13^3)$ | 1080 |
| 798.d6 | 19 | 9 | 6 | 0 | $14 \cdot 19^1 + O(19^2)$ | 1152 |
| 798.d5 | 19 | 6 | 4 | 0 | $6 \cdot 19^2 + O(19^3)$ | 2304 |
| 806.f3 | 13 | 3 | 1 | 0 | $8 \cdot 13^1 + O(13^2)$ | 1008 |
| 819.c1 | 13 | 9 | 1 | 0 | $5 \cdot 13^1 + O(13^2)$ | 864 |
| 903.b3 | 7 | 4 | 1 | 0 | $6 \cdot 7^2 + O(7^3)$ | 912 |
| 910.g6 | 7 | 2 | 4 | 0 | $2 \cdot 7^2 + O(7^3)$ | 576 |
| 910.g4 | 7 | 4 | 2 | 0 | $4 \cdot 7^1 + O(7^2)$ | 1152 |
| 938.d3 | 7 | 1 | 4 | 0 | $4 \cdot 7^1 + O(7^2)$ | 528 |
| 938.d3 | 67 | 9 | 60 | 0 | $31 \cdot 67^1 + O(67^2)$ | 528 |
| 1118.a2 | 13 | 12 | 10 | 0 | $6 \cdot 13^1 + O(13^2)$ | 156 |
| 1118.a2 | 43 | 11 | 23 | 0 | $25 \cdot 43^1 + O(43^2)$ | 156 |
| 1206.f1 | 67 | 39 | 59 | 0 | $22 \cdot 67^1 + O(67^2)$ | 10368 |
| 1342.b3 | 61 | 57 | 12 | 0 | $16 \cdot 61^1 + O(61^2)$ | 3200 |
| 1422.f1 | 79 | 4 | 62 | 0 | $21 \cdot 79^1 + O(79^2)$ | 3600 |
| 1638.f1 | 7 | 1 | 4 | 0 | $2 \cdot 7^1 + O(7^2)$ | 3240 |
| 1638.f1 | 13 | 3 | 1 | 0 | $12 \cdot 13^1 + O(13^2)$ | 3240 |
| 1806.g3 | 7 | 2 | 4 | 0 | $5 \cdot 7^1 + O(7^2)$ | 720 |
| 1890.k3 | 7 | 1 | 2 | 0 | $5 \cdot 7^2 + O(7^3)$ | 1296 |
| 1890.i2 | 7 | 4 | 2 | 0 | $3 \cdot 7^1 + O(7^2)$ | 1944 |
| 1890.r1 | 7 | 2 | 4 | 0 | $3 \cdot 7^2 + O(7^3)$ | 3888 |
| 1890.t2 | 7 | 1 | 4 | 0 | $5 \cdot 7^1 + O(7^2)$ | 648 |
| 1953.f1 | 7 | 4 | 2 | 0 | $5 \cdot 7^1 + O(7^2)$ | 6912 |
| 1953.f1 | 31 | 28 | 18 | 0 | $10 \cdot 31^1 + O(31^2)$ | 6912 |
| 1995.g3 | 19 | 6 | 9 | 0 | $16 \cdot 19^1 + O(19^2)$ | 360 |
| 2145.b5 | 5 | 1 | 3 | 0 | $2 \cdot 5^3 + O(5^4)$ | 19968 |
| 2145.b5 | 13 | 1 | 5 | 0 | $8 \cdot 13^1 + O(13^2)$ | 19968 |
| 2163.d3 | 7 | 1 | 4 | 0 | $5 \cdot 7^1 + O(7^2)$ | 312 |
| 2163.d3 | 103 | 81 | 18 | 0 | $92 \cdot 103^1 + O(103^2)$ | 312 |
| 2379.a2 | 13 | 1 | 3 | 0 | $4 \cdot 13^1 + O(13^2)$ | 528 |
| 2379.a2 | 61 | 9 | 57 | 0 | $22 \cdot 61^1 + O(61^2)$ | 528 |
| 2405.b3 | 5 | 1 | 3 | 0 | $3 \cdot 5^1 + O(5^2)$ | 608 |
| 2405.b3 | 37 | 10 | 14 | 0 | $14 \cdot 37^1 + O(37^2)$ | 608 |
| 2418.b1 | 13 | 9 | 3 | 0 | $9 \cdot 13^1 + O(13^2)$ | 1800 |
| 2457.f3 | 13 | 9 | 1 | 0 | $8 \cdot 13^2 + O(13^3)$ | 2160 |
| 2502.g3 | 139 | 120 | 36 | 0 | $62 \cdot 139^1 + O(139^2)$ | 19584 |
| 2562.f2 | 7 | 4 | 2 | 0 | $3 \cdot 7^1 + O(7^2)$ | 648 |
| 2562.f2 | 61 | 9 | 56 | 0 | $19 \cdot 61^1 + O(61^2)$ | 648 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2590.a2 | 7 | 4 | 1 | 0 | $1 \cdot 7^1 + O(7^2)$ | 3960 |
| 2590.a2 | 37 | 7 | 33 | 0 | $25 \cdot 37^1 + O(37^2)$ | 3960 |
| 2709.b1 | 7 | 1 | 4 | 0 | $5 \cdot 7^2 + O(7^3)$ | 65664 |
| 2709.b1 | 43 | 9 | 11 | 0 | $32 \cdot 43^1 + O(43^2)$ | 65664 |
| 2718.o1 | 151 | 97 | 84 | 0 | $125 \cdot 151^1 + O(151^2)$ | 15552 |
| 2730.m4 | 7 | 2 | 1 | 0 | $1 \cdot 7^1 + O(7^2)$ | 5184 |
| 2730.m5 | 7 | 2 | 1 | 0 | $1 \cdot 7^2 + O(7^3)$ | 10368 |
| 2771.a1 | 163 | 53 | 133 | 0 | $40 \cdot 163^1 + O(163^2)$ | 4266 |
| 3094.e2 | 7 | 4 | 2 | 0 | $3 \cdot 7^1 + O(7^2)$ | 1080 |
| 3145.b4 | 5 | 1 | 3 | 0 | $2 \cdot 5^3 + O(5^4)$ | 7872 |
| 3145.b4 | 37 | 10 | 23 | 0 | $24 \cdot 37^1 + O(37^2)$ | 7872 |
| 3206.e3 | 7 | 1 | 2 | 0 | $2 \cdot 7^1 + O(7^2)$ | 1320 |
| 3206.e3 | 229 | 203 | 75 | 0 | $65 \cdot 229^1 + O(229^2)$ | 1320 |
| 3294.b1 | 61 | 20 | 25 | 0 | $42 \cdot 61^1 + O(61^2)$ | 6048 |
| 3294.k3 | 61 | 25 | 20 | 0 | $58 \cdot 61^1 + O(61^2)$ | 2016 |
| 3458.c2 | 13 | 3 | 9 | 0 | $9 \cdot 13^1 + O(13^2)$ | 3888 |
| 3458.c2 | 19 | 7 | 1 | 0 | $18 \cdot 19^2 + O(19^3)$ | 3888 |
| 3474.h1 | 193 | 130 | 112 | 0 | $72 \cdot 193^1 + O(193^2)$ | 25920 |
| 3510.o2 | 13 | 9 | 1 | 0 | $5 \cdot 13^1 + O(13^2)$ | 1296 |
| 3605.c3 | 7 | 1 | 4 | 0 | $2 \cdot 7^1 + O(7^2)$ | 1560 |
| 3605.c3 | 103 | 9 | 2 | 0 | $65 \cdot 103^1 + O(103^2)$ | 1560 |
| 3870.h1 | 43 | 38 | 35 | 0 | $22 \cdot 43^1 + O(43^2)$ | 15552 |
| 3906.a1 | 31 | 5 | 1 | 0 | $30 \cdot 31^1 + O(31^2)$ | 12960 |

# Appendix B

In this Appendix, we will explain step-by-step how we checked by hand conjecture 2.5.4 and conjecture 2.5.6 using SageMath. We will give 2 examples with conjecture 2.5.6, curves $910.g6$ and $11.a3$, and 2 examples with conjecture 2.5.4; curves $315.b2$ and $77.c2$.

**Remark 3.4.3.** All the calculations can be done on CoCalc's page, which has a section to use SageMath online [49]. Also, we used the documentation of SageMath for writing our code, for how to use modular symbols see [1] and see [2] for how to use the Tate curve package.

**Example 3.4.4** (First example with conjecture 2.5.6)**.** Consider the elliptic curve $E/\mathbb{Q}$ with the Lmfdb label $910.g6$ [33]. A Weierstrass equation for $E$ is

$$E : y^2 + xy = x^3 - 1196x + 15760.$$

We can use the following code to check if $E$ has split multiplicative reduction at $p = 7$.

```
    Input:
    E = EllipticCurve("910.g6")
    E.has_split_multiplicative_reduction(7)
    Sagemath Output:
    True

```

The following code returns the $p$-adic expansion of the Tate $p$-adic period for the prime $p = 7$, defined in 1.1.22.

```
    Input:
    E = EllipticCurve("910.g6").tate_curve(7)
    E.parameter()
    Sagemath Output:
    2*7^2 + 2*7^4 + 5*7^6 + 4*7^7 + 3*7^8 + 6*7^9 + 4*7^10 +
   7^12 + 2*7^13 + 3*7^14 + 2*7^15 + 6*7^16 + 2*7^17 + 3*7^18
   + 5*7^19 + O(7^22)

```

For the calculation of the modular symbols, we use Eclib package implementation in SageMath: [4]:

```
 Input:
 from sage.schemes.elliptic_curves.ell_modular_symbols import ModularSymbolECLIB
 E = EllipticCurve("910.g6")
 M = ModularSymbolECLIB(E,+1)
 (M(0), M(1/7), M(2/7), M(3/7), M(4/7), M(5/7), M(6/7)) # The parenthesis is added to be able to output all the values at once as an ordered tuple. But it can also be done one by one.
 Sagemath Output:
 (2, 2, -2, 0, 0, -2, 2)

```

So we have that

$$\begin{aligned}&\lambda(0,1)=2;\ \lambda(1,7)=\lambda(6,7)=2;\ \lambda(2,7)=\lambda(5,7)=-2;\\&\lambda(3,7)=\lambda(4,7)=0\\&q_{E,p}=2\cdot 7^2+2\cdot 7^4+5\cdot 7^6+4\cdot 7^7+O(7^8)\end{aligned}$$

We can see that all modular symbols are integers, so $D=1$.

The left-hand side of equation 2.9 turns out to be

$$\prod_{a=1}^{6} a^{\mathrm{ord}_p(q_{E,p})\lambda(a,11)} = 1^{2\cdot 2}2^{2\cdot -2}3^{2\cdot 0}4^{2\cdot 0}5^{2\cdot -2}6^{2\cdot 2} \equiv 2 \pmod 7$$

and the right-hand side turn of equation 2.9 turns out to be

$$\tilde{q}_{E,p}^{\lambda(0,1)} = 2^2 \equiv 4 \pmod 7.$$

Therefore, we get the contradiction:

$$2 \equiv \pm 4 \pmod 7,$$

in $(\mathbb{Z}/7\mathbb{Z})^*/\left\langle -1 \right\rangle$.

**Example 3.4.5** (Second example with conjecture 2.5.6)**.** Consider the elliptic curve $E/\mathbb{Q}$ with the Lmfdb label $11.a3$ [31]. A Weierstrass equation for $E$ is

$$E: y^2+y=x^3-x^2.$$

We can use the following code to check if $E$ has split multiplicative reduction at $p=11$.

[4] The Eclib package was written and used by J. Cremona to make his database of elliptic curves [12], using the method described in [11].

```
Input:
E = EllipticCurve("11.a3")
E.has_split_multiplicative_reduction(11)
Sagemath Output:
True

```

The following code returns the $p$-adic expansion of the Tate $p$-adic period.

```
Input:
E = EllipticCurve("11.a3").tate_curve(11)
E.parameter()
Sagemath Output:
8*11 + 3*11^2 + 5*11^3 + 8*11^4 + 9*11^6 + 2*11^7 + 11^8 +
10*11^10 + 2*11^12 + 9*11^13 + 10*11^14 + 11^15 + 7*11^16 +
 7*11^17 + 2*11^18 + 6*11^19 + 4*11^20 + O(11^21)

```

For the calculation of the modular symbols, we use Eclib package implementation in SageMath (In the case of negative discriminant we have to multiply the values by 2):

```
Input:
from sage.schemes.elliptic_curves.ell_modular_symbols
import ModularSymbolECLIB
E = EllipticCurve("11.a3")
M = ModularSymbolECLIB(E,+1)
(M(0), M(1/11), M(2/11), M(3/11), M(4/11), M(5/11), M(6/11)
, M(7/11), M(8/11), M(9/11), M(10/11))
Sagemath Output:
(1/25, 0, 1/5, 1/10, -1/10, -1/5, -1/5, -1/10, 1/10, 1/5,
0)

```

So we have that

$$\begin{aligned}
&\lambda(0,1) = \frac{2}{25};\ \lambda(1,11) = \lambda(10,11) = 0;\ \lambda(2,11) = \lambda(9,11) = \frac{2}{5};\\
&\lambda(3,11) = \lambda(8,11) = \frac{1}{5}\\
&\lambda(4,11) = \lambda(7,11) = \frac{-1}{5};\ \lambda(5,11) = \lambda(6,11) = \frac{-2}{5}\\
&q_{E,p} = 8\cdot 11 + 3\cdot 11^2 + 5\cdot 11^3 + 8\cdot 11^4 + 9\cdot 11^6 + 2\cdot 11^7 + O(11^8)
\end{aligned}$$

We can see that the least common multiple of the denominators of the modular symbols is $D = 25$.

The left-hand side of equation 2.9 turns out to be

$$\prod_{a=1}^{11} a^{D\cdot \mathrm{ord}_p(q_{E,p})\lambda(a,11)} = 1^{25\cdot 0} 2^{\frac{25}{5}} 3^{\frac{25}{10}} 4^{\frac{-25}{10}} 5^{\frac{-25}{5}} 6^{\frac{-25}{5}} 7^{\frac{-25}{10}} 8^{\frac{25}{10}} 9^{\frac{25}{5}} 10^{25\cdot 0} \equiv 1 \pmod{11}$$

and the right-hand side turn of equation 2.9 turns out to be

$$\tilde{q}_{E,p}^{D\lambda(0,1)} = 8^{\frac{50}{25}} \equiv 9 \pmod{11}.$$

Therefore, we get the contradiction:

$$1 \equiv \pm 9 \pmod{11},$$

in $(\mathbb{Z}/11\mathbb{Z})^{*}/\langle -1 \rangle$.

**Example 3.4.6** (First example with conjecture 2.5.4)**.** Consider the elliptic curve $E/\mathbb{Q}$ with the Lmfdb label $315.b2$ [32]. A Weierstrass equation for $E$ is

$$E : y^2 + y = x^3 - 12x - 18$$

We can use the following code to check if $E$ has split multiplicative reduction at $p = 7$.

```
    Input:
    E = EllipticCurve("315.b2")
    E.has_split_multiplicative_reduction(7)
    Sagemath Output:
    True

```

The following code returns the $p$-adic expansion of the Tate $p$-adic period.

```
    Input:
    E = EllipticCurve("315.b2").tate_curve(7)
    E.parameter()
    Sagemath Output:
    2*7 + 2*7^2 + 2*7^3 + 6*7^5 + 7^6 + 6*7^7 + 5*7^8 + 6*7^9 +
     7^10 + 5*7^11 + 2*7^12 + 3*7^13 + 5*7^14 + 7^15 + 3*7^16 +
     4*7^17 + 2*7^18 + 7^19 + 6*7^20 + O(7^21)

```

For the calculation of the modular symbols, we use Eclib package implementation in SageMath (This elliptic curve has negative discriminant):

```
    Input:
    from sage.schemes.elliptic_curves.ell_modular_symbols
   import ModularSymbolECLIB
    E = EllipticCurve("315.b2")
    M = ModularSymbolECLIB(E,+1)
    (M(1/7), M(2/7), M(3/7), M(4/7), M(5/7), M(6/7))
    Sagemath Output:
    (1, -1, 0, 0, -1, 1)

```

We can get the arithmetic invariants of the elliptic curve $315.b2$ with Lmfdb [32]. From Lmfdb we can see that $\#E(\mathbb{Q}) = 1$, $C_E = 1$, and $\#\text{Ш}_E = 1$.

So, we have the that

$$\lambda(1,7)=\lambda(6,7)=2;\ \lambda(2,7)=\lambda(5,7)=-2;\ \lambda(3,7)=\lambda(4,7)=0$$
$$q_{E,p}=2\cdot 7+2\cdot 7^2+2\cdot 7^3+6\cdot 7^5+7^6+6\cdot 7^7+5\cdot 7^8+O(7^9)$$

We can see that all modular symbols are integers, so $D=1$.

The left-hand side of 2.7 turns out to be

$$\prod_{a=1}^{6} a^{\lambda(a,7)\mathrm{ord}_p(q_{E,p})}=1^2 2^{-2} 3^0 4^0 5^{-2} 6^2 \equiv 4 \pmod 7$$

and the right-hand side of 2.7 turns out to be

$$\tilde{q}^2_{E,p}\equiv 2^2\equiv 4 \pmod 7$$

So we get

$$4\equiv \pm 4 \pmod 7,$$

in $(\mathbb{Z}/7\mathbb{Z})^*/\langle -1\rangle$.

**Example 3.4.7** (Seconds example with conjecture 2.5.4)**.** Consider the elliptic curve $E/\mathbb{Q}$ with the Lmfdb label $77.c2$ [34]. A Weierstrass equation for $E$ is

$$E: y^2+xy=x^3+x^2+4x+11$$

We can use the following code to check if $E$ has split multiplicative reduction at $p=11$.

```
    Input:
    E = EllipticCurve("77.c2")
    E.has_split_multiplicative_reduction(11)
    Sagemath Output:
    True

```

The following code returns the $p$-adic expansion of the Tate $p$-adic period.

```
    Input:
    E = EllipticCurve("77.c2").tate_curve(11)
    E.parameter()
    Sagemath Output:
    3*11^2 + 9*11^3 + 9*11^4 + 6*11^5 + 6*11^6 + 10*11^7 +
   3*11^8 + 10*11^10 + 4*11^11 + 7*11^12 + 4*11^13 + 2*11^14 +
     4*11^16 + 8*11^17 + 8*11^18 + 4*11^19 + 3*11^20 + 6*11^21
   + O(11^22)

```

For the calculation of the modular symbols, we use Eclib package implementation in SageMath (This elliptic curve has negative discriminant):

```
Input:
from sage.schemes.elliptic_curves.ell_modular_symbols import ModularSymbolECLIB
E = EllipticCurve("77.c2")
M = ModularSymbolECLIB(E,+1)
(M(1/11), M(2/11), M(3/11), M(4/11), M(5/11), M(6/11), M(7/11), M(8/11), M(9/11), M(10/11))
Sagemath Output:
(1/2, 0, -1/2, 0, 0, 0, 0, -1/2, 0, 1/2)

```

We can get the arithmetic invariants of the elliptic curve $315.b2$ with Lmfdb [34]. From Lmfdb we can see that $\#E(\mathbb{Q}) = 2$, $C_E = 2$, and $\#Ш_E = 1$.

So, we have the that

$$\begin{aligned}
&\lambda(1,11) = \lambda(10,11) = 1;\ \lambda(2,11) = \lambda(9,11) = 0\\
&\lambda(3,11) = \lambda(8,11) = -1;\ \lambda(4,11) = \lambda(7,11) = 0;\ \lambda(5,11) = \lambda(6,11) = 0\\
&q_{E,p} = 3 \cdot 11^2 + 9 \cdot 11^3 + 9 \cdot 11^4 + 6 \cdot 11^5 + 6 \cdot 11^6 + 10 \cdot 11^7 + O(11^8)
\end{aligned}$$

We can see that the least common multiple of the denominators of the modular symbols is $D = 1$.

The left-hand side of 2.7 turns out to be

$$\prod_{a=1}^{11} a^{8\lambda(a,11)} = 1^8 2^0 3^{-8} 4^0 5^0 6^0 7^0 8^{-8} 9^0 10^8 \equiv 4 \pmod{11}$$

and the right-hand side of 2.7 turns out to be

$$\tilde{q}_{E,p}^{2\cdot 2} \equiv 3^4 \equiv 4 \pmod{11}$$

So we get

$$4 \equiv \pm 4 \pmod{11},$$

in $(\mathbb{Z}/11\mathbb{Z})^* / \langle -1 \rangle$.

# Bibliography

[1] Modular symbols attached to elliptic curves over $\mathbb{Q}$ - elliptic curves. https://doc.sagemath.org/html/en/references/.../ell modular symbols.html.

[2] parametrisation of $p$-adic curves with multiplicative reduction - elliptic curves. https://doc.sagemath.org/html/en/references/.../ell tate curve.html.

[3] Amod Agashe, Kenneth Ribet, and William A. Stein. The Manin constant. *Pure Appl. Math. Q.*, 2(2):617–636, 2006.

[4] Yvette Amice and Jacques Vélu. Distributions $p$-adiques associées aux séries de Hecke. In *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974)*, volume No. 24-25 of *Astérisque*, pages 119–131. Soc. Math. France, Paris, 1975.

[5] Felix Bergunde and Lennart Gehrmann. On the order of vanishing of Stickelberger elements of Hilbert modular forms. *Proc. Lond. Math. Soc. (3)*, 114(1):103–132, 2017.

[6] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[7] Spencer Bloch and Kazuya Kato. $L$-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[8] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[9] James Carlson, Arthur Jaffe, and Andrew Wiles, editors. *The Millennium Prize Problems.* American Mathematical Society, Providence, RI, June 2006.

[10] J. W. S. Cassels. Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. *J. Reine Angew. Math.*, 211:95–112, 1962.

[11] J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, second edition, 1997.

[12] John Cremona, Marcus Mo, Julien Puydt, William Stein, qed777, Giovanni Mascellani, François Bissey, and abergeron. eclib: v.20150827, August 2015.

[13] Henri Darmon. Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications. *Ann. of Math. (2)*, 154(3):589–639, 2001.

[14] Ehud de Shalit. On certain Galois representations related to the modular curve $X_1(p)$. *Compositio Math.*, 95(1):69–100, 1995.

[15] Ehud de Shalit. On the $p$-adic periods of $X_0(p)$. *Math. Ann.*, 303(3):457–472, 1995.

[16] Ehud de Shalit. $p$-adic periods and modular symbols of elliptic curves of prime conductor. *Invent. Math.*, 121(2):225–255, 1995.

[17] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[18] Martin Eichler. Quaternäre quadratische formen und die riemannsche vermutung fÜr die kongruenzzetafunktion. *Archiv der Mathematik*, 5(4–6):355–366, August 1954.

[19] Joseph L. Wetherell et al. *The pari script modsym.gp.* available at `http://pari.math.u-bordeaux.fr/Scripts/modsym.gp.`, 2002.

[20] G. Frey. Rationale Punkte auf Fermatkurven und getwisteten Modulkurven. *J. Reine Angew. Math.*, 331:185–191, 1982.

[21] A. Goldberger and E. de Shalit. Tamely ramified Hida theory. *Ann. Inst. Fourier (Grenoble)*, 52(1):1–45, 2002.

[22] Ralph Greenberg and Glenn Stevens. $p$-adic $L$-functions and $p$-adic periods of modular forms. *Invent. Math.*, 111(2):407–447, 1993.

[23] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of $L$-series. *Invent. Math.*, 84(2):225–320, 1986.

[24] Robin Hartshorne. *Algebraic geometry*, volume No. 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.

[25] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[26] Zev Klagsbrun, Travis Sherman, and James Weigandt. The Elkies curve has rank 28 subject only to GRH. *Math. Comp.*, 88(316):837–846, 2019.

[27] K. Kodaira. On the structure of compact complex analytic surfaces. I. *Amer. J. Math.*, 86:751–798, 1964.

[28] V. A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.

[29] Serge Lang. *Introduction to modular forms*, volume No. 222 of *Grundlehren der Mathematischen Wissenschaften*. Springer-Verlag, Berlin-New York, 1976.

[30] Juan Pablo Llerena. Github with the code and tables of mazur-tate numerical calculation. `https://github.com/JpLlerena/MazurTate`.

[31] The LMFDB Collaboration. The L-functions and modular forms database, home page of the elliptic curve over $\mathbb{Q}$ with lmfdb label `11.a3`. `https://www.lmfdb.org/EllipticCurve/Q/11/a/3`, 2023. [Online; accessed 27 November 2023].

[32] The LMFDB Collaboration. The L-functions and modular forms database, home page of the elliptic curve over $\mathbb{Q}$ with lmfdb label `315.b2`. `https://www.lmfdb.org/EllipticCurve/Q/315/b/2`, 2023. [Online; accessed 27 November 2023].

[33] The LMFDB Collaboration. The L-functions and modular forms database, home page of the elliptic curve over $\mathbb{Q}$ with lmfdb label `33.a3`. `https://www.lmfdb.org/EllipticCurve/Q/910/g/6`, 2023. [Online; accessed 27 November 2023].

[34] The LMFDB Collaboration. The L-functions and modular forms database, home page of the elliptic curve over $\mathbb{Q}$ with lmfdb label `77.c2`. `https://www.lmfdb.org/EllipticCurve/Q/77/c/2`, 2023. [Online; accessed 27 November 2023].

[35] E. Lutz. Sur l'equation y 2 = x3 - ax - b dans les corps p-adic. *J. Reine Angew. Math.*, pages 177:237–247, 1937.

[36] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186, 1977. With an appendix by Mazur and M. Rapoport.

[37] B. Mazur and P. Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.

[38] B. Mazur and J. Tate. Refined conjectures of the "Birch and Swinnerton-Dyer type". *Duke Math. J.*, 54(2):711–750, 1987.

[39] B. Mazur, J. Tate, and J. Teitelbaum. On $p$-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84(1):1–48, 1986.

[40] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 1995.

[41] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. 1922.

[42] T. Nagell. Solution de quelque problémes dans la théorie arithmétique des cubiques planes du premier genre. *Wid. Akad. Skrifter Oslo I*, 1935.

[43] André Néron. Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ. Math.*, (21):128, 1964.

[44] Kazuto Ota. Kato's Euler system and the Mazur-Tate refined conjecture of BSD type. *Amer. J. Math.*, 140(2):495–542, 2018.

[45] Francisco X. Portillo-Bobadilla. Experimental evidence on a refined conjecture of the BSD type. *Bol. Soc. Mat. Mex. (3)*, 25(3):529–541, 2019.

[46] Francisco Xavier Portillo-Bobadilla. *Computations on an equation of the Birch and Swinnerton-Dyer type*. ProQuest LLC, Ann Arbor, MI, 2004. Thesis (Ph.D.)–The University of Texas at Austin.

[47] K. A. Ribet. On modular representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[48] Peter Roquette. *Analytic theory of elliptic functions over local fields*, volume Heft 1 of *Hamburger Mathematische Einzelschriften (N.F.)*. Vandenhoeck & Ruprecht, Göttingen, 1970.

[49] Sagemath, Inc. CoCalc – Collaborative Calculation and Data Science, 2020. `https://cocalc.com`.

[50] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$). *Duke Math. J.*, 54(1):179–230, 1987.

[51] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume No. 1 of *Kanô Memorial Lectures*. Iwanami Shoten Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971. Publications of the Mathematical Society of Japan, No. 11.

[52] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[53] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[54] William Stein and Christian Wuthrich. Algorithms for the arithmetic of elliptic curves using Iwasawa theory. *Math. Comp.*, 82(283):1757–1792, 2013.

[55] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, volume Vol. 476 of *Lecture Notes in Math.*, pages 33–52. Springer, Berlin-New York, 1975.

[56] John Tate. Duality theorems in Galois cohomology over number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 288–295. Inst. Mittag-Leffler, Djursholm, 1963.

[57] John T. Tate. The arithmetic of elliptic curves. *Invent. Math.*, 23:179–206, 1974.

[58] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[59] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[60] Andrew Wiles. The Birch and Swinnerton-Dyer conjecture. In *The millennium prize problems*, pages 31–41. Clay Math. Inst., Cambridge, MA, 2006.

[61] Christian Wuthrich. Numerical modular symbols for elliptic curves. *Math. Comp.*, 87(313):2393–2423, 2018.